Embracing complexity of Systems-of-Systems using Model-Based Risk Assessment and Safety Analysis (MBRASA)

Workshop

Joakim Fröberg, joakim.froberg@safetyintegrity.se
Tom Strandberg tom.strandberg@syntell.se

TECOSA cag Syntell Safety Integrity

EVENT

The Scandinavian Conference on System and Software Safety 2022

Embracing complexity of Systems-of-Systems using Model-Based Risk Assessment and Safety Analysis (MBRASA)

Given the trends of connectivity and autonomy, a current challenge is to ensure safety among multiple vehicles or machines, so called systems-of-systems, where parts of the end-to-end function reside in the edge and where communication is done wirelessly.

Based on such extended systems definition, the hazard and risk analysis need to be extrapolated to ensure trustworthiness for the extended scope.

The purpose of this workshop is to present and obtain feedback on the evolution of the model-based approach to risk assessment and safety analysis (MBRASA) of systems-of-systems that was the topic of a workshop at SCSSS2021.

Agenda Nov 23

13:30 Introduction to MBRASA, TECoSA, research idea

13:35 Use cases presentation

13:45 The Approach

- Safety analysis moving into systems of systems
- System models supporting safety analysis
- Method approach

14:45 Workshop (including break)

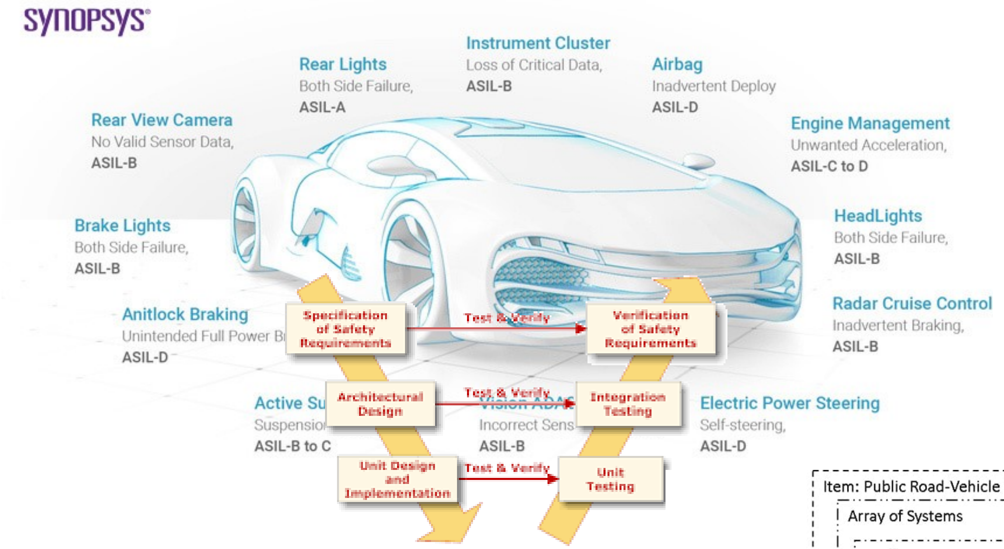
- Workshop set-up
- Group Discussions

15:45 Exchange and summary

16:30 Finish

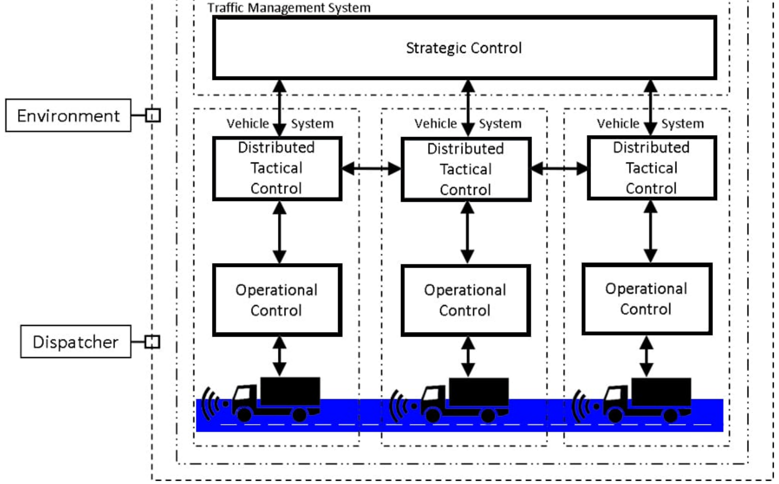
TECOSA

MBRASA – embracing complexity using Model-Based Risk Assessment and Safety Analysis



Item: Public Road-Vehicle Platooning (Distributed)

Array of Systems



TECOSA

MBRASA project

GOAL

- One goal is to support the industry by replacing complex and time-consuming work with safety processes and integration, with a trustworthy methodology and models, reducing the overall workload.

USE CASE(s)

PROJECT

- SME project
  - Syntell AB
  - Safety Integrity
  - Einride
  - KTH
- 7 Months, 2021-2022
- Supported by TECoSA and Vinnova

Participants

- Heike Schneider
- Tom Strandberg
- Lars-Olof Kihlström
- Joakim Fröberg
- Sebastian Holmqvist
- Fredrik Asplund
- Martin Törngren

TECoSA Syntell Safety Integrity

Agenda Nov 23

13:30 Introduction to MBRASA, TECoSA, research idea

13:35 Use case presentation

13:45 The Approach

- Safety analysis moving into systems of systems
- System models supporting safety analysis
- Method approach

14:45 Workshop (including break)

- Workshop set-up
- Group Discussions

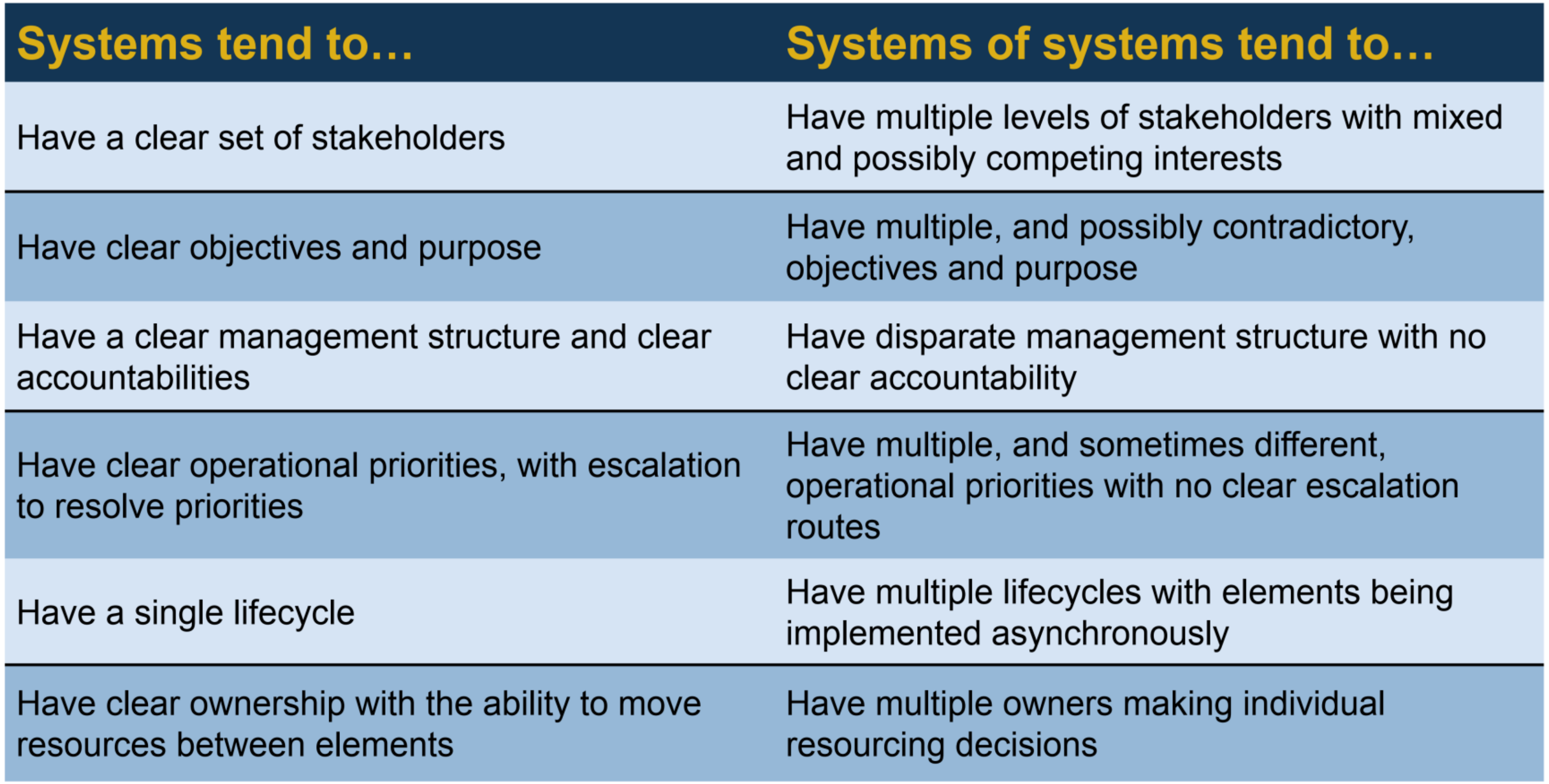
15:45 Exchange and summary

16:30 Finish

TECOSA

System of Systems

A System of Systems (SoS) is a collection of independent constituent systems, that collaborate to produce unique capabilities that they cannot produce alone.



Systems tend to…	Systems of systems tend to…
Have a clear set of stakeholders	Have multiple levels of stakeholders with mixed and possibly competing interests
Have clear objectives and purpose	Have multiple, and possibly contradictory, objectives and purpose
Have a clear management structure and clear accountabilities	Have disparate management structure with no clear accountability
Have clear operational priorities, with escalation to resolve priorities	Have multiple, and sometimes different, operational priorities with no clear escalation routes
Have a single lifecycle	Have multiple lifecycles with elements being implemented asynchronously
Have clear ownership with the ability to move resources between elements	Have multiple owners making individual resourcing decisions

Source: INCOSE Systems of Systems Primer INCOSE-TP-2018-003-01.0

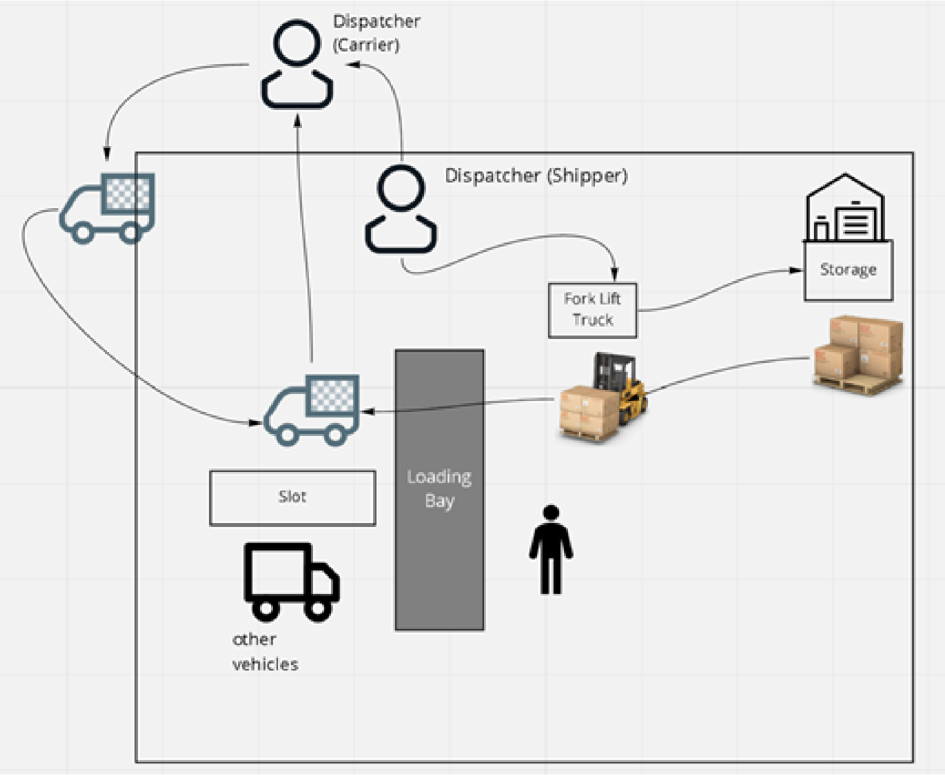
Cases

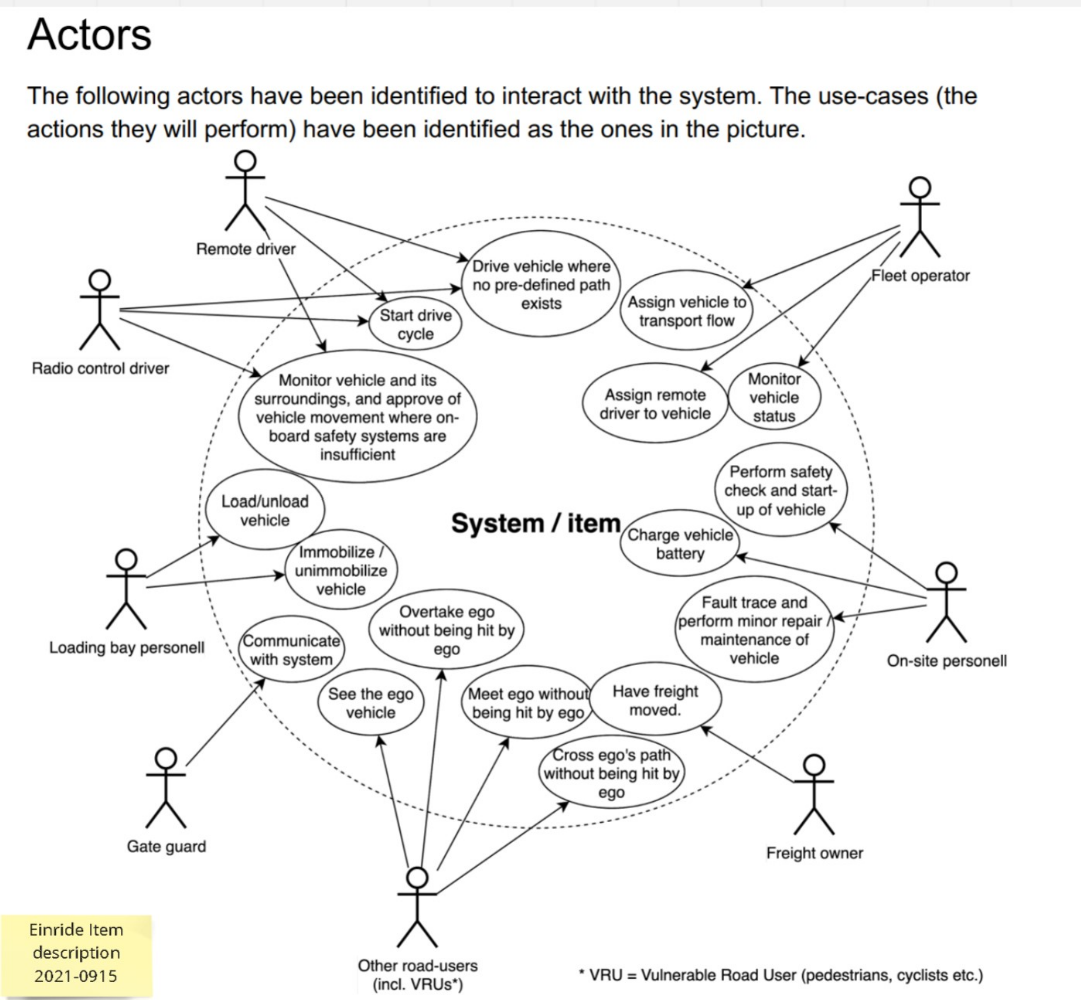
Einride loading/unloading

Platooning

Use case - Einride

Loading/Unloading at Terminal





Actors

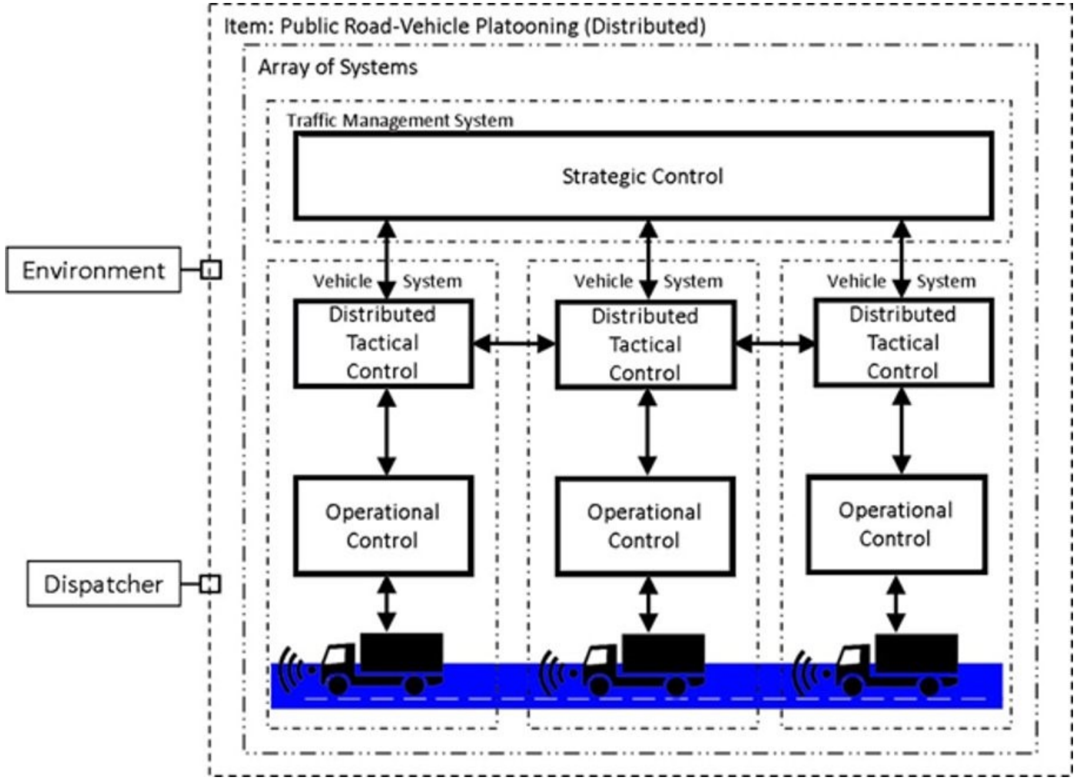
The following actors have been identified to interact with the system. The use-cases (the actions they will perform) have been identified as the ones in the picture.

