Contents

CONTEXT bonaventure_0_ctxt

SETS

VEHICLE

TUNNEL_TRAVEL_LANE

CONSTANTS

TRAVEL_LANE_I

TRAVEL_LANE_II

Tunnel

Tunnel_part1

Tunnel_part2

Visibility_Limit

aa

bb

cc

Vehicle_Length

AXIOMS

axm0_1: $partition(TUNNEL\_TRAVEL\_LANE, \{TRAVEL\_LANE\_I\}, \{TRAVEL\_LANE\_II\})$

axm0_2: $Tunnel \subseteq \mathbb{N}$

axm0_3: $Tunnel\_part1 \subseteq Tunnel$

axm0_4: $Tunnel\_part2 \subseteq Tunnel$

axm0_5: $Visibility\_Limit \in Tunnel\_part1 \pfun Tunnel$

axm0_6: $aa \in \mathbb{N}$

axm0_7: $bb \in \mathbb{N}$

axm0_8: $cc \in \mathbb{N}$

axm0_9: $finite(VEHICLE)$

axm0_10: $Vehicle\_Length \in VEHICLE \tfun \mathbb{N}$

p0_1: $aa < bb$

p0_2: $bb < cc$

p0_3: $Tunnel\_part1 = aa \upto bb$

p0_4: $Tunnel\_part2 = bb \upto cc$

p0_5: $Tunnel = Tunnel\_part1 \cup Tunnel\_part2$

p0_7: $\forall xx \cdot (xx \in dom(Visibility\_Limit) \limp Visibility\_Limit(xx) > xx)$

END

CONTEXT bonaventure_1_ctxt
EXTENDS bonaventure_0_ctxt
SETS
TRAFFIC_LEVEL
CONSTANTS
NORMAL
DENSE
SLOWED
CONGESTION
MAXIMAL_TUNNEL_OCCUPATION
AXIOMS
axm1_1: $partition(TRAFFIC\_LEVEL, \{NORMAL\}, \{DENSE\}, \{SLOWED\}, \{CONGESTION\})$
axm1_2: $MAXIMAL\_TUNNEL\_OCCUPATION \in \mathbb{N}_1$
END

CONTEXT bonaventure_2_ctxt
EXTENDS bonaventure_1_ctxt
END

CONTEXT bonaventure_3_ctxt
EXTENDS bonaventure_2_ctxt
SETS

Sensor
OPERATING_MODE
Traffic_Light
COLOR

CONSTANTS

NORMAL_MODE
DEGRADED_MODE_I
DEGRADED_MODE_II
RED
GREEN
ORANGE
VdM_Sensor
MtQ_Sensor
AID
Traffic_Light_William
Traffic_Light_Wellington
Traffic_Light_Position
Traffic_Light_Coverage_Rear
Traffic_Light_Color
Sensor_Position
Sensor_Coverage_Front
Sensor_Coverage_Rear
Sensor_Detection_Accuracy

AXIOMS

axm1: $partition(OPERATING\_MODE, \{NORMAL\_MODE\}, \{DEGRADED\_MODE\_I\}, \{DEGRADED\_MODE\_II\})$
axm2: $partition(COLOR, \{RED\}, \{GREEN\}, \{ORANGE\})$
@axm3 VdM_Sensor $\subseteq$ Sensor
axm4: $partition(Sensor, VdM\_Sensor, MtQ\_Sensor)$
axm5: $AID \in MtQ\_Sensor$
axm6: $Traffic\_Light\_William \in Traffic\_Light$
axm7: $Traffic\_Light\_Wellington \in Traffic\_Light$
axm8: $Traffic\_Light\_Position \in Traffic\_Light \to Tunnel$
axm9: $Traffic\_Light\_Coverage\_Rear \in Traffic\_Light \to Tunnel$
axm10: $Traffic\_Light\_Color = Traffic\_Light \times COLOR$
axm11: $Sensor\_Position \in Sensor \to Tunnel$
axm12: $AID \mapsto cc \in Sensor\_Position$
axm13: $Sensor\_Coverage\_Front \in Sensor \to Tunnel$
axm14: $AID \mapsto cc \in Sensor\_Coverage\_Front$
axm15: $Sensor\_Coverage\_Rear \in Sensor \to Tunnel$
axm16: $AID \mapsto aa \in Sensor\_Coverage\_Rear$
axm17: $Sensor\_Detection\_Accuracy \in Sensor \to \mathbb{N}$
axm18: $AID \mapsto 1 \in Sensor\_Detection\_Accuracy$
axm19: $VdM\_Sensor \neq \varnothing$
axm20: $finite(Sensor)$
p3_1: $\forall xx \cdot (xx \in VdM\_Sensor \Rightarrow Sensor\_Detection\_Accuracy(xx) \geq Sensor\_Detection\_Accuracy(AID))$

END

MACHINE bonaventure_0_mch
SEES bonaventure_0_ctxt
VARIABLES
Vehicle
Vehicle_Front_Position
Vehicle_Travel_Lane
Speed_Limit
Min_Brake_Distance
INVARIANTS
inv0_1: $Vehicle \subseteq VEHICLE$
inv0_2: $Vehicle\_Front\_Position \in Vehicle \rightarrow Tunnel$
inv0_3: $Vehicle\_Travel\_Lane \in Vehicle \rightarrow TUNNEL\_TRAVEL\_LANE$
inv0_4: $Speed\_Limit \in Tunnel \rightarrow \mathbb{N}$
inv0_5: $Min\_Brake\_Distance \in ran(Speed\_Limit) \rightarrow \mathbb{N}$
p0_6: $\forall xx \cdot ((xx \in Vehicle \wedge Vehicle\_Front\_Position(xx) \in Tunnel\_part1) \Rightarrow Vehicle\_Travel\_Lane(xx) = TRAVEL\_LANE\_I)$
p0_8: $\forall xx \cdot (xx \in dom(Visibility\_Limit) \Rightarrow Visibility\_Limit(xx) - xx \geq Min\_Brake\_Distance(Speed\_Limit(xx)))$
p0_10: $\forall xx1, xx2 \cdot ((xx1 \in Vehicle \wedge xx2 \in Vehicle \wedge xx1 \neq xx2) \Rightarrow ((Vehicle\_Front\_Position(xx1) - Vehicle\_Length(xx1)) .. Vehicle\_Front\_Position(xx1) \cap (Vehicle\_Front\_Position(xx2) - Vehicle\_Length(xx2)) .. Vehicle\_Front\_Position(xx2) = \varnothing \vee Vehicle\_Travel\_Lane(xx1) \neq Vehicle\_Travel\_Lane(xx2)))$
EVENTS
Initialisation
introduire un evenement de simulation pour l'entree des vehicules
begin
act1: $Vehicle := \varnothing$
act2: $Vehicle\_Front\_Position := \varnothing$
act3: $Vehicle\_Travel\_Lane := \varnothing$
act4: $Speed\_Limit := Tunnel \times \{70\}$
act5: $Min\_Brake\_Distance := \{70 \mapsto 0\}$
end
Event ctrl_BringVehicleInsideTunnel ⟨ordinary⟩ $\widehat{=}$
any
vehicle
front
travelLane
where
grd1: $vehicle \in VEHICLE \setminus Vehicle$
grd2: $front \in Tunnel$
grd3: $travelLane \in TUNNEL\_TRAVEL\_LANE$
grd4: $front \in Tunnel\_part1 \Rightarrow travelLane = TRAVEL\_LANE\_I$
grd5: $\forall xx \cdot (xx \in Vehicle \Rightarrow ((Vehicle\_Front\_Position(xx) - Vehicle\_Length(xx)) .. Vehicle\_Front\_Position(xx) \cap (front - Vehicle\_Length(vehicle)) .. front = \varnothing \vee Vehicle\_Travel\_Lane(xx) \neq travelLane))$
then
act1: $Vehicle := Vehicle \cup \{vehicle\}$
act2: $Vehicle\_Front\_Position(vehicle) := front$
act3: $Vehicle\_Travel\_Lane(vehicle) := travelLane$
end
Event BringOutEachVehiclePresentInTunnel ⟨ordinary⟩ $\widehat{=}$
LA TACHE DE VERIFICATION SYSML/KAOS FAIT APPARAÎTRE QU'IL DOIT S'AGIR ICI D'UN RAFFINEMENT MILESTONE ET PAS AND
any
Vehicle_Out
Vehicle_In
newVehicleFronts
newTravelLanes

where

grd0: $Vehicle \neq \varnothing$

grd1: $partition(Vehicle, Vehicle\_Out, Vehicle\_In)$

grd2: $newVehicleFronts \in Vehicle\_In \rightarrow Tunnel$

grd3: $newTravelLanes \in Vehicle\_In \rightarrow TUNNEL\_TRAVEL\_LANE$

grd4: $\forall xx \cdot ((xx \in Vehicle\_In \wedge newVehicleFronts(xx) \in Tunnel\_part1) \Rightarrow newTravelLanes(xx) = TRAVEL\_LANE\_I)$

grd5: $\forall xx1, xx2 \cdot ((xx1 \in Vehicle\_In \wedge xx2 \in Vehicle\_In \wedge xx1 \neq xx2) \Rightarrow ((newVehicleFronts(xx1) - Vehicle\_Length(xx1)) .. newVehicleFronts(xx1) \cap (newVehicleFronts(xx2) - Vehicle\_Length(xx2)) .. newVehicleFronts(xx2) = \varnothing \vee newTravelLanes(xx1) \neq newTravelLanes(xx2)))$

then

act1: $Vehicle := Vehicle \setminus Vehicle\_Out$

act2: $Vehicle\_Front\_Position := newVehicleFronts$

act3: $Vehicle\_Travel\_Lane := newTravelLanes$

end

END

MACHINE bonaventure_1_mch
REFINES bonaventure_0_mch
SEES bonaventure_1_ctxt
VARIABLES

Vehicle
Vehicle_Front_Position
Vehicle_Travel_Lane
Speed_Limit
Min_Brake_Distance
traffic_level
Vehicle_Speed

INVARIANTS

inv1_1: $traffic\_level \in TRAFFIC\_LEVEL$

inv1_2: $Vehicle\_Speed \in Vehicle \to \mathbb{N}$

p1_1: $\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \leq Speed\_Limit(Vehicle\_Front\_Position(xx)))$

p1_2: $(traffic\_level = NORMAL \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \geq 40))))$

p1_3: $(traffic\_level = DENSE \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 35 \mathinner{..} 39))))$

p1_4: $(traffic\_level = SLOWED \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 25 \mathinner{..} 34))))$

p1_5: $(traffic\_level = CONGESTION \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) < 15))))$
@sysmlkaos_(MoveVehicle_Guard=>BringOutEachVehiclePresentInTunnel_Guard) : prouvé par le raffinement classique Event-B