Remote driver
Fleet operator
Radio control driver
Drive vehicle where no pre-defined path exists
Start drive cycle
Assign vehicle to transport flow
Monitor vehicle and its surroundings, and approve of vehicle movement where on-board safety systems are insufficient
Assign remote driver to vehicle
Monitor vehicle status
Perform safety check and start-up of vehicle
Load/unload vehicle
System / item
Charge vehicle battery
Immobilize / unimmobilize vehicle
Loading bay personell
Fault trace and perform minor repair / maintenance of vehicle
On-site personell
Overtake ego without being hit by ego
Communicate with system
See the ego vehicle
Meet ego without being hit by ego
Have freight moved.
Cross ego's path without being hit by ego
Gate guard
Freight owner
Other road-users (incl. VRUs*)

* VRU = Vulnerable Road User (pedestrians, cyclists etc.)

Einride Item
description
2021-0915

Use Case - Platooning


Item: Public Road-Vehicle Platooning (Distributed)
Array of Systems
Traffic Management System
Strategic Control
Vehicle System
Distributed Tactical Control
Operational Control
Vehicle System
Distributed Tactical Control
Operational Control
Vehicle System
Distributed Tactical Control
Operational Control
Environment
Dispatcher

Agenda Nov 23

13:30 Introduction to MBRASA, TECoSA, research idea

13:35 Use case presentation

13:45 The Approach

- Safety analysis moving into systems of systems
- System models supporting safety analysis
- Method approach

14:45 Workshop (including break)

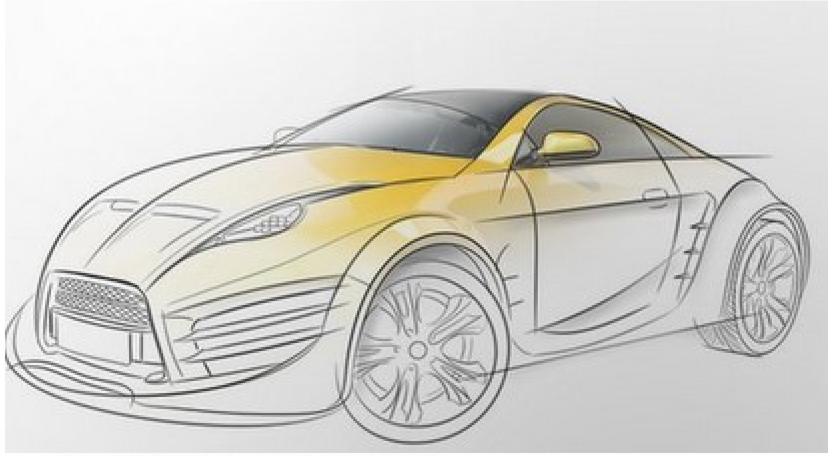
- Workshop set-up
- Group Discussions

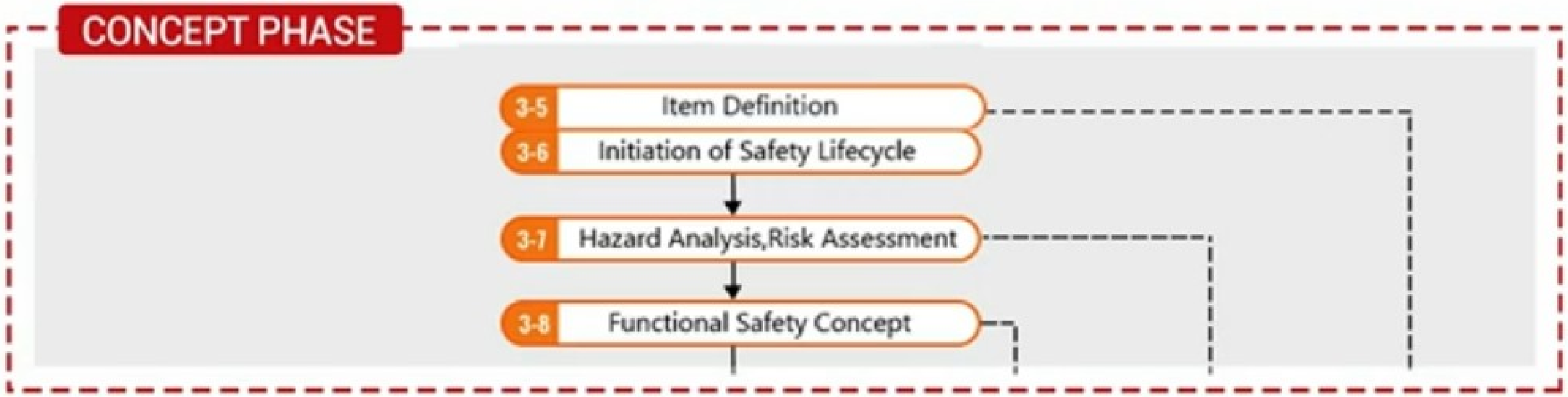
15:45 Exchange and summary

16:30 Finish

TECOSA

Hazard analysis and risk assessment





CONCEPT PHASE

3-5 Item Definition

3-6 Initiation of Safety Lifecycle

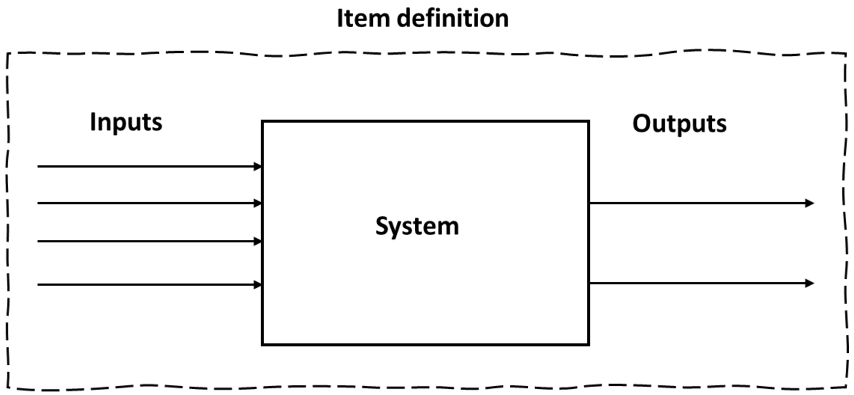
3-7 Hazard Analysis,Risk Assessment

3-8 Functional Safety Concept

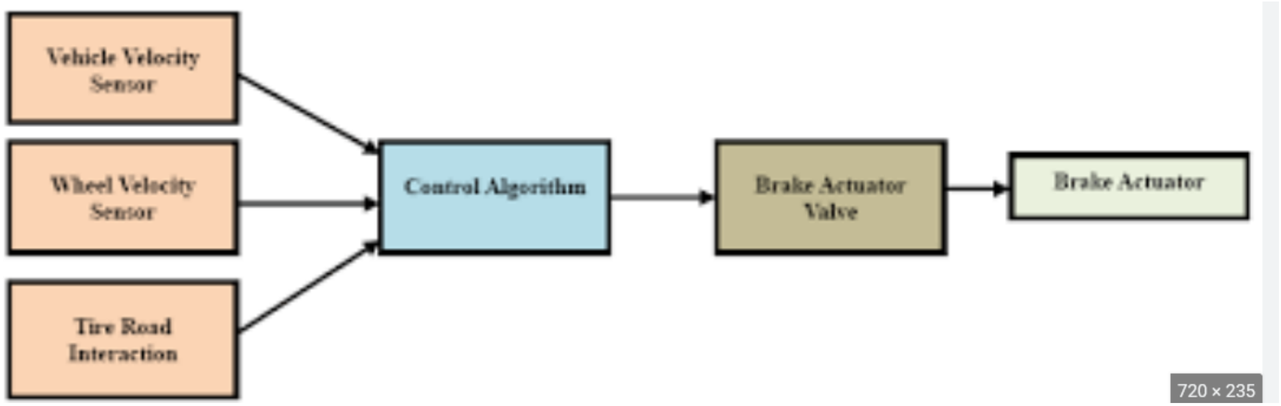
ISO 26262

Item

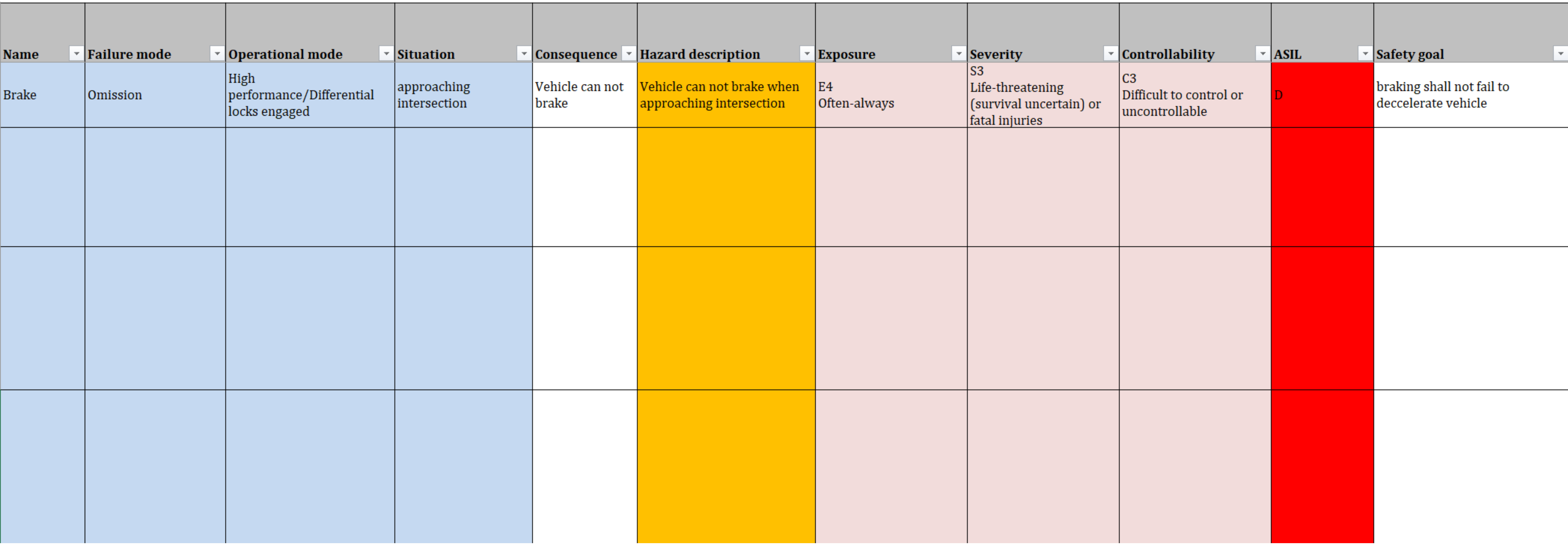
- Input, logic, output
- Model to define scope and function



- Example, electronic braking system



Hazard Analysis and Risk Assessment, HARA

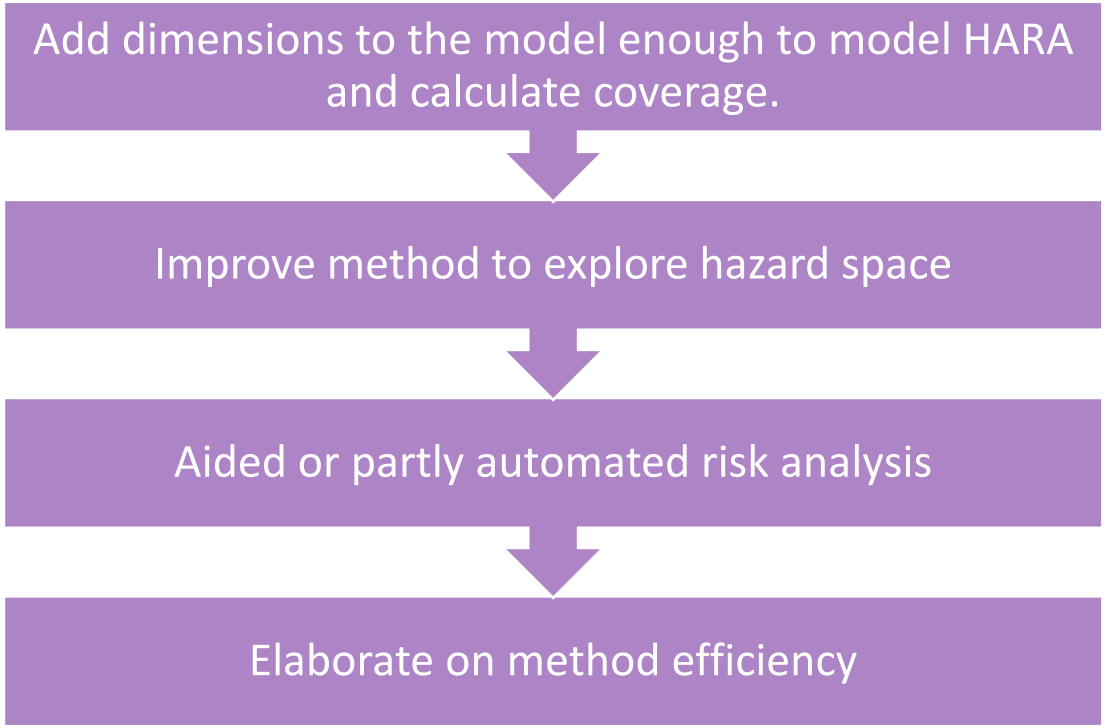


Name	Failure mode	Operational mode	Situation	Consequence	Hazard description	Exposure	Severity	Controllability	ASIL	Safety goal
Brake	Omission	High performance/Differential locks engaged	approaching intersection	Vehicle can not brake	Vehicle can not brake when approaching intersection	E4 Often-always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

Problem description

- SoS complexity
  - HARA Search space large
- SoS Managerial independence
  - Development and change across organizations
- SoS operational independence
  - User information about SoS doings
- SoS emerging behavior
  - Hard to foresee

HARA for SoS, The Vision



Add dimensions to the model enough to model HARA and calculate coverage.