sysmlkaos_(MoveVehicle_Post=>ManageCongestion_Guard): ⟨theorem⟩
$\forall delay, newTravelLanes, updatedVehicleFronts, newVehicleSpeeds, Vehicle\_Out, Vehicle\_In, trafficLevel, newVehicleFronts \cdot ($
$($
$delay \in \mathbb{N}_1$
$\wedge Vehicle \neq \varnothing$
$\wedge updatedVehicleFronts = (\lambda xx \cdot xx \in Vehicle | Vehicle\_Front\_Position(xx) + Vehicle\_Speed(xx) * delay)$
$\wedge Vehicle\_In = updatedVehicleFronts^{-1}[Tunnel]$
$\wedge Vehicle\_Out = Vehicle \setminus Vehicle\_In$
$\wedge newVehicleSpeeds \in Vehicle\_In \to \mathbb{N}$
$\wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 0..Speed\_Limit(updatedVehicleFronts(xx))))$
$\wedge newTravelLanes \in Vehicle\_In \to TUNNEL\_TRAVEL\_LANE$
$\wedge newVehicleFronts = Vehicle\_Out \lhd updatedVehicleFronts$
$\wedge trafficLevel \in TRAFFIC\_LEVEL$
$\wedge (trafficLevel = NORMAL \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \geq 40))))$
$\wedge (trafficLevel = DENSE \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 35 \mathinner{..} 39))))$
$\wedge (trafficLevel = SLOWED \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 25 \mathinner{..} 34))))$
$\wedge (trafficLevel = CONGESTION \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) < 15))))$
$\wedge (\forall xx \cdot ((xx \in Vehicle\_In \wedge newVehicleFronts(xx) \in Tunnel\_part1) \Rightarrow newTravelLanes(xx) = TRAVEL\_LANE\_I))$
$\wedge (\forall xx1, xx2 \cdot ((xx1 \in Vehicle\_In \wedge xx2 \in Vehicle\_In \wedge xx1 \neq xx2) \Rightarrow ((newVehicleFronts(xx1) - Vehicle\_Length(xx1))..newVehicleFronts(xx1) \cap (newVehicleFronts(xx2) - Vehicle\_Length(xx2))..newVehicleFronts(xx2) = \varnothing \vee newTravelLanes(xx1) \neq newTravelLanes(xx2))))$
$)$
$\Rightarrow (TRUE = TRUE))$
@sysmlkaos_(ManageCongestion_Post=>BringOutEachVehiclePresentInTunnel_Post) : prouvé par le raffinement classique Event-B, car ManageCongestion préserve la post-condition de MoveVehicle.

ON PEUT CONSTATER QUE SANS LE BUT MoveVehicle, IL N'AURAIT PAS ÉTÉ POSSIBLE DE SATISFAIRE BringOutEachVehiclePresentInTunnel ET LES PREUVES SYSML/KAOS AURAIENT PERMIS DE DETECTER CET ETAT DE FAITS

EVENTS

Initialisation ⟨extended⟩

begin

act1: $Vehicle := \varnothing$

act2: $Vehicle\_Front\_Position := \varnothing$

act3: $Vehicle\_Travel\_Lane := \varnothing$

act4: $Speed\_Limit := Tunnel \times \{70\}$

act5: $Min\_Brake\_Distance := \{70 \mapsto 0\}$

act7: $traffic\_level := NORMAL$

act8: $Vehicle\_Speed := \varnothing$

end

Event ctrl_BringVehicleInsideTunnel ⟨ordinary⟩ $\widehat{=}$

extends ctrl_BringVehicleInsideTunnel

any

vehicle

front

travelLane

speed

trafficLevel

where

grd1: $vehicle \in VEHICLE \setminus Vehicle$

grd2: $front \in Tunnel$

grd3: $travelLane \in TUNNEL\_TRAVEL\_LANE$

grd4: $front \in Tunnel\_part1 \Rightarrow travelLane = TRAVEL\_LANE\_I$

grd5: $\forall xx \cdot (xx \in Vehicle \Rightarrow ((Vehicle\_Front\_Position(xx) - Vehicle\_Length(xx)) .. Vehicle\_Front\_Position(xx) \cap (front - Vehicle\_Length(vehicle)) .. front = \varnothing \vee Vehicle\_Travel\_Lane(xx) \neq travelLane))$

grd6: $speed \in 0 .. Speed\_Limit(front)$

grd7: $trafficLevel \in TRAFFIC\_LEVEL$

grd8: $trafficLevel = NORMAL \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \geq 40 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \geq 40)))$

grd9: $trafficLevel = DENSE \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \in 35 .. 39 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 35 .. 39)))$

grd10: $trafficLevel = SLOWED \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed \in 25 .. 34 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 25 .. 34)))$

grd11: $trafficLevel = CONGESTION \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed < 15 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) < 15)))$

then

act1: $Vehicle := Vehicle \cup \{vehicle\}$

act2: $Vehicle\_Front\_Position(vehicle) := front$

act3: $Vehicle\_Travel\_Lane(vehicle) := travelLane$

act4: $Vehicle\_Speed(vehicle) := speed$

act5: $traffic\_level := trafficLevel$

end

Event ctrl_ChangeSpeed ⟨ordinary⟩ $\widehat{=}$

any

vehicle

speed

trafficLevel

where

grd1: $vehicle \in Vehicle$

grd2: $speed \in 0 .. Speed\_Limit(Vehicle\_Front\_Position(vehicle)) \setminus \{Vehicle\_Speed(vehicle)\}$

grd3: $trafficLevel \in TRAFFIC\_LEVEL$

grd4:
$trafficLevel = NORMAL \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \geq 40 \wedge (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \geq 40)))$
grd5:
$trafficLevel = DENSE \Rightarrow (((card(Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \in 35 \mathinner{..} 39 \wedge (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \in 35 \mathinner{..} 39)))$
grd6:
$trafficLevel = SLOWED \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed \in 25 \mathinner{..} 34 \wedge (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \in 25 \mathinner{..} 34)))$
grd7:
$trafficLevel = CONGESTION \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed < 15 \wedge (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) < 15)))$

then

act1: $Vehicle\_Speed(vehicle) := speed$
act2: $traffic\_level := trafficLevel$

end

Event MoveVehicle ⟨ordinary⟩ $\widehat{=}$
refines BringOutEachVehiclePresentInTunnel

any

delay
newTravelLanes
updatedVehicleFronts
newVehicleSpeeds
Vehicle_Out
Vehicle_In
trafficLevel
newVehicleFronts

where

grd0: $delay \in \mathbb{N}_1$
grd01: $Vehicle \neq \varnothing$
grd1: $updatedVehicleFronts = (\lambda xx \cdot xx \in Vehicle | Vehicle\_Front\_Position(xx) + Vehicle\_Speed(xx) * delay)$
les prouveurs ont beaucoup de mal avec ce type de definition: il est necessaire a chaque fois d'expliciter le resultat ou de donner le superset dans le cas de la cardinalite
grd2: $Vehicle\_In = updatedVehicleFronts^{-1}[Tunnel]$
grd3: $Vehicle\_Out = Vehicle \setminus Vehicle\_In$
grd4: $newVehicleSpeeds \in Vehicle\_In \rightarrow \mathbb{N}$
grd5: $\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 0 .. Speed\_Limit(updatedVehicleFronts(xx)))$

grd6: $newTravelLanes \in Vehicle\_In \rightarrow TUNNEL\_TRAVEL\_LANE$
grd7: $newVehicleFronts = Vehicle\_Out \lhd updatedVehicleFronts$
grd8: $trafficLevel \in TRAFFIC\_LEVEL$
grd9:
$(trafficLevel = NORMAL \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \geq 40))))$
grd10:
$(trafficLevel = DENSE \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 35 \mathinner{..} 39))))$
grd11:
$(trafficLevel = SLOWED \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 25 \mathinner{..} 34))))$
grd12:
$(trafficLevel = CONGESTION \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) < 15))))$
grd13: $\forall xx \cdot ((xx \in Vehicle\_In \wedge newVehicleFronts(xx) \in Tunnel\_part1) \Rightarrow newTravelLanes(xx) = TRAVEL\_LANE\_I)$
grd14: $\forall xx1, xx2 \cdot ((xx1 \in Vehicle\_In \wedge xx2 \in Vehicle\_In \wedge xx1 \neq xx2) \Rightarrow ((newVehicleFronts(xx1) - Vehicle\_Length(xx1)) .. newVehicleFronts(xx1) \cap (newVehicleFronts(xx2) - Vehicle\_Length(xx2)) .. newVehicleFronts(xx2) = \varnothing \vee newTravelLanes(xx1) \neq newTravelLanes(xx2)))$

then

act1: $Vehicle := Vehicle\_In$

act2: $Vehicle\_Front\_Position := newVehicleFronts$

act3: $Vehicle\_Travel\_Lane := newTravelLanes$

act4: $traffic\_level := trafficLevel$

act5: $Vehicle\_Speed := newVehicleSpeeds$

end

Event ManageCongestion ⟨ordinary⟩ $\widehat{=}$

begin

skip

end

END

MACHINE bonaventure_2_mch
REFINES bonaventure_1_mch
SEES bonaventure_1_ctxt
VARIABLES

trafficReaded
Vehicle
Vehicle_Front_Position
Vehicle_Travel_Lane
Speed_Limit
Min_Brake_Distance
traffic_level
Vehicle_Speed
Observed_Vehicle
Observed_Vehicle_Speed
Observed_Vehicle_Front_Position
Observed_Vehicle_Travel_Lane
observed_traffic_level

INVARIANTS

inv0: $trafficReaded \in BOOL$
inv01: $Observed\_Vehicle \subseteq VEHICLE$
inv1: $trafficReaded = TRUE \Rightarrow Observed\_Vehicle \subseteq Vehicle$
inv2: $Observed\_Vehicle\_Speed \in Observed\_Vehicle \rightarrow \mathbb{N}$
inv3: $Observed\_Vehicle\_Front\_Position \in Observed\_Vehicle \rightarrow Tunnel$
inv4: $Observed\_Vehicle\_Travel\_Lane \in Observed\_Vehicle \rightarrow TUNNEL\_TRAVEL\_LANE$
inv5: $observed\_traffic\_level \in TRAFFIC\_LEVEL$
p2_1:
$observed\_traffic\_level = NORMAL$
$\Rightarrow (((card(Observed\_Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40$
$\wedge (\forall xx \cdot (xx \in Observed\_Vehicle \Rightarrow Observed\_Vehicle\_Speed(xx) \geq 40)))$
p2_2:
$observed\_traffic\_level = DENSE$
$\Rightarrow (((card(Observed\_Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40$
$\wedge (\forall xx \cdot (xx \in Observed\_Vehicle \Rightarrow Observed\_Vehicle\_Speed(xx) \in 35 \mathinner{..} 39)))$
p2_3:
$observed\_traffic\_level = SLOWED$
$\Rightarrow (((card(Observed\_Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40$
$\wedge (\forall xx \cdot (xx \in Observed\_Vehicle \Rightarrow Observed\_Vehicle\_Speed(xx) \in 25 \mathinner{..} 34)))$
p2_4:
$observed\_traffic\_level = CONGESTION$
$\Rightarrow (((card(Observed\_Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40$
$\wedge (\forall xx \cdot (xx \in Observed\_Vehicle \Rightarrow Observed\_Vehicle\_Speed(xx) < 15)))$
p2_5:
$\forall xx \cdot ((xx \in Observed\_Vehicle \wedge Observed\_Vehicle\_Front\_Position(xx) \in Tunnel\_part1)$
$\Rightarrow Observed\_Vehicle\_Travel\_Lane(xx) = TRAVEL\_LANE\_I)$
p2_6:
$\forall xx1, xx2 \cdot ((xx1 \in Observed\_Vehicle \wedge xx2 \in Observed\_Vehicle \wedge xx1 \neq xx2)$
$\Rightarrow ((Observed\_Vehicle\_Front\_Position(xx1) - Vehicle\_Length(xx1)) \mathinner{..} Observed\_Vehicle\_Front\_Position(xx1)$
$\cap (Observed\_Vehicle\_Front\_Position(xx2) - Vehicle\_Length(xx2)) \mathinner{..} Observed\_Vehicle\_Front\_Position(xx2)$
$= \varnothing \vee Observed\_Vehicle\_Travel\_Lane(xx1) \neq Observed\_Vehicle\_Travel\_Lane(xx2)))$
p2_7:
$\forall xx \cdot (xx \in Observed\_Vehicle$
$\Rightarrow Observed\_Vehicle\_Speed(xx) \leq Speed\_Limit(Observed\_Vehicle\_Front\_Position(xx)))$