Improve method to explore hazard space

Aided or partly automated risk analysis

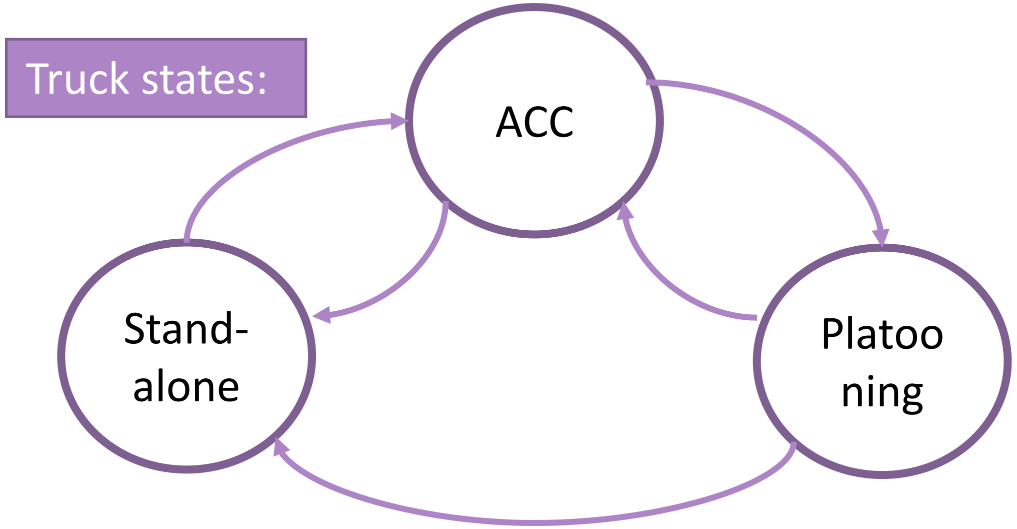
Elaborate on method efficiency

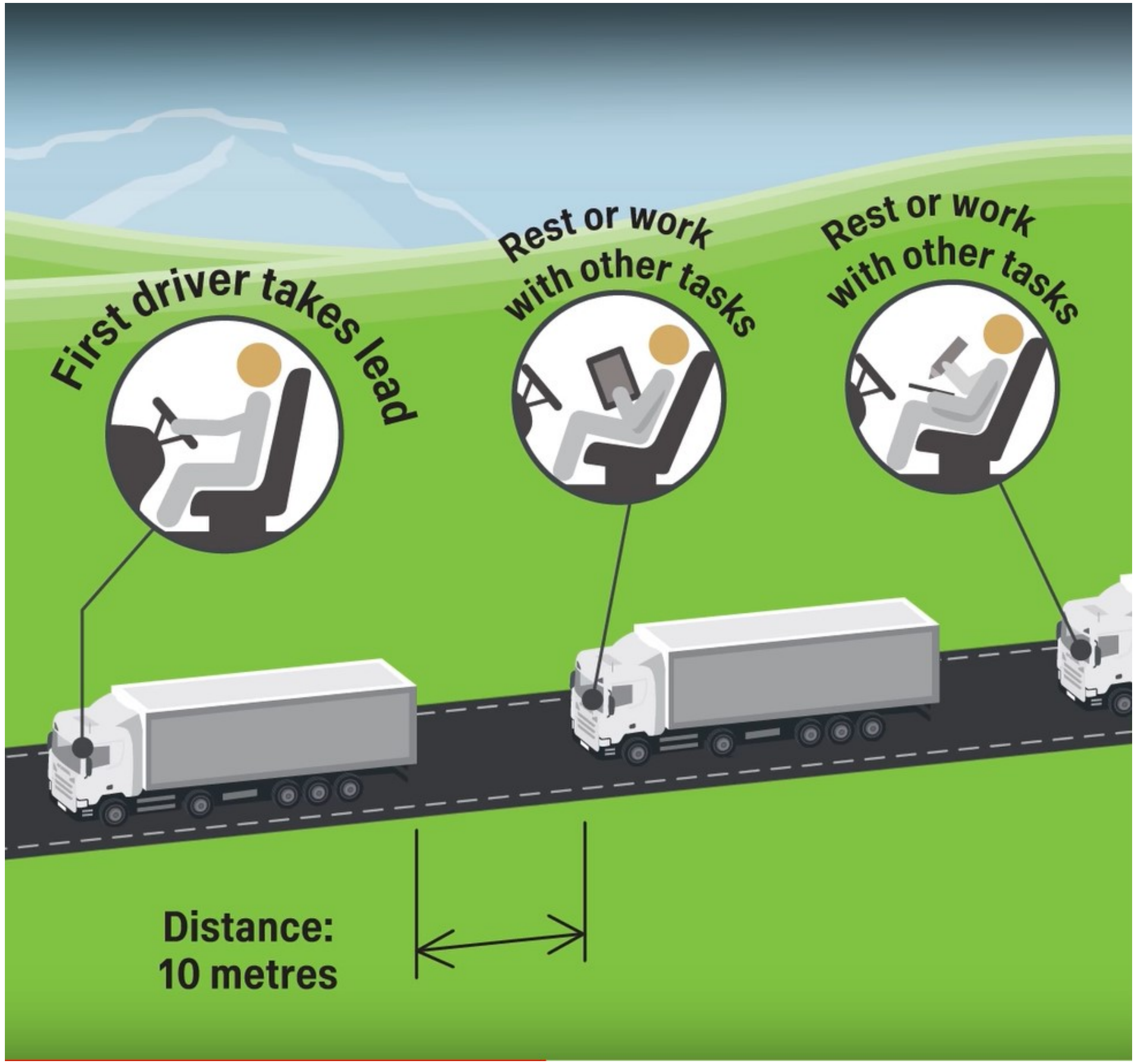
Wanted:
Better exploration of hazard space, Reuse of items, Reuse of HARA Results, structured change of existing items

Description of platooning example

- Drivers in trucks
- X number of trucks
- Entering platooning procedure:
  - Joining behind
  - Truck is in ACC mode, auto brake on
  - Agree to go to platooning
  - Auto brake disabled
  - Distance is shortened
- Following leader, dependent on wireless signal

Truck states:

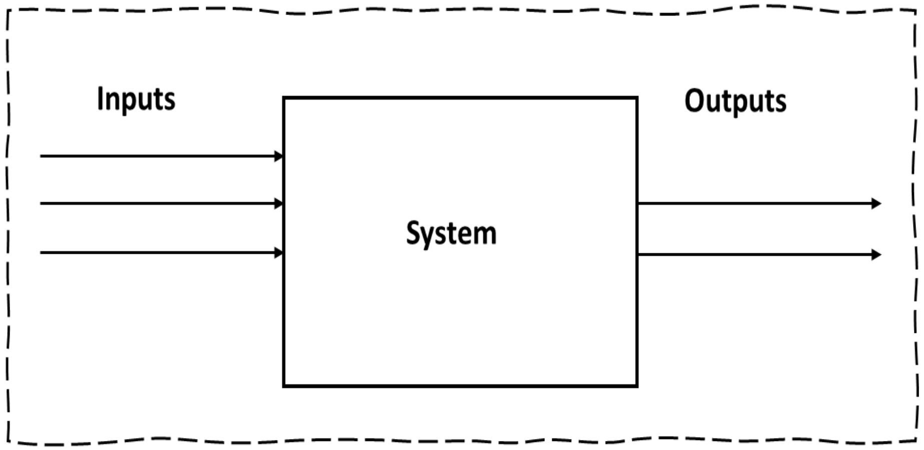




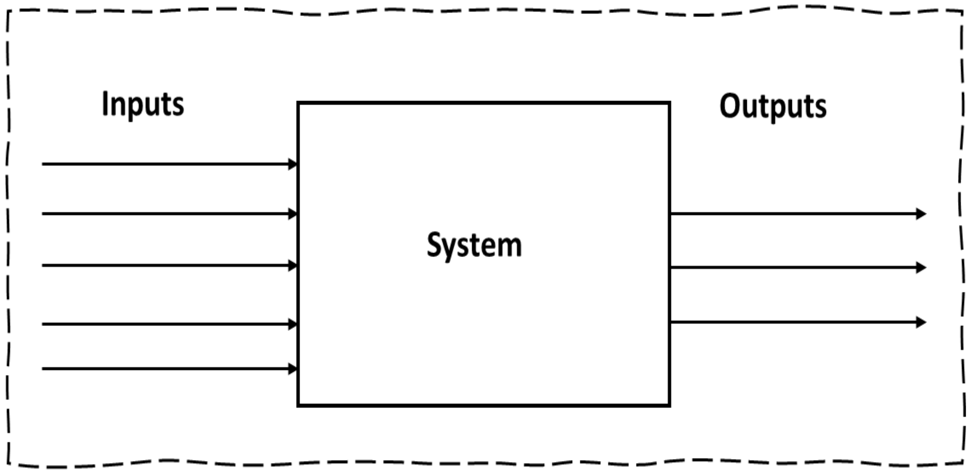
Picture: Scania youtube channel, 2018

Existing items in a truck

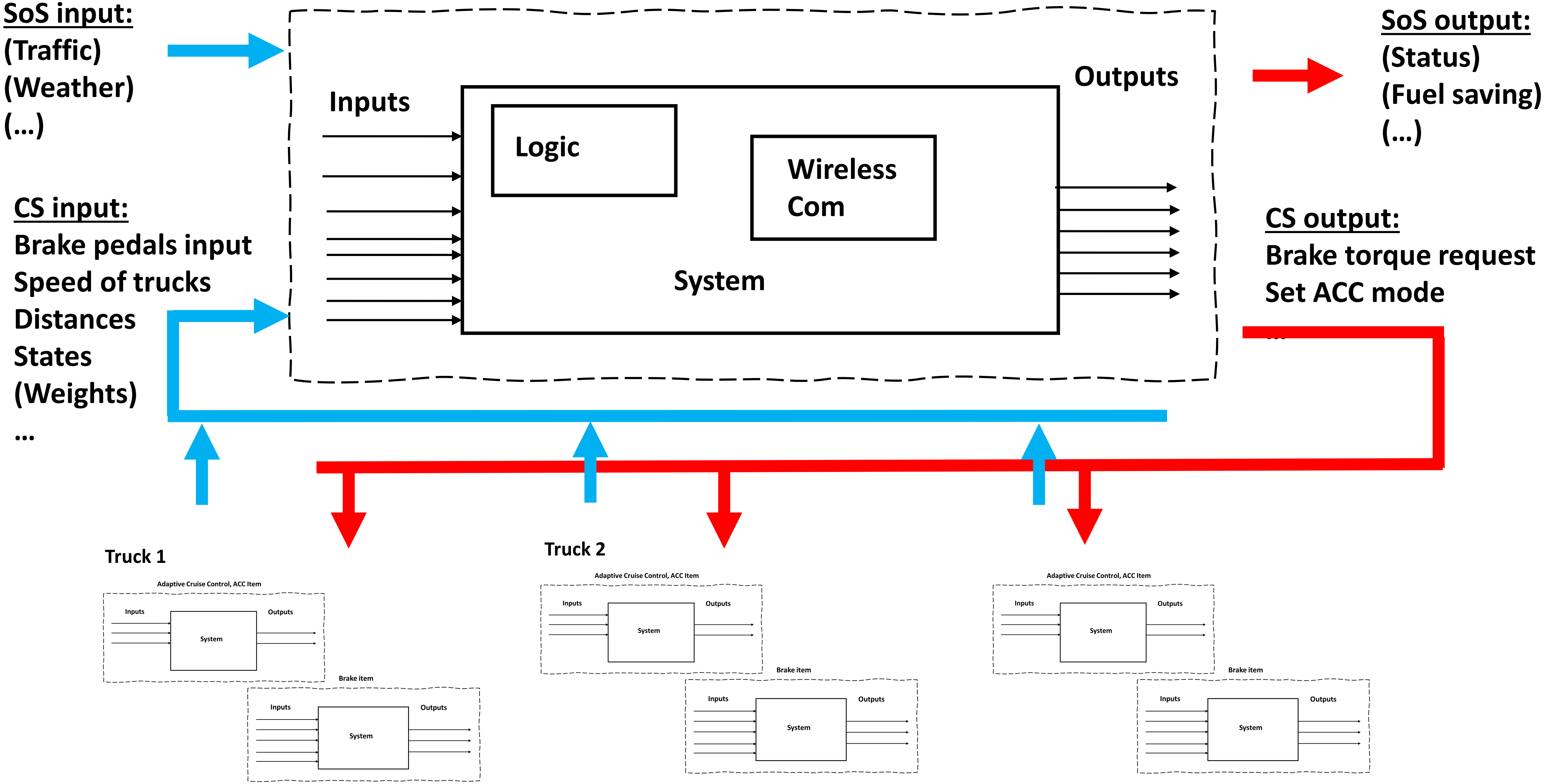
Adaptive Cruise Control, ACC Item



Brake item



Platoon Brake Item



SoS input:
(Traffic)
(Weather)
(…)

CS input:
Brake pedals input
Speed of trucks
Distances
States
(Weights)
…

Inputs

Logic

Wireless Com

System

Outputs

SoS output:
(Status)
(Fuel saving)
(…)

CS output:
Brake torque request
Set ACC mode
…

Truck 1

Adaptive Cruise Control, ACC Item
Inputs
System
Outputs

Brake item
Inputs
System
Outputs

Truck 2

Adaptive Cruise Control, ACC Item
Inputs
System
Outputs

Brake item
Inputs
System
Outputs

Adaptive Cruise Control, ACC Item
Inputs
System
Outputs

Brake item
Inputs
System
Outputs

HARA, FTA, Safety concept

✓ Identify delta of items

Explore added hazards of items

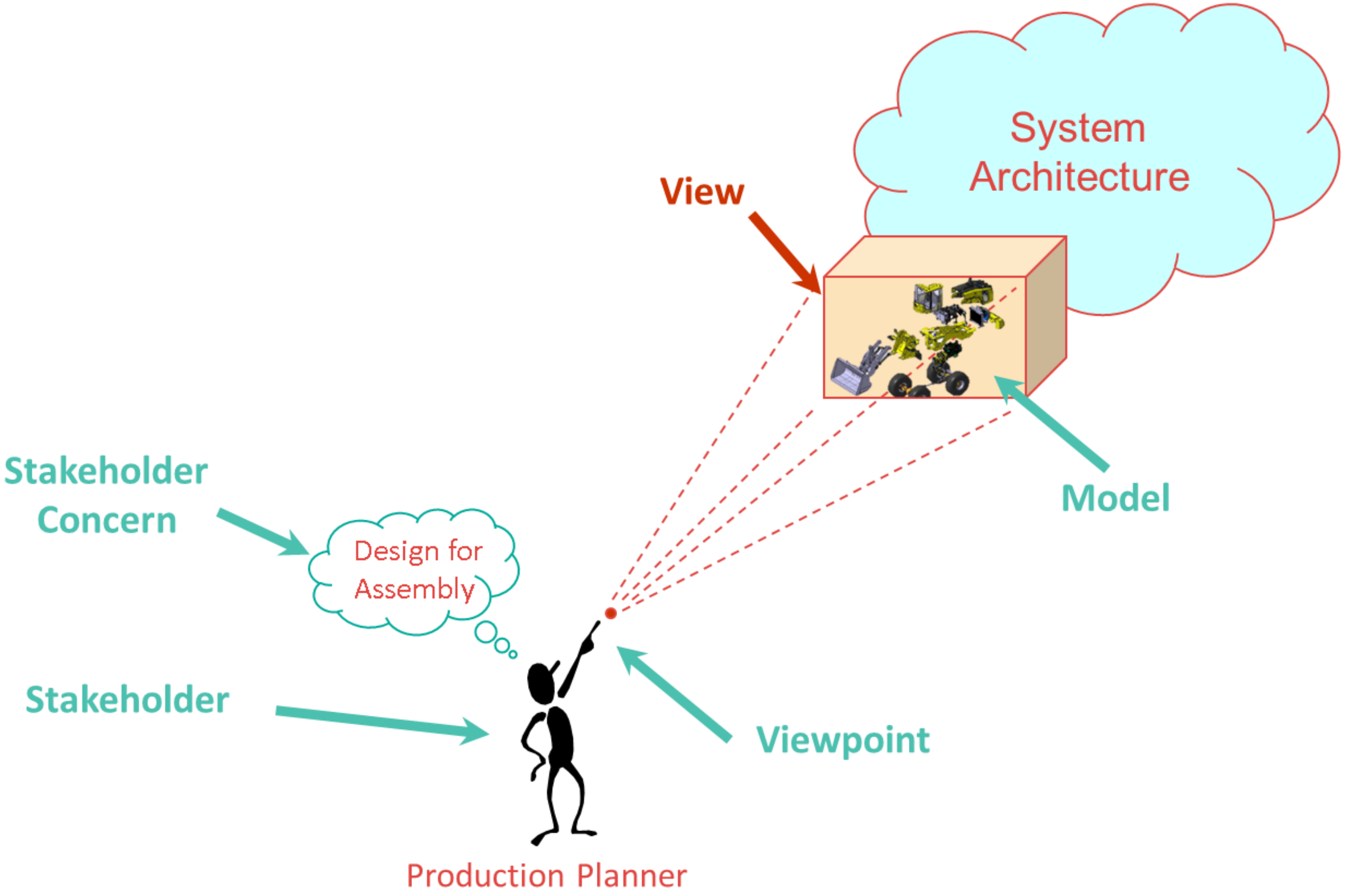
⚠ Explore hazards for SoS

Model

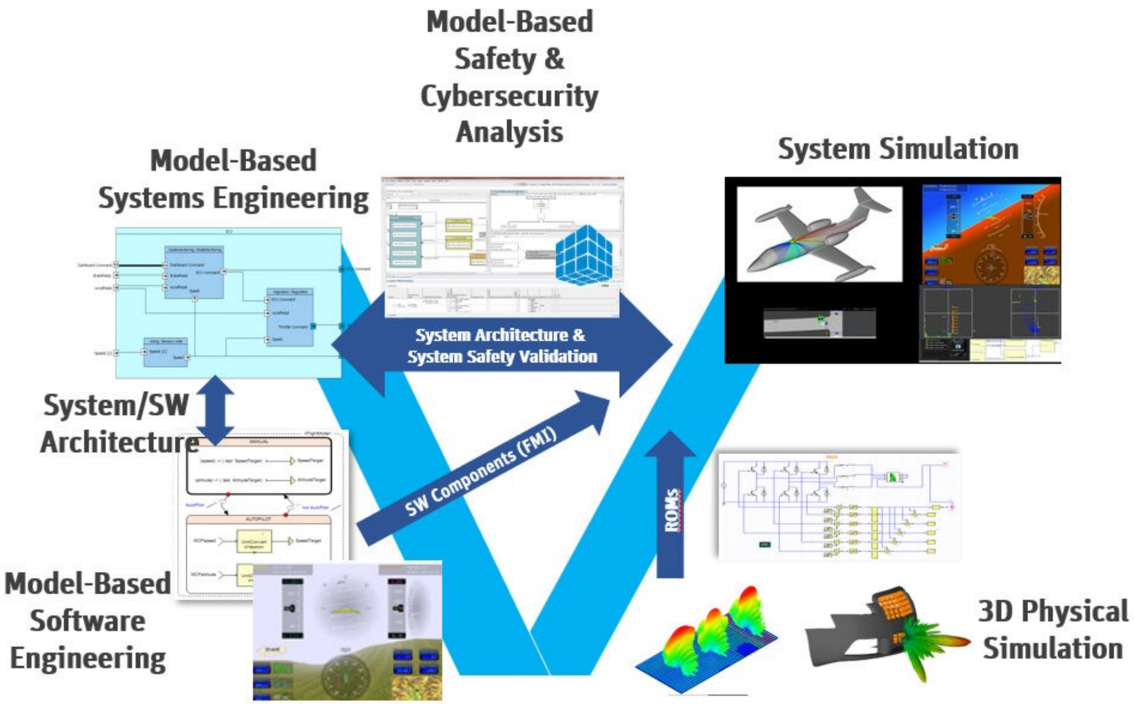
- An abstraction or representation of a system, entity, phenomenon, or process of interest.