EVENTS
Initialisation ⟨extended⟩

begin

act1: $Vehicle := \varnothing$
act2: $Vehicle\_Front\_Position := \varnothing$
act3: $Vehicle\_Travel\_Lane := \varnothing$
act4: $Speed\_Limit := Tunnel \times \{70\}$
act5: $Min\_Brake\_Distance := \{70 \mapsto 0\}$
act7: $traffic\_level := NORMAL$
act8: $Vehicle\_Speed := \varnothing$
act9: $Observed\_Vehicle := \varnothing$
act10: $Observed\_Vehicle\_Speed := \varnothing$
act11: $Observed\_Vehicle\_Front\_Position := \varnothing$
act12: $Observed\_Vehicle\_Travel\_Lane := \varnothing$
act13: $observed\_traffic\_level := NORMAL$
act14: $trafficReaded := FALSE$

end

Event ctrl_BringVehicleInsideTunnel ⟨ordinary⟩ $\widehat{=}$
extends ctrl_BringVehicleInsideTunnel

any

vehicle
front
travelLane
speed
trafficLevel

where

grd1: $vehicle \in VEHICLE \setminus Vehicle$
grd2: $front \in Tunnel$
grd3: $travelLane \in TUNNEL\_TRAVEL\_LANE$
grd4: $front \in Tunnel\_part1 \Rightarrow travelLane = TRAVEL\_LANE\_I$
grd5: $\forall xx \cdot (xx \in Vehicle \Rightarrow ((Vehicle\_Front\_Position(xx) - Vehicle\_Length(xx)) .. Vehicle\_Front\_Position(xx) \cap (front - Vehicle\_Length(vehicle)) .. front = \varnothing \vee Vehicle\_Travel\_Lane(xx) \neq travelLane))$
grd6: $speed \in 0 .. Speed\_Limit(front)$
grd7: $trafficLevel \in TRAFFIC\_LEVEL$
grd8: $trafficLevel = NORMAL \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \geq 40 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \geq 40)))$
grd9: $trafficLevel = DENSE \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \in 35 .. 39 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 35 .. 39)))$
grd10: $trafficLevel = SLOWED \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed \in 25 .. 34 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 25 .. 34)))$
grd11: $trafficLevel = CONGESTION \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed < 15 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) < 15)))$

then

act1: $Vehicle := Vehicle \cup \{vehicle\}$
act2: $Vehicle\_Front\_Position(vehicle) := front$
act3: $Vehicle\_Travel\_Lane(vehicle) := travelLane$
act4: $Vehicle\_Speed(vehicle) := speed$
act5: $traffic\_level := trafficLevel$
act6: $trafficReaded := FALSE$

end

Event ctrl_ChangeSpeed ⟨ordinary⟩ $\widehat{=}$
extends ctrl_ChangeSpeed

any

vehicle
speed
trafficLevel

where

grd1: $vehicle \in Vehicle$
grd2: $speed \in 0 \mathinner{..} Speed\_Limit(Vehicle\_Front\_Position(vehicle)) \setminus \{Vehicle\_Speed(vehicle)\}$
grd3: $trafficLevel \in TRAFFIC\_LEVEL$
grd4: $trafficLevel = NORMAL \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land speed \geq 40 \land (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \geq 40)))$
grd5: $trafficLevel = DENSE \Rightarrow (((card(Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land speed \in 35 \mathinner{..} 39 \land (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \in 35 \mathinner{..} 39)))$
grd6: $trafficLevel = SLOWED \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land speed \in 25 \mathinner{..} 34 \land (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \in 25 \mathinner{..} 34)))$
grd7: $trafficLevel = CONGESTION \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land speed < 15 \land (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) < 15)))$

then

act1: $Vehicle\_Speed(vehicle) := speed$
act2: $traffic\_level := trafficLevel$

end

Event MoveVehicle ⟨ordinary⟩ $\widehat{=}$
extends MoveVehicle

any

$delay$
$newTravelLanes$
$updatedVehicleFronts$
$newVehicleSpeeds$
$Vehicle\_Out$
$Vehicle\_In$
$trafficLevel$
$newVehicleFronts$

where

grd0: $delay \in \mathbb{N}_1$
grd01: $Vehicle \neq \varnothing$
grd1: $updatedVehicleFronts = (\lambda xx \cdot xx \in Vehicle | Vehicle\_Front\_Position(xx) + Vehicle\_Speed(xx) * delay)$
les prouveurs ont beaucoup de mal avec ce type de definition: il est necessaire a chaque fois d'expliciter le resultat ou de donner le superset dans le cas de la cardinalite
grd2: $Vehicle\_In = updatedVehicleFronts^{-1}[Tunnel]$
grd3: $Vehicle\_Out = Vehicle \setminus Vehicle\_In$
grd4: $newVehicleSpeeds \in Vehicle\_In \to \mathbb{N}$
grd5: $\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 0..Speed\_Limit(updatedVehicleFronts(xx)))$

grd6: $newTravelLanes \in Vehicle\_In \to TUNNEL\_TRAVEL\_LANE$
grd7: $newVehicleFronts = Vehicle\_Out \lhd updatedVehicleFronts$
grd8: $trafficLevel \in TRAFFIC\_LEVEL$
grd9: $(trafficLevel = NORMAL \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \geq 40))))$
grd10: $(trafficLevel = DENSE \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 35 \mathinner{..} 39))))$
grd11: $(trafficLevel = SLOWED \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 25 \mathinner{..} 34))))$
grd12: $(trafficLevel = CONGESTION \Rightarrow (((card(Vehicle\_In)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) < 15))))$
grd13: $\forall xx \cdot ((xx \in Vehicle\_In \land newVehicleFronts(xx) \in Tunnel\_part1) \Rightarrow newTravelLanes(xx) = TRAVEL\_LANE\_I)$