- Uses of models:
  - Communication
  - Understanding
  - Analysis

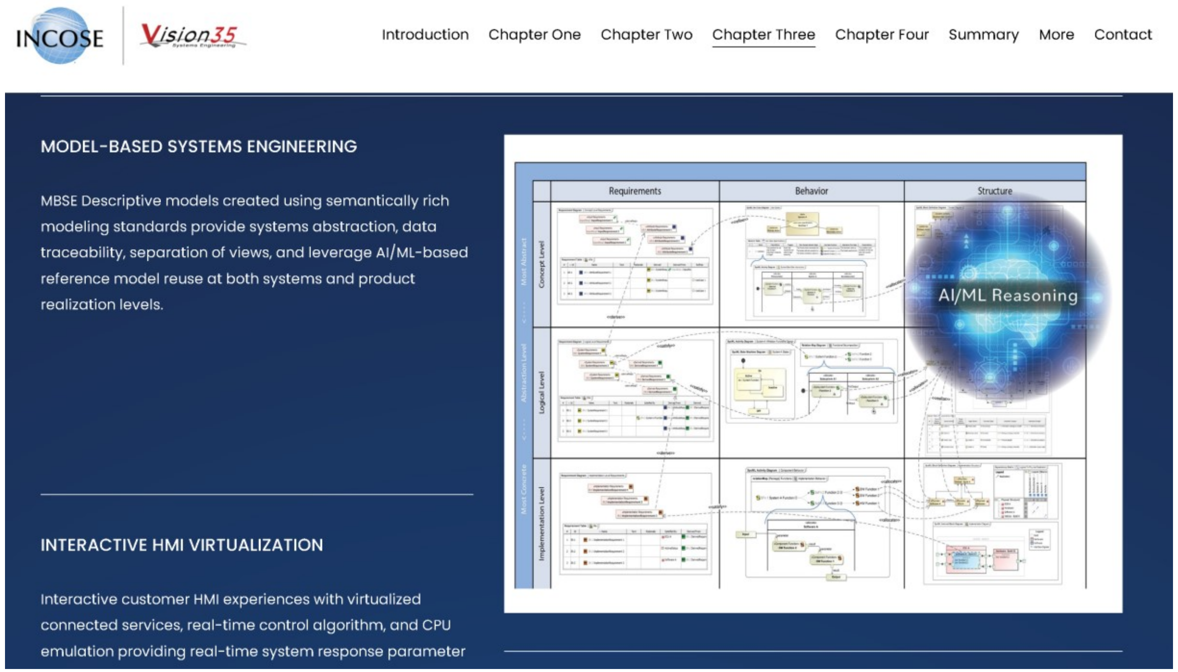
- Responds to a need:
  - WHAT
  - for WHOM
  - And HOW



Model-Based (Systems) Engineering


Model-Based Safety & Cybersecurity Analysis
Model-Based Systems Engineering
System Simulation
System Architecture & System Safety Validation
System/SW Architecture
SW Components (FMI)
ROMs
Model-Based Software Engineering
3D Physical Simulation

https://digitallabs.edrmedeso.com/events/webinar-functional-safety



MODEL-BASED SYSTEMS ENGINEERING

MBSE Descriptive models created using semantically rich modeling standards provide systems abstraction, data traceability, separation of views, and leverage AI/ML-based reference model reuse at both systems and product realization levels.

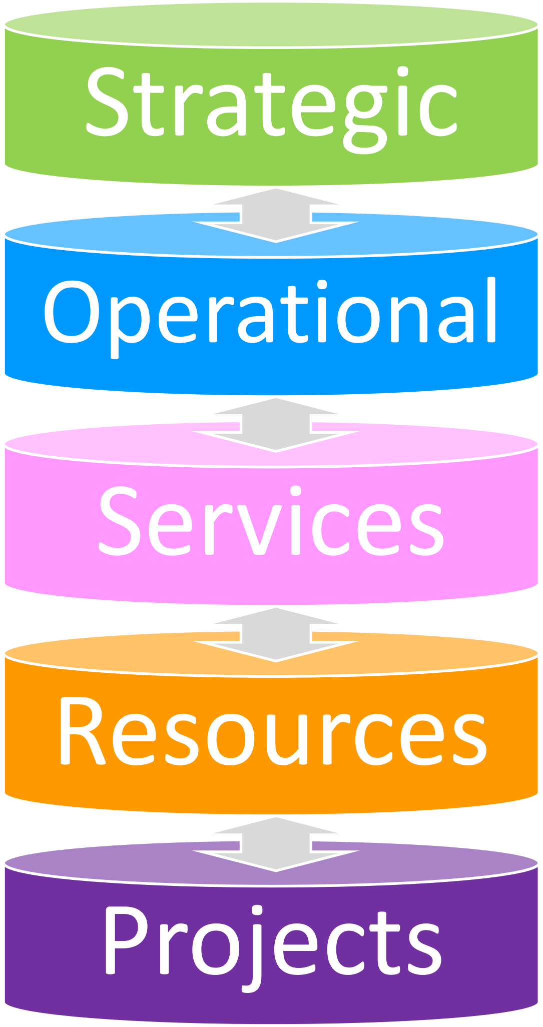
INTERACTIVE HMI VIRTUALIZATION

Interactive customer HMI experiences with virtualized connected services, real-time control algorithm, and CPU emulation providing real-time system response parameter

International Council on Systems Engineering (INCOSE) Systems Engineering Vision 2035
https://violin-strawberry-9kms.squarespace.com/

Enterprise architecture framework

Allows model to be created that deal not only with software or design but with concerns of an enterprise as a whole.



Strategic

Enterprise goals and capabilities (to meet market needs and stakeholder requirements)

Operational

Describing the environment and how you will operate your enterprise.

Services

The Services that can be called upon to carry out operational activities or capabilities.

Resources

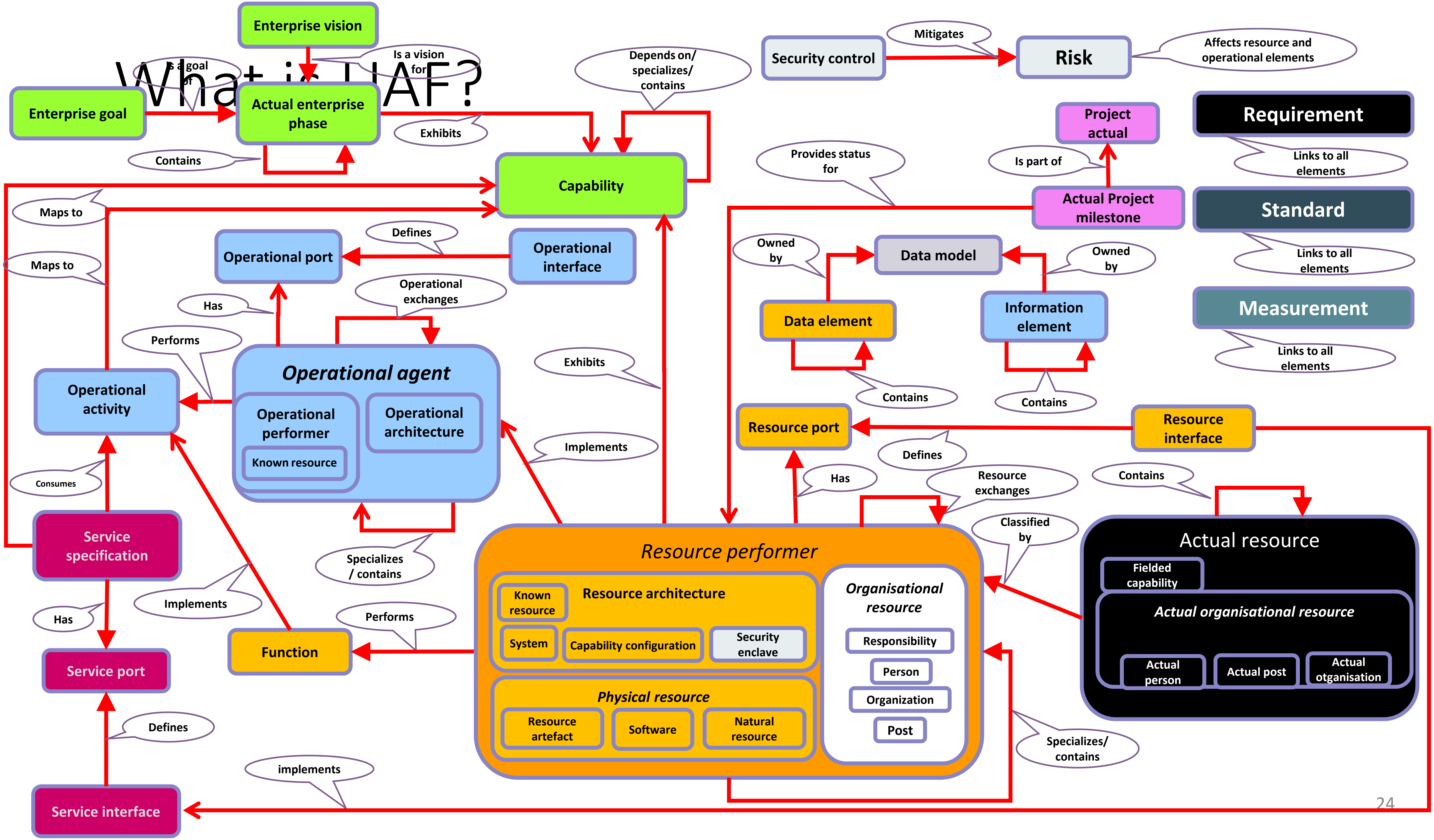
The actual resources and their configurations that you will need to carry out activities.

Projects

Describes the Projects, their relationships and how they contribute to establish capabilities.

Adapted from Unified Architecture Framework (UAF)
https://www.omg.org/uaf/index.htm

What is UAF?



Enterprise vision
Is a vision for
Enterprise goal
Is a goal of
Actual enterprise phase
Contains
Exhibits
Depends on/ specializes/ contains
Capability
Maps to
Maps to
Operational port
Defines
Operational interface
Has
Operational exchanges
Performs
Operational agent
Operational performer
Operational architecture
Known resource
Operational activity
Exhibits
Implements
Consumes
Service specification
Implements
Has
Service port
Defines
Service interface
implements
Function
Performs
Specializes / contains
Security control
Mitigates
Risk
Affects resource and operational elements
Project actual
Is part of
Actual Project milestone
Provides status for
Requirement
Links to all elements
Standard
Links to all elements
Measurement
Links to all elements
Owned by
Data model
Owned by
Data element
Information element
Contains
Contains
Resource port
Resource interface
Defines
Has
Resource exchanges
Contains
Classified by
Resource performer
Known resource
Resource architecture
System
Capability configuration
Security enclave
Physical resource
Resource artefact
Software
Natural resource
Organisational resource
Responsibility
Person
Organization
Post
Actual resource
Fielded capability
Actual organisational resource
Actual person
Actual post
Actual otganisation
Specializes/ contains

Electric Site Model

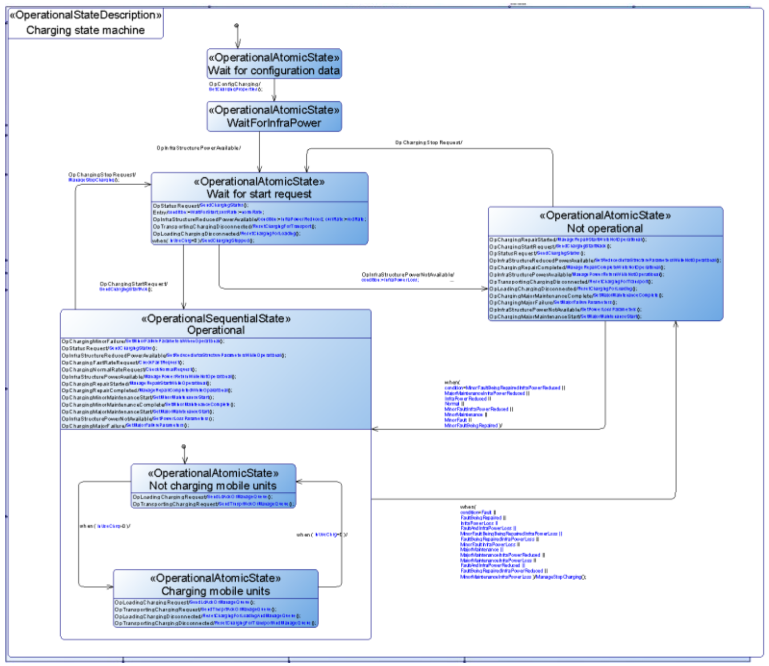
CO_2 reduction?

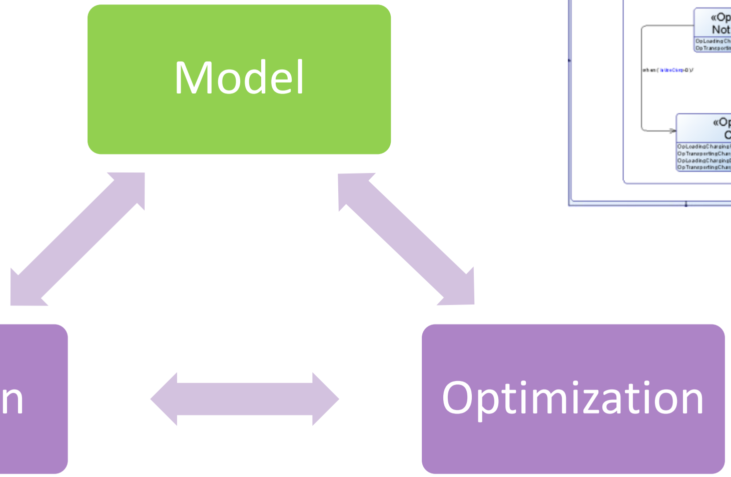
TCO reduction?

ELECTRIC SITE – a test stone quarry site with electrical, autonomous machines

THESIS COMPOSITION

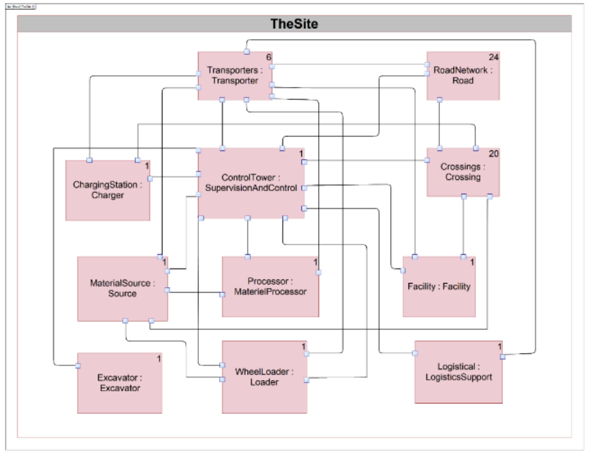
- UAF Architecture
- Behaviour, requirements
- State machines



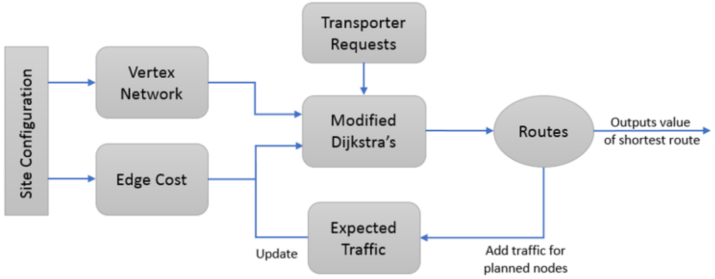


- Production
- Traffic flow
- Critical scenarios

- Scheduling
- Routing

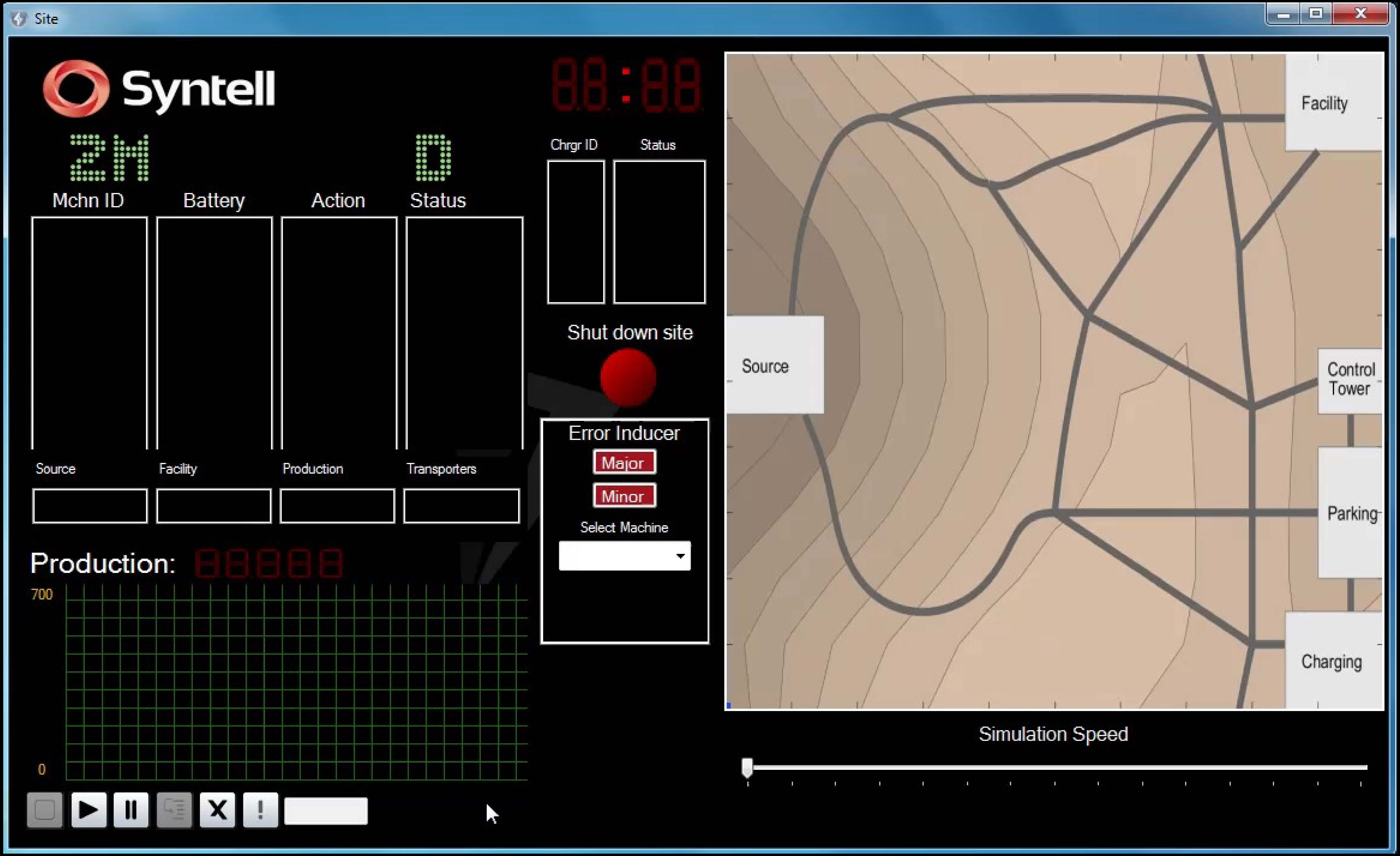


TheSite
Transporters : Transporter
6
RoadNetwork : Road
24
ChargingStation : Charger
1
ControlTower : SupervisionAndControl
1
Crossings : Crossing
20
MaterialSource : Source
1
Processor : MaterielProcessor
1
Facility : Facility
1
Excavator : Excavator
1
WheelLoader : Loader
1
Logistical : LogisticsSupport
1



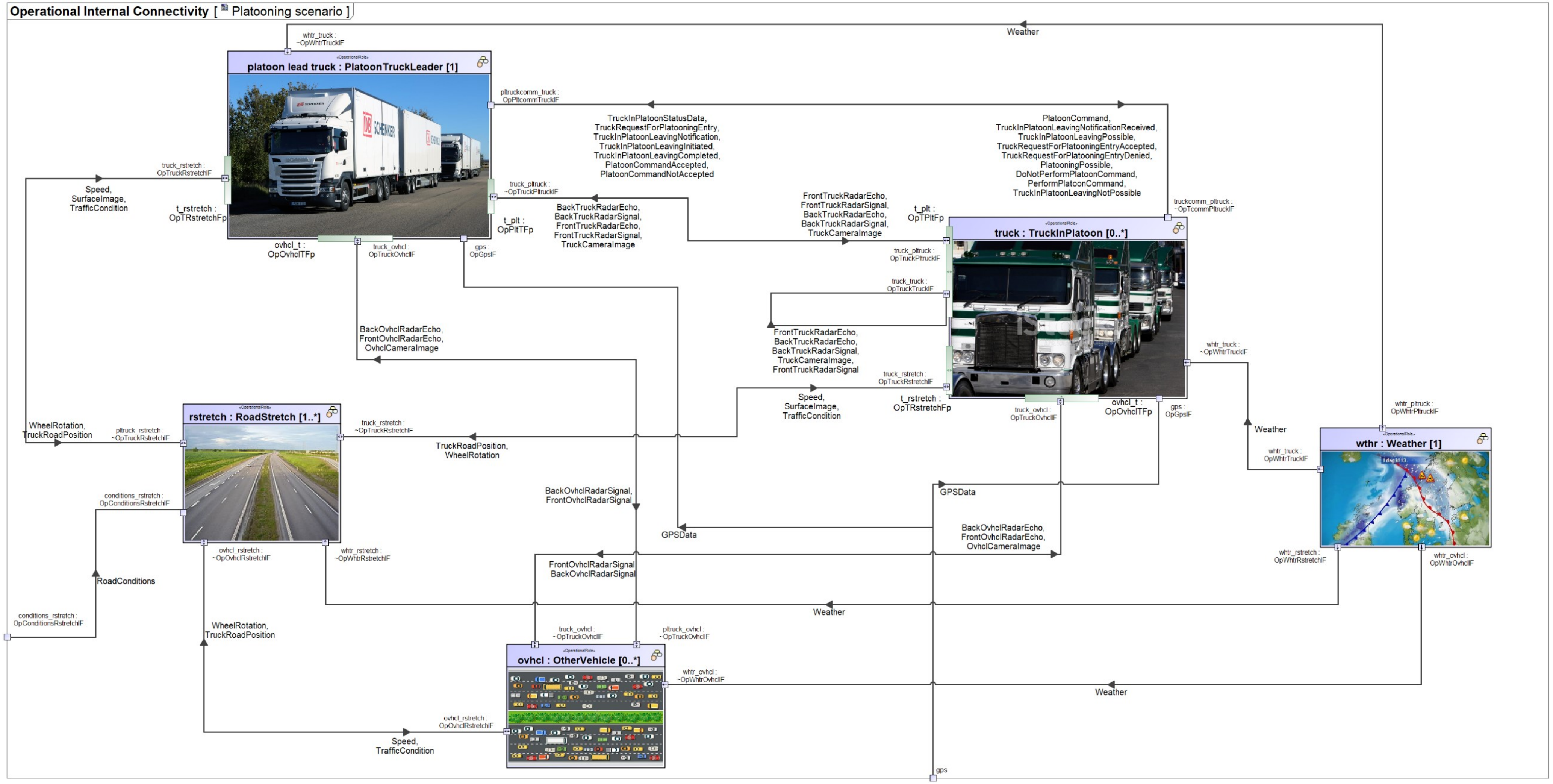
$$C = ArrivalTime + w \cdot Traffic$$

w – a *weight* scalar to handle congestion


Site
Syntell
88:88
2M
0
Mchn ID
Battery
Action
Status
Chrgr ID
Status
Shut down site
Source
Facility
Production
Transporters
Error Inducer
Major
Minor
Select Machine
Production: 88888
700
0
Facility
Source
Control Tower
Parking
Charging
Simulation Speed

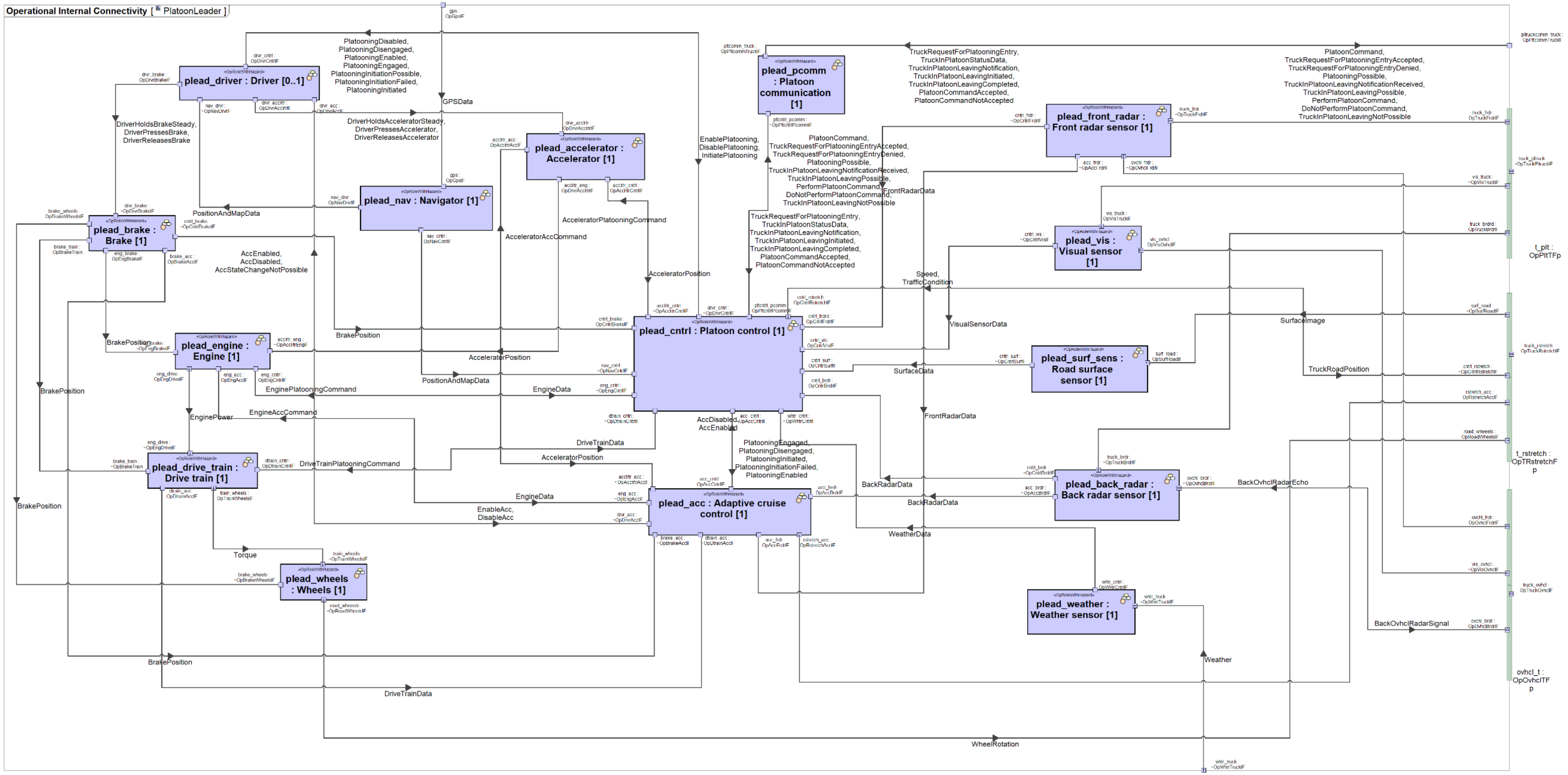
Logical Model of Truck, Platoon & Environment

Shows the context (“ODD”) in which the SoS is operated

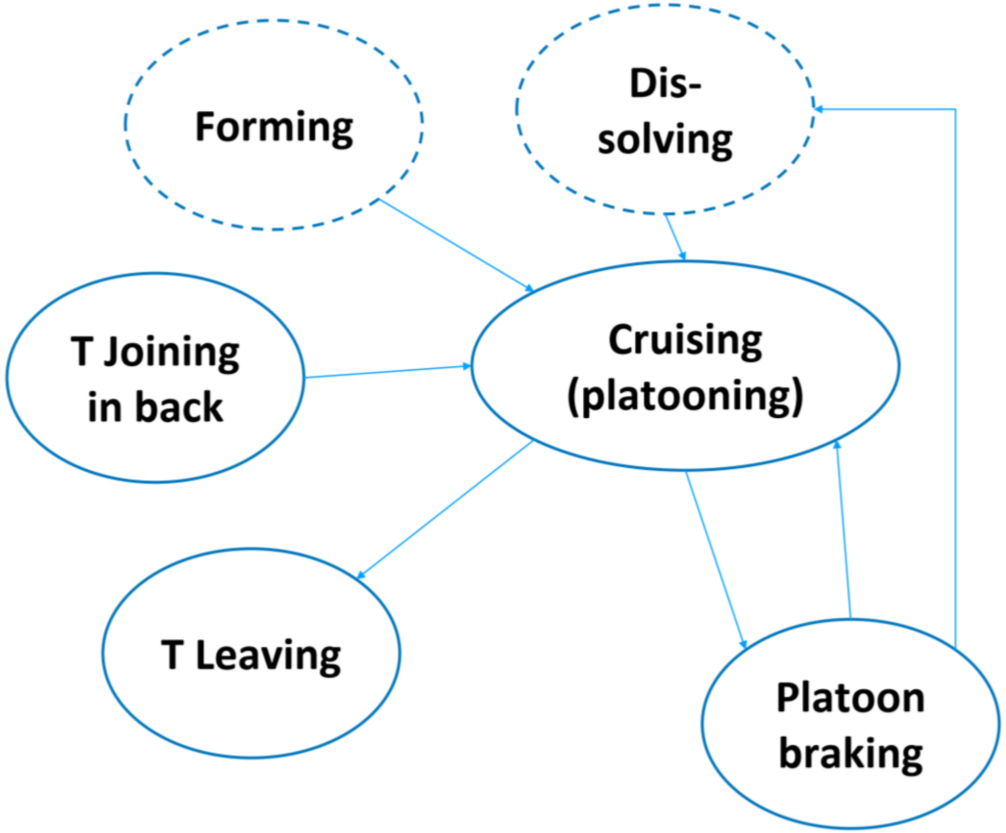

Operational Internal Connectivity [Platooning scenario]
Weather
whtr_truck : ~OpWhtrTruckIF
«OperationalRole»
platoon lead truck : PlatoonTruckLeader [1]
pltruckcomm_truck : OpPltcommTruckIF
TruckInPlatoonStatusData, TruckRequestForPlatooningEntry, TruckInPlatoonLeavingNotification, TruckInPlatoonLeavingInitiated, TruckInPlatoonLeavingCompleted, PlatoonCommandAccepted, PlatoonCommandNotAccepted
PlatoonCommand, TruckInPlatoonLeavingNotificationReceived, TruckInPlatoonLeavingPossible, TruckRequestForPlatooningEntryAccepted, TruckRequestForPlatooningEntryDenied, PlatooningPossible, DoNotPerformPlatoonCommand, PerformPlatoonCommand, TruckInPlatoonLeavingNotPossible
truck_rstretch : OpTruckRstretchIF
Speed, SurfaceImage, TrafficCondition
t_rstretch : OpTRstretchFp
truck_pltruck : ~OpTruckPltruckIF
t_plt : OpPltTFp
BackTruckRadarEcho, BackTruckRadarSignal, FrontTruckRadarEcho, FrontTruckRadarSignal, TruckCameraImage
FrontTruckRadarEcho, FrontTruckRadarSignal, BackTruckRadarEcho, BackTruckRadarSignal, TruckCameraImage
t_plt : OpTPltFp
truckcomm_pltruck : ~OpTcommPltruckIF
«OperationalRole»
truck : TruckInPlatoon [0..*]
ovhcl_t : OpOvhclTFp
truck_ovhcl : OpTruckOvhclIF
gps : OpGpsIF
truck_pltruck : OpTruckPltruckIF
truck_truck : OpTruckTruckIF
BackOvhclRadarEcho, FrontOvhclRadarEcho, OvhclCameraImage
FrontTruckRadarEcho, BackTruckRadarEcho, BackTruckRadarSignal, TruckCameraImage, FrontTruckRadarSignal
truck_rstretch : OpTruckRstretchIF
Speed, SurfaceImage, TrafficCondition
t_rstretch : OpTRstretchFp
truck_ovhcl : OpTruckOvhclIF
ovhcl_t : OpOvhclTFp
gps : OpGpsIF
whtr_truck : ~OpWhtrTruckIF
Weather
whtr_truck : OpWhtrTruckIF
whtr_pltruck : OpWhtrPltruckIF
«OperationalRole»
wthr : Weather [1]
WheelRotation, TruckRoadPosition
pltruck_rstretch : ~OpTruckRstretchIF
«OperationalRole»
rstretch : RoadStretch [1..*]
truck_rstretch : ~OpTruckRstretchIF
TruckRoadPosition, WheelRotation
conditions_rstretch : OpConditionsRstretchIF
BackOvhclRadarSignal, FrontOvhclRadarSignal
GPSData
GPSData
BackOvhclRadarEcho, FrontOvhclRadarEcho, OvhclCameraImage
ovhcl_rstretch : ~OpOvhclRstretchIF
whtr_rstretch : ~OpWhtrRstretchIF
FrontOvhclRadarSignal BackOvhclRadarSignal
RoadConditions
whtr_rstretch : OpWhtrRstretchIF
whtr_ovhcl : OpWhtrOvhclIF
Weather
conditions_rstretch : OpConditionsRstretchIF
WheelRotation, TruckRoadPosition
truck_ovhcl : ~OpTruckOvhclIF
pltruck_ovhcl : ~OpTruckOvhclIF
«OperationalRole»
ovhcl : OtherVehicle [0..*]
whtr_ovhcl : ~OpWhtrOvhclIF
Weather
ovhcl_rstretch : OpOvhclRstretchIF
Speed, TrafficCondition
gps