grd14: $\forall xx1, xx2 \cdot ((xx1 \in Vehicle\_In \wedge xx2 \in Vehicle\_In \wedge xx1 \neq xx2) \Rightarrow ((newVehicleFronts(xx1) - Vehicle\_Length(xx1)) .. newVehicleFronts(xx1) \cap (newVehicleFronts(xx2) - Vehicle\_Length(xx2)) .. newVehicleFronts(xx2) = \varnothing \vee newTravelLanes(xx1) \neq newTravelLanes(xx2)))$

then

act1: $Vehicle := Vehicle\_In$
act2: $Vehicle\_Front\_Position := newVehicleFronts$
act3: $Vehicle\_Travel\_Lane := newTravelLanes$
act4: $trafficlevel := trafficLevel$
act5: $Vehicle\_Speed := newVehicleSpeeds$
act6: $trafficReaded := FALSE$

end

Event DetermineTrafficLevel ⟨ordinary⟩ $\widehat{=}$

refines ManageCongestion

any

observedTrafficLevel
observedVehicles
observedSpeeds
observedFrontPositions
observedTravelLanes

where

grd0: $observedVehicles \subseteq Vehicle$
lecture du trafic
grd1: $Vehicle \neq \varnothing \Rightarrow observedVehicles \neq \varnothing$
grd2: $observedSpeeds = observedVehicles \lhd Vehicle\_Speed$
lecture de la vitesse des vehicules
grd3: $observedFrontPositions = observedVehicles \lhd Vehicle\_Front\_Position$
lecture du trafic
grd4: $observedTravelLanes = observedVehicles \lhd Vehicle\_Travel\_Lane$
lecture du trafic
grd5:
$observedTrafficLevel = NORMAL \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) \geq 40)))$
determination du niveau de trafic
grd6:
$observedTrafficLevel = DENSE \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) \in 35 .. 39)))$
grd7:
$observedTrafficLevel = SLOWED \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) \in 25 .. 34)))$
grd8:
$observedTrafficLevel = CONGESTION \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) < 15)))$

then

act1: $Observed\_Vehicle := observedVehicles$
act2: $Observed\_Vehicle\_Speed := observedSpeeds$
act3: $Observed\_Vehicle\_Front\_Position := observedFrontPositions$
act4: $Observed\_Vehicle\_Travel\_Lane := observedTravelLanes$
act5: $observed\_traffic\_level := observedTrafficLevel$
act6: $trafficReaded :\in BOOL$

end

Event RegulateTrafficLevel ⟨ordinary⟩ $\widehat{=}$

refines ManageCongestion

begin

skip

end

Event SuperviseTrafficLevel ⟨ordinary⟩ $\widehat{=}$
refines ManageCongestion
begin
skip
end
END

MACHINE bonaventure_3_mch
REFINES bonaventure_2_mch
SEES bonaventure_3_ctxt
VARIABLES

trafficReaded
Vehicle
Vehicle_Front_Position
Vehicle_Travel_Lane
Speed_Limit
Min_Brake_Distance
traffic_level
Vehicle_Speed
Observed_Vehicle
Observed_Vehicle_Speed
Observed_Vehicle_Front_Position
Observed_Vehicle_Travel_Lane
observed_traffic_level
operating_mode
Traffic_Signal_Program
Sensor_Observed_Traffic_Level
Sensor_Observed_Vehicle
Sensor_Observed_Vehicle_Speed
Is_Sensor_Detection_Available
tsc_observed_traffic_level
trafficReadedCGMU
trafficReadedCIGC

INVARIANTS

inv1: $operating\_mode \in OPERATING\_MODE$
inv2: $Traffic\_Signal\_Program \in Traffic\_Light\_Color \to \mathbb{N}$
inv3: $Sensor\_Observed\_Traffic\_Level \in Sensor \nrightarrow TRAFFIC\_LEVEL$
inv4: $Sensor\_Observed\_Vehicle \in Sensor \leftrightarrow VEHICLE$
inv4_1: $trafficReaded = TRUE \Rightarrow Sensor\_Observed\_Vehicle \in Sensor \leftrightarrow Observed\_Vehicle$
inv5: $\forall xx \cdot (xx \in Observed\_Vehicle \Rightarrow card(Sensor\_Observed\_Vehicle^{-1}[\{xx\}]) \geq 1)$
inv6: $Sensor\_Observed\_Vehicle\_Speed \in Sensor\_Observed\_Vehicle \to \mathbb{N}$
inv7: $Is\_Sensor\_Detection\_Available \in Sensor \to BOOL$
inv8: $tsc\_observed\_traffic\_level \in TRAFFIC\_LEVEL$
inv9: $Observed\_Vehicle = ran(Sensor\_Observed\_Vehicle)$
inv10: $trafficReadedCGMU \in BOOL$
inv11: $trafficReadedCIGC \in BOOL$
inv12: $trafficReadedCGMU = TRUE \wedge trafficReadedCIGC = TRUE \Rightarrow trafficReaded = TRUE$
p3_2: $(operating\_mode = NORMAL\_MODE \wedge trafficReadedCIGC = TRUE) \Rightarrow (AID \in dom(Sensor\_Observed\_Traffi$
$observed\_traffic\_level = Sensor\_Observed\_Traffic\_Level(AID))$
p3_3:
$(operating\_mode \in \{DEGRADED\_MODE\_I, DEGRADED\_MODE\_II\} \wedge trafficReadedCGMU = TRUE)$
$\Rightarrow (Sensor\_Observed\_Traffic\_Level[VdM\_Sensor] \neq \varnothing$
$\wedge\ observed\_traffic\_level \in Sensor\_Observed\_Traffic\_Level[VdM\_Sensor])$
p3_4: $operating\_mode = NORMAL\_MODE \Rightarrow Is\_Sensor\_Detection\_Available(AID) = TRUE$
p3_5:
$(operating\_mode \in \{DEGRADED\_MODE\_I, DEGRADED\_MODE\_II\}$
$\Rightarrow Is\_Sensor\_Detection\_Available(AID) = FALSE)$