Logical Breakdown of a Truck

Shows the logical components of a truck prepared for platooning


Operational Internal Connectivity [PlatoonLeader]
«OpRoleWithHazard»
plead_driver : Driver [0..1]
plead_pcomm : Platoon communication [1]
plead_front_radar : Front radar sensor [1]
plead_accelerator : Accelerator [1]
plead_nav : Navigator [1]
plead_brake : Brake [1]
plead_vis : Visual sensor [1]
plead_cntrl : Platoon control [1]
plead_engine : Engine [1]
plead_surf_sens : Road surface sensor [1]
plead_drive_train : Drive train [1]
plead_acc : Adaptive cruise control [1]
plead_back_radar : Back radar sensor [1]
plead_wheels : Wheels [1]
plead_weather : Weather sensor [1]
gps : OpGpsIF
drvr_cntrl : OpDrvrCntrlIF
drvr_brake : OpDrvrBrakeIF
nav_drvr : ~OpNavDrvrIF
drvr_acclrtr : OpDrvrAcclrtrIF
drvr_acc : OpDrvrAccIF
PlatooningDisabled, PlatooningDisengaged, PlatooningEnabled, PlatooningEngaged, PlatooningInitiationPossible, PlatooningInitiationFailed, PlatooningInitiated
GPSData
DriverHoldsBrakeSteady, DriverPressesBrake, DriverReleasesBrake
DriverHoldsAcceleratorSteady, DriverPressesAccelerator, DriverReleasesAccelerator
acclrtr_acc : OpAcclrtrAccIF
acclrtr_eng : OpDrvrAcclrtrIF
acclrtr_cntrl : OpAcclrtrCntrlIF
nav_drvr : OpNavDrvrIF
nav_cntrl : OpNavCntrlIF
PositionAndMapData
brake_wheels : OpBrakeWheelsIF
drvr_brake : ~OpDrvrBrakeIF
cntrl_brake : ~OpCntrlBrakeIF
brake_train : OpBrakeTrain
eng_brake : OpEngBrakeIF
brake_acc : OpBrakeAccIF
AccEnabled, AccDisabled, AccStateChangeNotPossible
AcceleratorPlatooningCommand
AcceleratorAccCommand
AcceleratorPosition
EnablePlatooning, DisablePlatooning, InitiatePlatooning
pltcomm_truck : OpPltcommTruckIF
pltcntrl_pcomm : ~OpPltcntrlPcommIF
TruckRequestForPlatooningEntry, TruckInPlatoonStatusData, TruckInPlatoonLeavingNotification, TruckInPlatoonLeavingInitiated, TruckInPlatoonLeavingCompleted, PlatoonCommandAccepted, PlatoonCommandNotAccepted
PlatoonCommand, TruckRequestForPlatooningEntryAccepted, TruckRequestForPlatooningEntryDenied, PlatooningPossible, TruckInPlatoonLeavingNotificationReceived, TruckInPlatoonLeavingPossible, PerformPlatoonCommand, DoNotPerformPlatoonCommand, TruckInPlatoonLeavingNotPossible
FrontRadarData
cntrl_frdr : ~OpCntrlFrdrIF
truck_frdr : ~OpTruckFrdrIF
acc_frdr : ~OpAccFrdrIF
ovchl_frdr : ~OpOvhclFrdrIF
pltruckcomm_truck : OpPltcommTruckIF
truck_frdr : OpTruckFrdrIF
truck_pltruck : ~OpTruckPltruckIF
vis_truck : ~OpVisTruckIF
vis_truck : OpVisTruckIF
cntrl_vis : ~OpCntrlVisIF
vis_ovhcl : OpVisOvhclIF
truck_brdrd : OpTruckBrdrIF
t_plt : OpPltTFp
Speed, TrafficCondition
VisualSensorData
SurfaceImage
surf_road : ~OpSurfRoadIF
truck_rstretch : OpTruckRstretchIF
acclrtr_cntrl : ~OpAcclrtrCntrlIF
drvr_cntrl : ~OpDrvrCntrlIF
pltcntrl_pcomm : OpPltcntrlPcommIF
cntrl_rstretch : OpCntrlRstretchIF
cntrl_frdrd : OpCntrlFrdrIF
cntrl_brake : OpCntrlBrakeIF
cntrl_vis : OpCntrlVisIF
cntrl_surf : OpCntrlSurfIF
cntrl_brdr : OpCntrlBrdrIF
nav_cntrl : ~OpNavCntrlIF
eng_cntrl : ~OpEngCntrlIF
BrakePosition
accltr_eng : ~OpAcclrtrEngIF
eng_brake : ~OpEngBrakeIF
eng_drive : OpEngDriveIF
eng_acc : OpEngAccIF
eng_cntrl : OpEngCntrlIF
EnginePlatooningCommand
EngineData
SurfaceData
cntrl_surf : ~OpCntrlSurfIF
surf_road : OpSurfRoadIF
TruckRoadPosition
cntrl_rstretch : ~OpCntrlRstretchIF
rstretch_acc : OpRstretchAccIF
road_wheeels : OpRoadWheelsIF
EnginePower
EngineAccCommand
dtrain_cntrl : ~OpDtrainCntrlIF
acc_cntrl : ~OpAccCntrlIF
whtr_cntrl : ~OpWhtrCntrlIF
AccDisabled, AccEnabled
DriveTrainData
PlatooningEngaged, PlatooningDisengaged, PlatooningInitiated, PlatooningInitiationFailed, PlatooningEnabled
t_rstretch : OpTRstretchFp
eng_drive : ~OpEngDriveIF
brake_train : ~OpBrakeTrain
dtrain_cntrl : OpDtrainCntrlIF
DriveTrainPlatooningCommand
acclrtr_acc : ~OpAcclrtrAccIF
acc_cntrl : OpAccCntrlIF
acc_brdr : OpAccBrdrIF
BackRadarData
truck_brdr : ~OpTruckBrdrIF
cntrl_brdr : ~OpCntrlBrdrIF
acc_brdr : ~OpAccBrdrIF
ovchl_brdr : ~OpOvhclBrdrIF
BackOvhclRadarEcho
dtrain_acc : OpDtrainAccIF
train_wheels : OpTrainWheelsIF
eng_acc : ~OpEngAccIF
drvr_acc : ~OpDrvrAccIF
EnableAcc, DisableAcc
brake_acc : ~OpBrakeAccIF
dtrain_acc : ~OpDtrainAccIF
acc_frdr : OpAccFrdrIF
rstretch_acc : OpRstretchAccIF
WeatherData
ovchl_frdr : OpOvhclFrdrIF
Torque
train_wheels : ~OpTrainWheelsIF
brake_wheels : ~OpBrakeWheelsIF
road_wheels : ~OpRoadWheelsIF
whtr_cntrl : OpWhtrCntrlIF
whtr_truck : ~OpWhtrTruckIF
vis_ovhcl : ~OpVisOvhclIF
truck_ovhcl : OpTruckOvhclIF
BackOvhclRadarSignal
ovchl_brdr : OpOvhclBrdrIF
Weather
ovhcl_t : OpOvhclTFp
WheelRotation

Scenarios w possible hazards

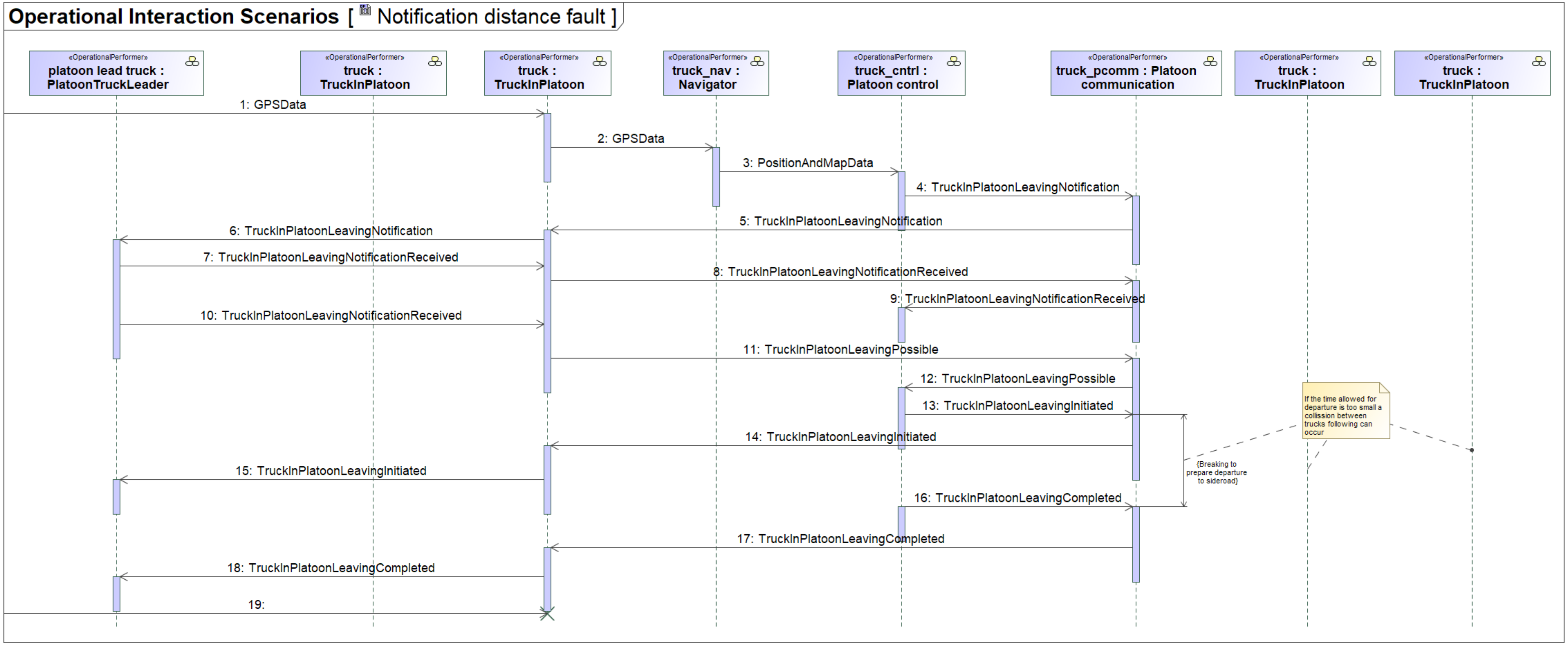


While being able to deal with:

- Traffic Restrictions (speed limit changes, queues, gradients)
- Parameter handling
- Gap handling
- Other Vehicle interaction handling
- Platoon length handling

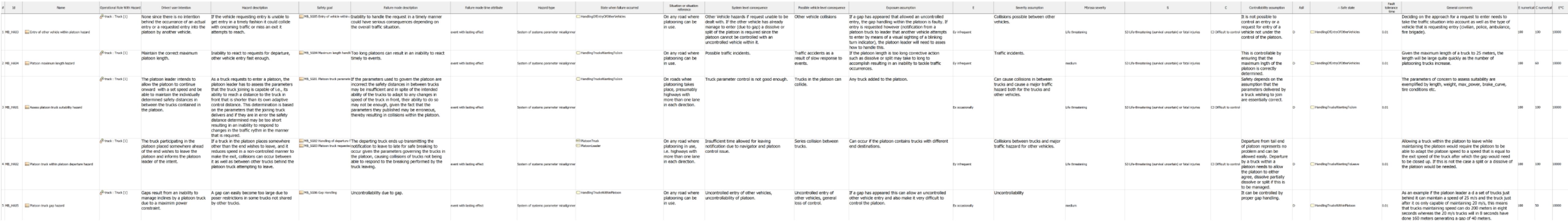
Truck Platooning Scenario

Shows a truck leaving the platoon, communicating with the others, speed control & platoon behavior

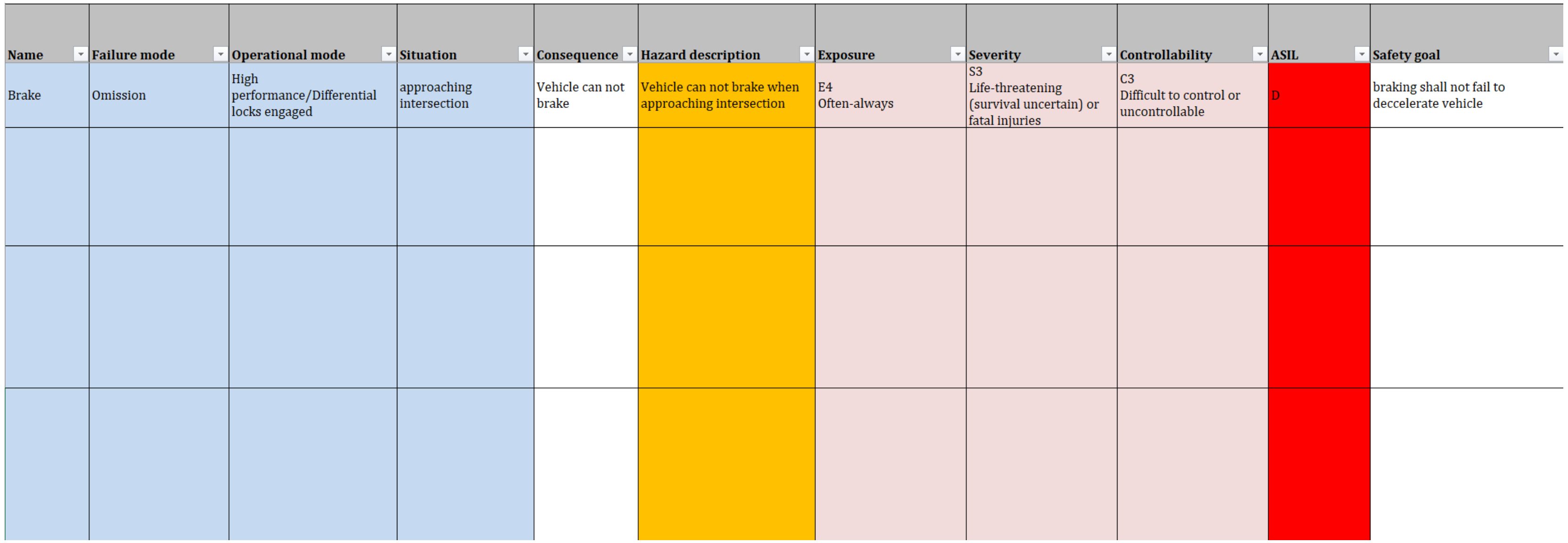

Operational Interaction Scenarios [Notification distance fault]
«OperationalPerformer» platoon lead truck : PlatoonTruckLeader
«OperationalPerformer» truck : TruckInPlatoon
«OperationalPerformer» truck : TruckInPlatoon
«OperationalPerformer» truck_nav : Navigator
«OperationalPerformer» truck_cntrl : Platoon control
«OperationalPerformer» truck_pcomm : Platoon communication
«OperationalPerformer» truck : TruckInPlatoon
«OperationalPerformer» truck : TruckInPlatoon
1: GPSData
2: GPSData
3: PositionAndMapData
4: TruckInPlatoonLeavingNotification
5: TruckInPlatoonLeavingNotification
6: TruckInPlatoonLeavingNotification
7: TruckInPlatoonLeavingNotificationReceived
8: TruckInPlatoonLeavingNotificationReceived
9: TruckInPlatoonLeavingNotificationReceived
10: TruckInPlatoonLeavingNotificationReceived
11: TruckInPlatoonLeavingPossible
12: TruckInPlatoonLeavingPossible
13: TruckInPlatoonLeavingInitiated
14: TruckInPlatoonLeavingInitiated
15: TruckInPlatoonLeavingInitiated
16: TruckInPlatoonLeavingCompleted
17: TruckInPlatoonLeavingCompleted
18: TruckInPlatoonLeavingCompleted
19:
{Breaking to prepare departure to sideroad}
If the time allowed for departure is too small a collission between trucks following can occur

Hazard Analysis Report

Compiles the information from the scenarios



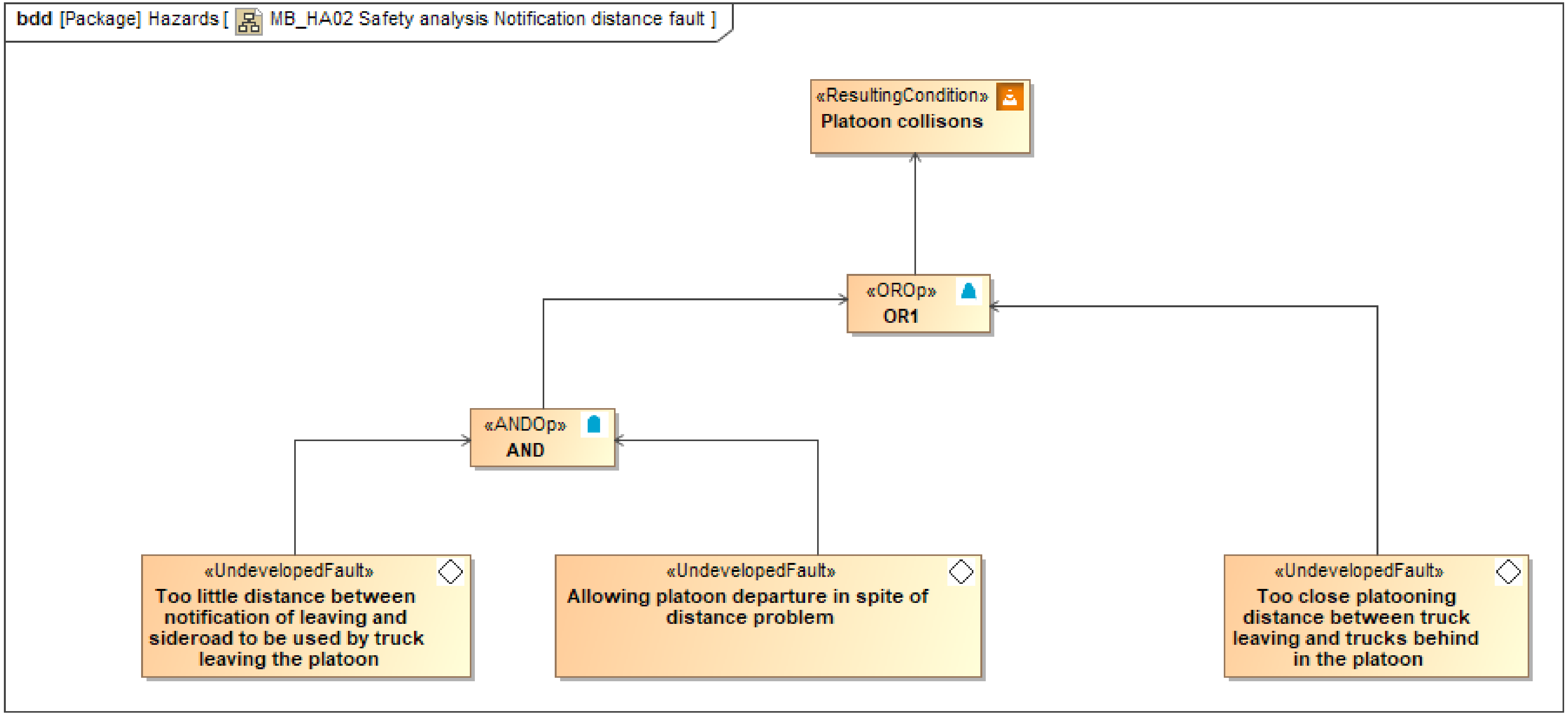
#	Id	Name	Operational Role With Hazard	Driver/ user intention	Hazard description	Safety goal	Failure mode description	Failure mode time attribute	Hazard type	State when failure occurred	Situation or situation reference	System level consequence	Possible vehicle level consequence	Exposure assumption	E	Severity assumption	Mbrasa severity	S	C	Controllability assumption	Asil	Safe state	Fault tolerance time	General comments	E numerical	C numerical	E*C
1	MB_HA03	Entry of other vehicle within platoon hazard	track : Truck [1]	None since there is no intention behind the occurrance of an actual entry or a requested entry into the platoon by another vehicle.	If the vehicle requesting entry is unable to get entry in a timely fashion it could collide with oncoming traffic or miss an exit it attempts to reach.	MB_SG05 Entry of vehicle within	Inability to handle the request in a timely manner could have serious consequences depending on the overall traffic situation.	event with lasting effect	System of systems parameter misalignmer	HandlingOfEntryOfOtherVehicles	On any road where platooning can be in use.	Other Vehicle hazards if request unable to be dealt with. If the other vehicle has already manage to enter (due to gap) a dissolve or split of the platoon is required since the platoon cannot be controlled with an uncontrolled vehicle within it.	Other vehicle collisions	If a gap has appeared that allowed an uncontrolled entry, the gap handling within the platoon is faulty. If entry is requested however (notification from a platoon truck to leader that another vehicle attempts to enter by means of a visual sighting of a blinking turn indicator), the platoon leader will need to asses how to handle this.	Ey infrequent	Collisions possible between other vehicles.	Life threatening	S3 Life-threatening (survival uncertain) or fatal injuries	C3 Difficult to control	It is not possible to control an entry or a request for entry of a vehicle not under the control of the platoon.	D	HandlingOfEntryOfOtherVehicles	0.01	Deciding on the approach for a request to enter needs to take the traffic situation into account as well as the type of vehicle that is requesting entry (civilian, police, ambulance, fire brigade).	100	100	10000
2	MB_HA04	Platoon maximum length hazard	track : Truck [1]	Maintain the correct maximum platoon length.	Inability to react to requests for departure, other vehicle entry fast enough.	MB_SG04 Maximum length handli	Too long platoons can result in an inability to react timely to events.	event with lasting effect	System of systems parameter misalignmer	HandlingTrucksWantingToJoin	On any road where platooning can be in use.	Possible traffic incidents.	Traffic accidents as a result of slow response to events.	If the platoon length is too long corrective action such as dissolve or split may take to long to accomplish resulting in an inability to tackle traffic occurrences.	Ey infrequent	Traffic incidents.	medium	S3 Life-threatening (survival uncertain) or fatal injuries		This is controllable by ensuring that the maximum lngth of the platoon is correctly determined.	D	HandlingOfEntryOfOtherVehicles	0.01	Given the maximum length of a truck to 25 meters, the length will be large quite quickly as the number of platooning trucks increase.	100	60	10000
3	MB_HA01	Assess platoon truck suitability hazard	track : Truck [1]	The platoon leader intends to allow the platoon to continue onward with a set speed and be able to maintain the individually determined safety distances in between the trucks contained in the platoon.	As a truck requests to enter a platoon, the platoon leader has to assess the parameters that the truck joining is capable of i.e., its ability to reach a distance to the truck in front that is shorter than its own adaptive control distance. This determination is based on the parameters that the joining truck delivers and if they are in error the safety distance determined may be too short resulting in an inability to respond to changes in the traffic rythm in the manner that is required.	MB_SG01 Platoon truck paramete	If the parameters used to govern the platoon are incorrect the safety distances in between trucks may be insufficient and in spite of the intended ability of the trucks to adapt to any changes in speed of the truck in front, their ability to do so may not be enough, given the fact that the parameters they published may be erroneous, thereby resulting in collisions within the platoon.	event with lasting effect	System of systems parameter misalignmer	HandlingTrucksWantingToJoin	On roads whee platooning takes place, presumably highways with more than one lane in each direction.	Truck parameter control is not good enough.	Trucks in the platoon can collide.	Any truck added to the platoon.	Ex occasionally	Can cause collisions in between trucks and cause a major traffic hazard both for the trucks and other vehicles.	Life threatening	S3 Life-threatening (survival uncertain) or fatal injuries	C3 Difficult to control	Safety depends on the assumption that the parameters delivered by a truck wishing to join are essentially correct.	D	HandlingTrucksWantingToJoin	0.01	The parameters of concern to assess suitability are exemplified by length, weight, max_power, brake_curve, tire conditions etc.	100	100	10000
4	MB_HA02	Platoon truck within platoon departure hazard	track : Truck [1]	The truck participating in the platoon placed somewhere ahead of the end wishes to leave the platoon and informs the platoon leader of the intent.	If a truck in the platoon places somewhere other than the end wishes to leave, and it reduces speed in a non-controlled manner to make the exit, collisions can occur between it as well as between other trucks behind the platoon truck attempting to leave.	MB_SG02 Handling of departure f MB_SG03 Platoon truck requested	The departing truck ends up transmitting the notification to leave to late for safe breaking to occur given the parameters governing the trucks in the platoon, causing collisions of trucks not being able to respond to the breaking performed by the truck leaving.	event with lasting effect	System of systems parameter misalignmer	PlatoonTruck PlatoonLeader	On any road where platooning in use, i.e. highways with more than one lane in each direction.	Insufficient time allowed for leaving notification due to navigator and platoon control issue.	Series collision between trucks.	Can occur if the platoon contains trucks with different end destinations.	Ey infrequent	Collisions between trucks and major traffic hazzard for other vehicles.	Life threatening	S3 Life-threatening (survival uncertain) or fatal injuries	C3 Difficult to control	Departure from tail end of platoon represents no problem and can be allowed easily. Departure by a truck within a platoon needs to allow the platoon to either agree, dissolve partially dissolve or split if this is to be managed.	D	HandlingTrucksWantingToLeave	0.01	Allowing a truck within the platoon to leave while maintaining the platoon would require the platoon to be able to adapt the platoon speed to a speed that is equal to the exit speed of the truck after which the gap would need to be closed up. If this is not the case a split or a dissolve of the platoon would be needed.	100	100	10000
5	MB_HA05	Platoon truck gap hazard	track : Truck [1]	Gaps result from an inability to manage inclines by a platoon truck due to a maximim power constraint.	A gap can easily become too large due to poser restrictions in some trucks not shared by other trucks.	MB_SG06 Gap Handling	Uncontrollability due to gap.	event with lasting effect	System of systems parameter misalignmer	HandlingTrucksWithinPlatoon	On any road where platooning can be in use.	Uncontrolled entry of other vehicles, uncontrollability of platoon.	Uncontrolled entry of other vehicles, general loss of control.	If a gap has appeared this can allow an uncontrolled other vehicle entry and also make it very difficult to control the platoon.	Ex occasionally	Uncontrollability	medium			It can be controlled by proper gap handling.	D	HandlingTrucksWithinPlatoon	0.01	As an example if the platoon leader a d a set of trucks just behind it can maintain a speed of 25 m/s and the truck just after it os only capable of maintaining 20 m/s, this means that trucks maintaining speed can do 200 meters in eight seconds whereas the 20 m/s trucks will in 8 seconds have done 160 meters generating a gap of 40 meters.	100	50	10000



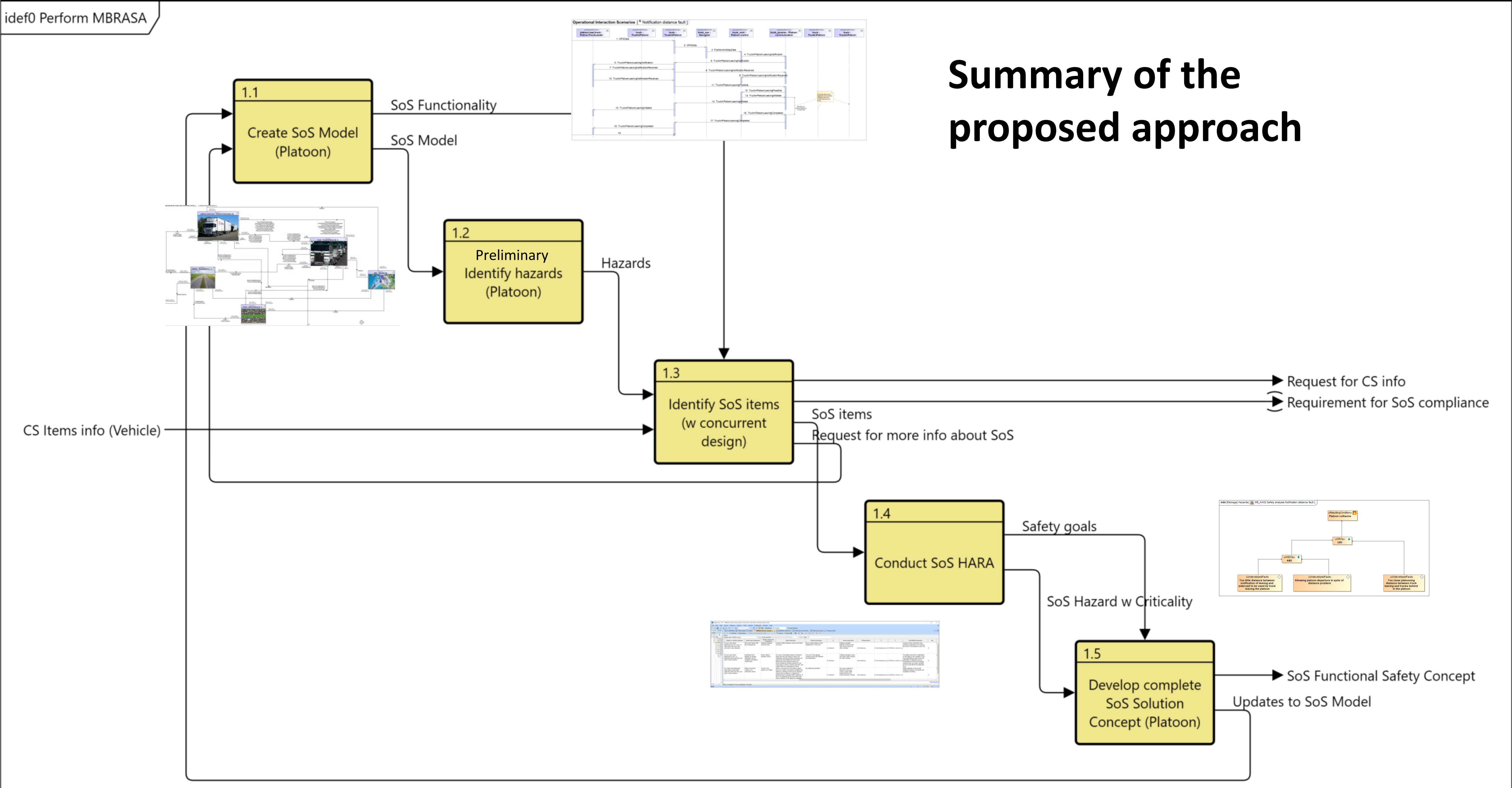
Name	Failure mode	Operational mode	Situation	Consequence	Hazard description	Exposure	Severity	Controllability	ASIL	Safety goal
Brake	Omission	High performance/Differential locks engaged	approaching intersection	Vehicle can not brake	Vehicle can not brake when approaching intersection	E4 Often-always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

Fault Tree Analysis (FTA)

Shows how a critical failure is broken down into potential causes and the logic


bdd [Package] Hazards [MB_HA02 Safety analysis Notification distance fault]
«ResultingCondition»
Platoon collisons
«OROp»
OR1
«ANDOp»
AND
«UndevelopedFault»
Too little distance between notification of leaving and sideroad to be used by truck leaving the platoon
«UndevelopedFault»
Allowing platoon departure in spite of distance problem
«UndevelopedFault»
Too close platooning distance between truck leaving and trucks behind in the platoon

Summary of the proposed approach


idef0 Perform MBRASA
1.1
Create SoS Model (Platoon)
SoS Functionality
SoS Model
Operational Interaction Scenarios
1.2
Preliminary Identify hazards (Platoon)
Hazards
1.3
Identify SoS items (w concurrent design)
CS Items info (Vehicle)
Request for CS info
Requirement for SoS compliance
SoS items
Request for more info about SoS
1.4
Conduct SoS HARA
Safety goals
SoS Hazard w Criticality
1.5
Develop complete SoS Solution Concept (Platoon)
SoS Functional Safety Concept
Updates to SoS Model

Project: MBRASA	Organization:	Date: 2022-11-14

Agenda Nov 23

13:30 Introduction to MBRASA, TECoSA, research idea

13:35 Use case presentation

13:45 The Approach

- Safety analysis moving into systems of systems
- System models supporting safety analysis
- Method approach

14:45 Workshop (including break)

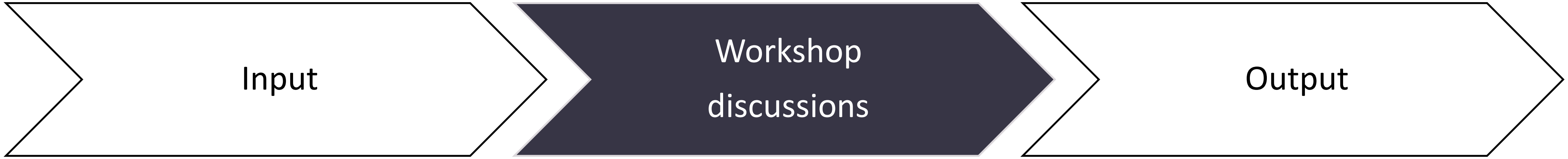
- Workshop set-up
- Group Discussions

15:45 Exchange and summary

16:30 Finish

Workshop setup

MBRASA Goal: facilitate the work for engineers to perform the safety work (with the end result of safer systems).