p3_6:
$\forall xx \cdot (xx \in dom(Sensor\_Observed\_Traffic\_Level) \land Sensor\_Observed\_Traffic\_Level(xx) = NORMAL \Rightarrow (((card(Sensor\_Observed\_Vehicle[\{xx\}]) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall yy \cdot (yy \in Sensor\_Observed\_Vehicle[\{xx\}] \Rightarrow Sensor\_Observed\_Vehicle\_Speed(xx \mapsto yy) \geq 40))))$

p3_7:
$\forall xx \cdot (xx \in dom(Sensor\_Observed\_Traffic\_Level) \land Sensor\_Observed\_Traffic\_Level(xx) = DENSE \Rightarrow (((card(Sensor\_Observed\_Vehicle[\{xx\}]) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall yy \cdot (yy \in Sensor\_Observed\_Vehicle[\{xx\}] \Rightarrow Sensor\_Observed\_Vehicle\_Speed(xx \mapsto yy) \in 35 .. 39))))$

p3_8:
$\forall xx \cdot (xx \in dom(Sensor\_Observed\_Traffic\_Level) \land Sensor\_Observed\_Traffic\_Level(xx) = SLOWED \Rightarrow (((card(Sensor\_Observed\_Vehicle[\{xx\}]) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall yy \cdot (yy \in Sensor\_Observed\_Vehicle[\{xx\}] \Rightarrow Sensor\_Observed\_Vehicle\_Speed(xx \mapsto yy) \in 25 .. 34))))$

p3_9:
$\forall xx \cdot (xx \in dom(Sensor\_Observed\_Traffic\_Level) \land Sensor\_Observed\_Traffic\_Level(xx) = CONGESTION \Rightarrow (((card(Sensor\_Observed\_Vehicle[\{xx\}]) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall yy \cdot (yy \in Sensor\_Observed\_Vehicle[\{xx\}] \Rightarrow Sensor\_Observed\_Vehicle\_Speed(xx \mapsto yy) < 15))))$

p3_10: $trafficReadedCGMU = TRUE \Rightarrow ((VdM\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRUE\}]) \lhd Sensor\_Observed\_Vehicle \in VdM\_Sensor \leftrightarrow Vehicle$

p3_11: $trafficReadedCIGC = TRUE \Rightarrow ((MtQ\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRUE\}]) \lhd Sensor\_Observed\_Vehicle \in MtQ\_Sensor \leftrightarrow Vehicle$

p3_12: $\forall xx, yy \cdot ((xx \in dom(Sensor\_Observed\_Traffic\_Level) \cap ((VdM\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRU$
$yy \in Sensor\_Observed\_Vehicle[\{xx\}] \land trafficReadedCGMU = TRUE) \Rightarrow (Vehicle\_Front\_Position(yy) - Vehicle\_Length(yy)) .. Vehicle\_Front\_Position(yy) \cap Sensor\_Coverage\_Rear(xx) .. Sensor\_Coverage\_Front(xx) \neq \varnothing)$

p3_13: $\forall xx, yy \cdot ((xx \in dom(Sensor\_Observed\_Traffic\_Level) \cap ((MtQ\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRU$
$yy \in Sensor\_Observed\_Vehicle[\{xx\}] \land trafficReadedCIGC = TRUE) \Rightarrow (Vehicle\_Front\_Position(yy) - Vehicle\_Length(yy)) .. Vehicle\_Front\_Position(yy) \cap Sensor\_Coverage\_Rear(xx) .. Sensor\_Coverage\_Front(xx) \neq \varnothing)$

p3_14: $\forall xx, yy \cdot ((xx \in dom(Sensor\_Observed\_Traffic\_Level) \cap (Is\_Sensor\_Detection\_Available^{-1}[\{TRUE\}]) \land yy \in Sensor\_Observed\_Vehicle[\{xx\}] \land trafficReaded = TRUE) \Rightarrow (Vehicle\_Front\_Position(yy) - Vehicle\_Length(yy)) .. Vehicle\_Front\_Position(yy) \cap Sensor\_Coverage\_Rear(xx) .. Sensor\_Coverage\_Front(xx) \neq \varnothing)$

EVENTS

Initialisation ⟨extended⟩

begin

act1: $Vehicle := \varnothing$
act2: $Vehicle\_Front\_Position := \varnothing$
act3: $Vehicle\_Travel\_Lane := \varnothing$
act4: $Speed\_Limit := Tunnel \times \{70\}$
act5: $Min\_Brake\_Distance := \{70 \mapsto 0\}$
act7: $traffic\_level := NORMAL$
act8: $Vehicle\_Speed := \varnothing$
act9: $Observed\_Vehicle := \varnothing$
act10: $Observed\_Vehicle\_Speed := \varnothing$
act11: $Observed\_Vehicle\_Front\_Position := \varnothing$
act12: $Observed\_Vehicle\_Travel\_Lane := \varnothing$
act13: $observed\_traffic\_level := NORMAL$
act14: $trafficReaded := FALSE$
act15: $operating\_mode := NORMAL\_MODE$
act16: $Traffic\_Signal\_Program := Traffic\_Light\_Color \times \{10\}$
act17: $Sensor\_Observed\_Traffic\_Level := Sensor \times \{NORMAL\}$
act18: $Sensor\_Observed\_Vehicle := \varnothing$

act19: $Sensor\_Observed\_Vehicle\_Speed := \varnothing$
act20: $Is\_Sensor\_Detection\_Available := Sensor \times \{TRUE\}$
act21: $tsc\_observed\_traffic\_level := NORMAL$
act22: $trafficReadedCGMU := FALSE$
act23: $trafficReadedCIGC := FALSE$

end

Event ctrl_BringVehicleInsideTunnel ⟨ordinary⟩ $\widehat{=}$
extends ctrl_BringVehicleInsideTunnel