Input

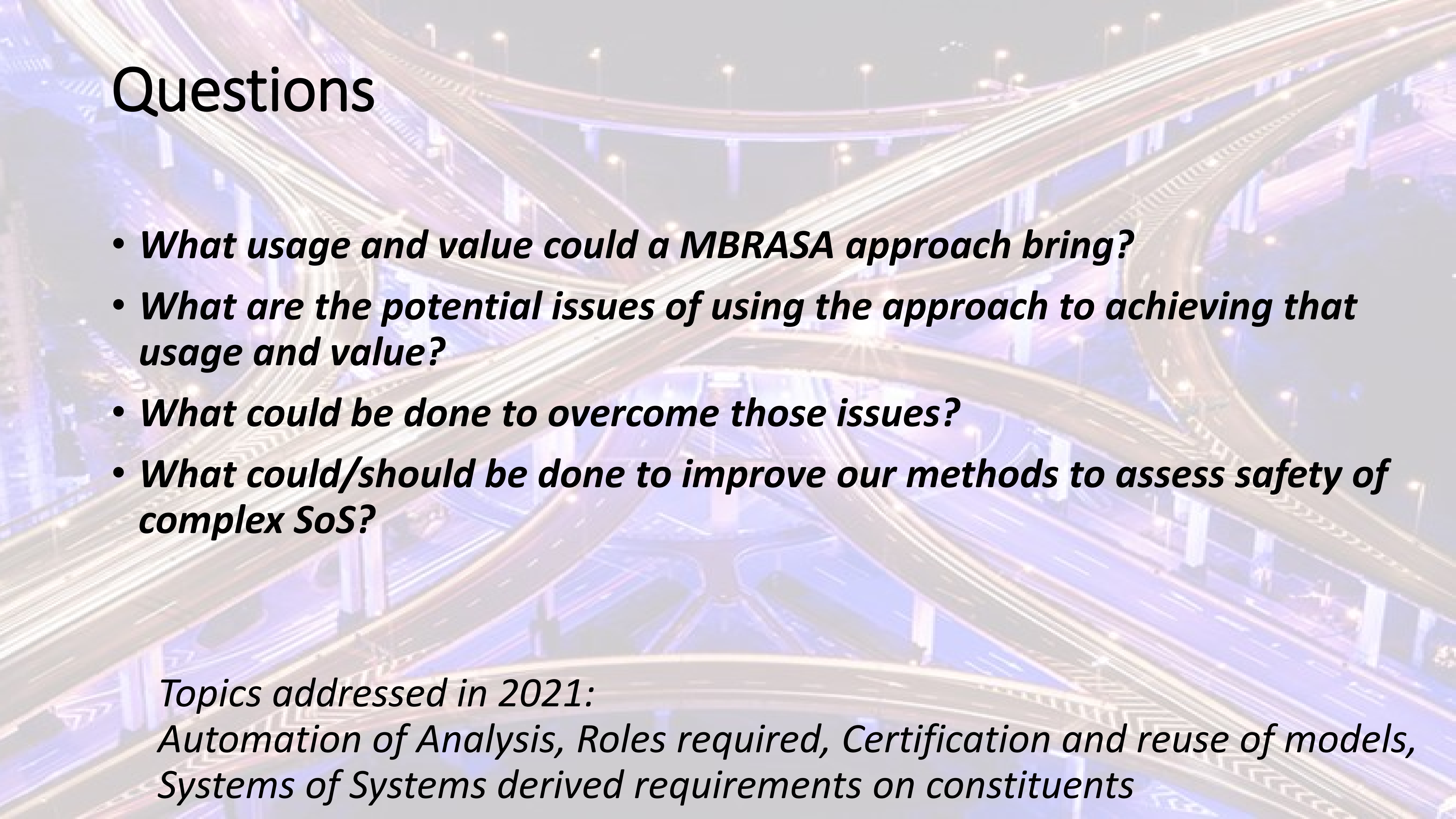
Workshop discussions

Output

- MBRASA approach
  - Safety analysis approach
  - System modelling approach
  - Use cases
- Personal experiences

- Considering a MBRASA approach as applied to your domain, what benefits could a MBRASA approach bring? What keeps us from reaping those benefits?
- Start by a round table presentation and appoint a note taker and presenter

- Reflections from each group, summarized in 3 key points
- As a follow up, for those interested, a summary of the workshop discussions as an amendment to the MBRASA project report.

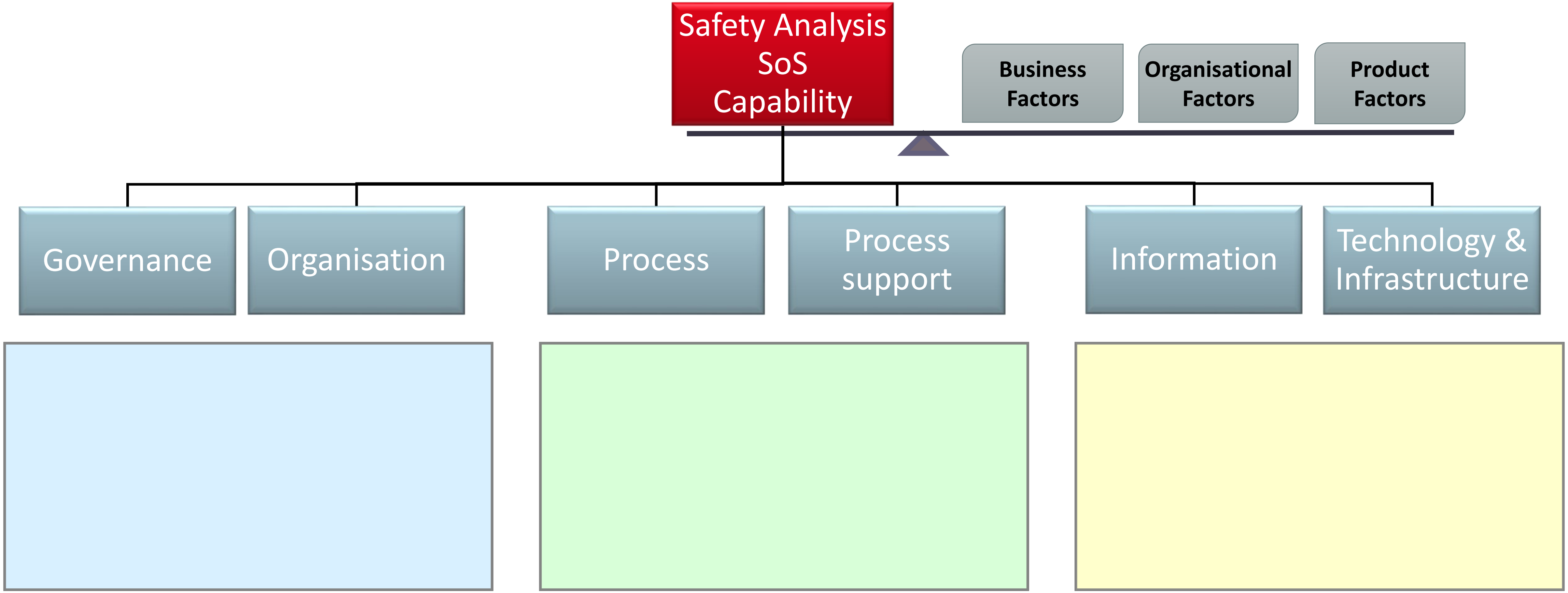


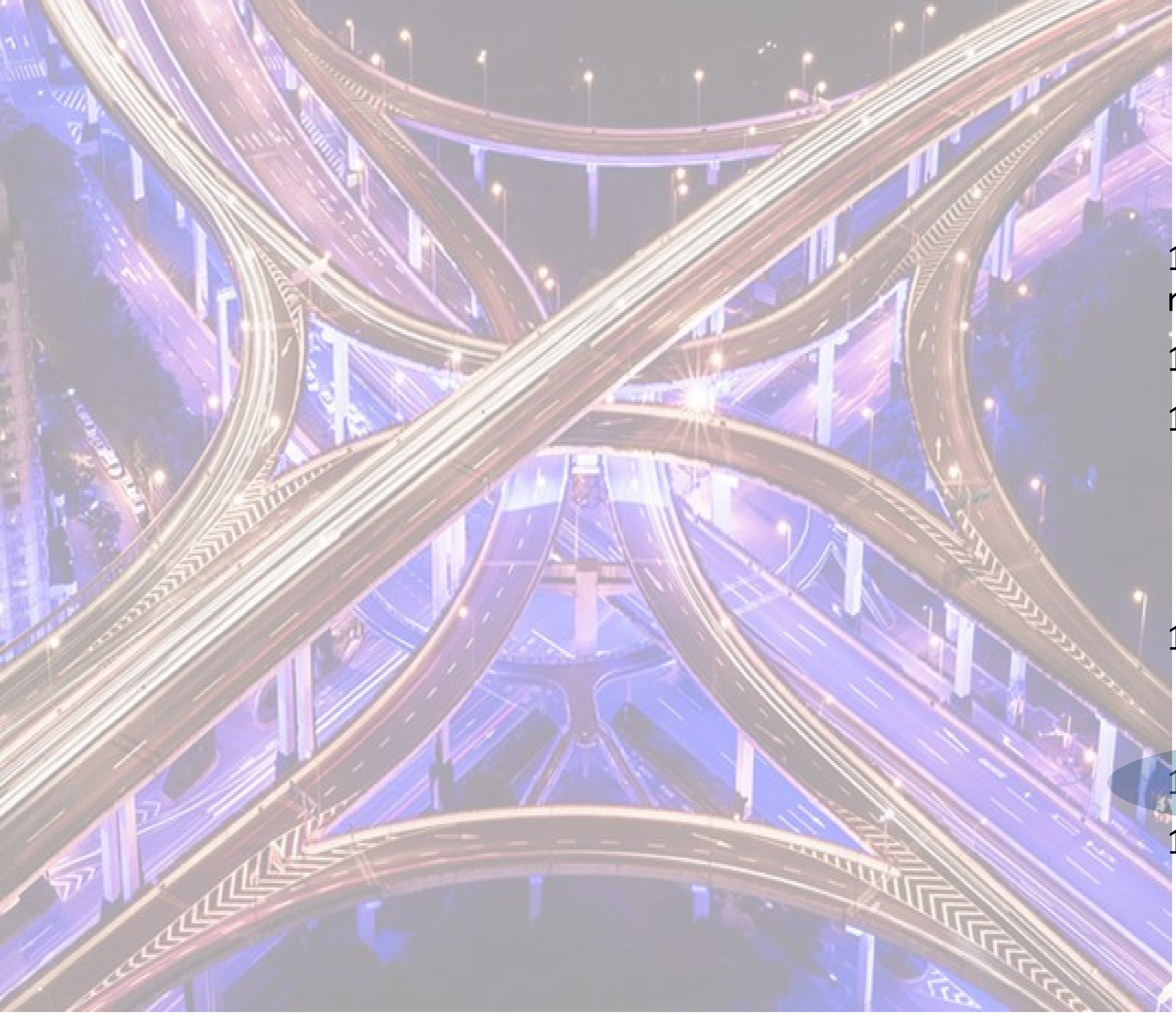
Questions

- ***What usage and value could a MBRASA approach bring?***
- ***What are the potential issues of using the approach to achieving that usage and value?***
- ***What could be done to overcome those issues?***
- ***What could/should be done to improve our methods to assess safety of complex SoS?***

Topics addressed in 2021:
Automation of Analysis, Roles required, Certification and reuse of models, Systems of Systems derived requirements on constituents

Capability Model - Safety Analysis of SoS





Agenda Nov 23

13:30 Introduction to MBRASA, TECoSA, research idea

13:35 Use case presentation

13:45 The Approach

- Safety analysis moving into systems of systems
- System models supporting safety analysis
- Method approach

14:45 Workshop (including break)

- Workshop set-up
- Group Discussions

15:45 Exchange and summary

16:30 Finish

TECOSA

Presentation and discussion

Each group, summarize in three (3) points the highlights of your discussion

A-Alfa
Diver Down Keep Clear
B-Bravo
Dangerous Cargo
C-Charlie
Yes
D-Delta
Keep Clear
E-Echo
Altering Course to Starboard
F-Foxtrot
Disabled

GROUPS:

B-Bravo
Dangerous Cargo

C-Charlie
Yes

D-Delta
Keep Clear

F-Foxtrot
Disabled

1. ***What usage and value could a MBRASA approach bring?***

2. ***What are the potential issues of using the approach to achieving that usage and value?***

3. ***What could be done to overcome those issues?***

4. ***What could/should be done to improve our methods to assess safety of complex SoS?***

Syntax: "+" for usage and value, "-" for issues (problems), "!" for proposal for improvement

B-Bravo
Dangerous Cargo

Bravo group:

+ The method seems useful to be able to evaluate a system-of-systems before detailed design.

+ The delta identification

- Physical limits of the systems is overlooked.
- If a model is too complex it may indicate non-safety.

! Strive for simplicity

D-Delta
Keep Clear

Delta group:

- Lacking assurance of environmental model. For instance road markings.
- Lacking a method for communicating requirements (and traceability) between developing organizations. This includes not only truck manufacturers but infrastructure.

! Consider iterative process to gradually improve the uncertainty of the model.

! Sotif and cybersecurity is needed as part of the approach. There are very many attack vectors for a platoon. Each truck has interface.

C-Charlie
Yes

Charlie group:+ Repeatable

+ Modelling the system builds skills

+ Governance added

+ Standardization need to be enforced

- Not sure it is possible to model, but how else could it be done?

! Tools may be built for this.

F-Foxtrot
Disabled

Foxtrot group:

+ provides for overview

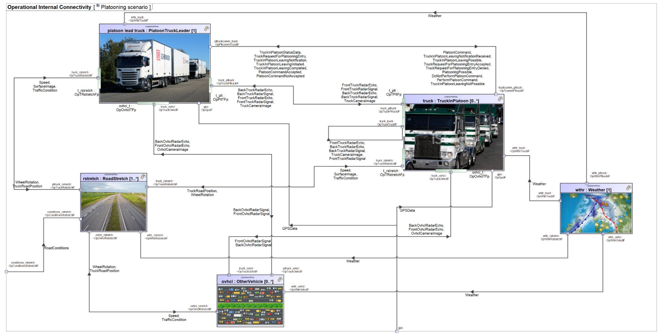
+ behavioural aspects of the SoS could be elicited by the SoS model and used as requirements for constituents.

+ Aid in decision making

- Analysis needed for freedom of interference between parts.
- Safety case needs more details.

! The STPA method could be incorporated to improve.

Agile Systems Lifecycle Management

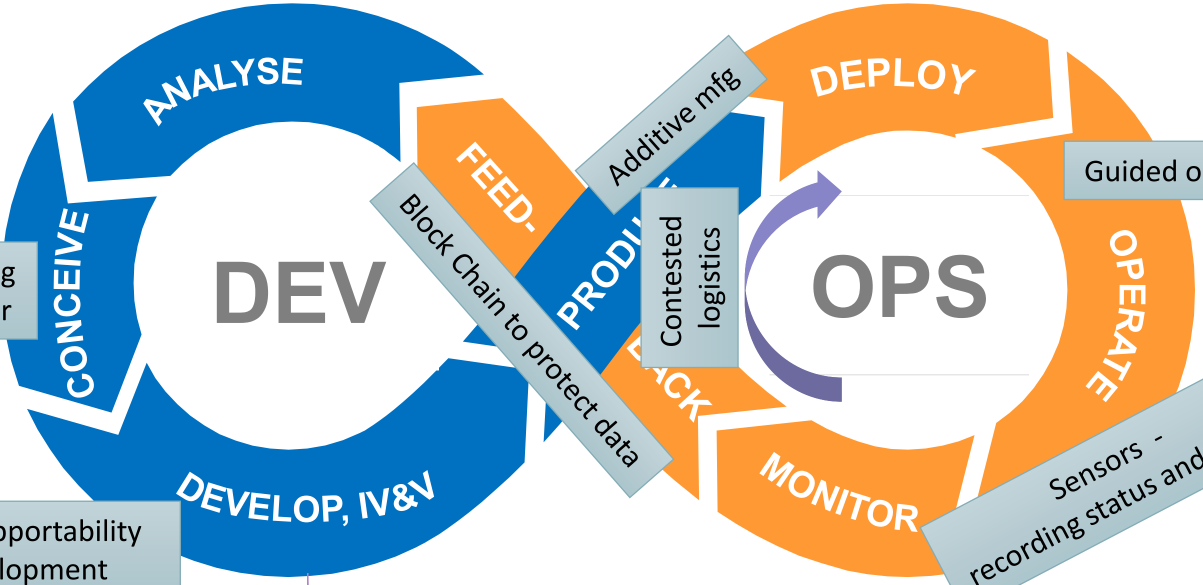


AI/ ML
Making sense of Big Data

Robotics and unmanned systems
(facilitating deployment/supply)

System-of-Interest IRL

Enterprise and System Modelling
Making the right decisions faster



Additive mfg

Block Chain to protect data

Contested logistics

Guided operations

Sensors - recording status and trends

MB SE, safety and Supportability
Analysis – faster development

Support system

Requirements
Engineering

Systems
Engineering

Logistics
Engineering and Mgmt

Configuration Management

Thanks for participating!

For questions and follow up, please contact us

Joakim Fröberg,
joakim.froberg@safetyintegrity.se

Tom Strandberg
tom.strandberg@syntell.se