any
vehicle
front
travelLane
speed
trafficLevel

where
grd1: $vehicle \in VEHICLE \setminus Vehicle$
grd2: $front \in Tunnel$
grd3: $travelLane \in TUNNEL\_TRAVEL\_LANE$
grd4: $front \in Tunnel\_part1 \Rightarrow travelLane = TRAVEL\_LANE\_I$
grd5: $\forall xx \cdot (xx \in Vehicle \Rightarrow ((Vehicle\_Front\_Position(xx) - Vehicle\_Length(xx)) .. Vehicle\_Front\_Position(xx) \cap (front - Vehicle\_Length(vehicle)) .. front = \varnothing \vee Vehicle\_Travel\_Lane(xx) \neq travelLane))$
grd6: $speed \in 0 .. Speed\_Limit(front)$
grd7: $trafficLevel \in TRAFFIC\_LEVEL$
grd8: $trafficLevel = NORMAL \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \geq 40 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \geq 40)))$
grd9: $trafficLevel = DENSE \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \in 35 .. 39 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 35 .. 39)))$
grd10: $trafficLevel = SLOWED \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed \in 25 .. 34 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) \in 25 .. 34)))$
grd11: $trafficLevel = CONGESTION \Rightarrow ((((card(Vehicle)+1)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \wedge speed < 15 \wedge (\forall xx \cdot (xx \in Vehicle \Rightarrow Vehicle\_Speed(xx) < 15)))$

then
act1: $Vehicle := Vehicle \cup \{vehicle\}$
act2: $Vehicle\_Front\_Position(vehicle) := front$
act3: $Vehicle\_Travel\_Lane(vehicle) := travelLane$
act4: $Vehicle\_Speed(vehicle) := speed$
act5: $traffic\_level := trafficLevel$
act6: $trafficReaded := FALSE$
act7: $trafficReadedCGMU := FALSE$
act8: $trafficReadedCIGC := FALSE$

end

Event ctrl_ChangeSpeed ⟨ordinary⟩ $\widehat{=}$
extends ctrl_ChangeSpeed

any
vehicle
speed
trafficLevel

where
grd1: $vehicle \in Vehicle$
grd2: $speed \in 0 .. Speed\_Limit(Vehicle\_Front\_Position(vehicle)) \setminus \{Vehicle\_Speed(vehicle)\}$
grd3: $trafficLevel \in TRAFFIC\_LEVEL$
grd4: $trafficLevel = NORMAL \Rightarrow (((card(Vehicle)*100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \wedge speed \geq 40 \wedge (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \geq 40)))$

grd5:
$traffic Level = DENSE \Rightarrow (((card(Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land speed \in 35 \mathinner{..} 39 \land (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \in 35 \mathinner{..} 39)))$
grd6:
$traffic Level = SLOWED \Rightarrow (((card(Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land speed \in 25 \mathinner{..} 34 \land (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) \in 25 \mathinner{..} 34)))$
grd7:
$traffic Level = CONGESTION \Rightarrow (((card(Vehicle) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land speed < 15 \land (\forall xx \cdot (xx \in Vehicle \setminus \{vehicle\} \Rightarrow Vehicle\_Speed(xx) < 15)))$

then

act1: $Vehicle\_Speed(vehicle) := speed$
act2: $traffic\_level := traffic Level$

end

Event MoveVehicle ⟨ordinary⟩ $\widehat{=}$
extends MoveVehicle

any

$delay$
$newTravelLanes$
$updatedVehicleFronts$
$newVehicleSpeeds$
$Vehicle\_Out$
$Vehicle\_In$
$trafficLevel$
$newVehicleFronts$

where

grd0: $delay \in \mathbb{N}_1$
grd01: $Vehicle \neq \varnothing$
grd1: $updatedVehicleFronts = (\lambda xx \cdot xx \in Vehicle | Vehicle\_Front\_Position(xx) + Vehicle\_Speed(xx) * delay)$
les prouveurs ont beaucoup de mal avec ce type de definition: il est necessaire a chaque fois d'expliciter le resultat ou de donner le superset dans le cas de la cardinalite
grd2: $Vehicle\_In = updatedVehicleFronts^{-1}[Tunnel]$
grd3: $Vehicle\_Out = Vehicle \setminus Vehicle\_In$
grd4: $newVehicleSpeeds \in Vehicle\_In \to \mathbb{N}$
grd5: $\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 0 \mathinner{..} Speed\_Limit(updatedVehicleFronts(xx)))$

grd6: $newTravelLanes \in Vehicle\_In \to TUNNEL\_TRAVEL\_LANE$
grd7: $newVehicleFronts = Vehicle\_Out \lhd updatedVehicleFronts$
grd8: $traffic Level \in TRAFFIC\_LEVEL$
grd9:
$(traffic Level = NORMAL \Rightarrow (((card(Vehicle\_In) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \geq 40))))$
grd10:
$(traffic Level = DENSE \Rightarrow (((card(Vehicle\_In) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 35 \mathinner{..} 39))))$
grd11:
$(traffic Level = SLOWED \Rightarrow (((card(Vehicle\_In) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) \in 25 \mathinner{..} 34))))$
grd12:
$(traffic Level = CONGESTION \Rightarrow (((card(Vehicle\_In) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall xx \cdot (xx \in Vehicle\_In \Rightarrow newVehicleSpeeds(xx) < 15))))$
grd13: $\forall xx \cdot ((xx \in Vehicle\_In \land newVehicleFronts(xx) \in Tunnel\_part1) \Rightarrow newTravelLanes(xx) = TRAVEL\_LANE\_I)$
grd14: $\forall xx1, xx2 \cdot ((xx1 \in Vehicle\_In \land xx2 \in Vehicle\_In \land xx1 \neq xx2) \Rightarrow ((newVehicleFronts(xx1) - Vehicle\_Length(xx1)) \mathinner{..} newVehicleFronts(xx1) \cap (newVehicleFronts(xx2) - Vehicle\_Length(xx2)) \mathinner{..} newVehicleFronts(xx2) = \varnothing \lor newTravelLanes(xx1) \neq newTravelLanes(xx2)))$

then

act1: $Vehicle := Vehicle\_In$
act2: $Vehicle\_Front\_Position := newVehicleFronts$

act3: $Vehicle\_Travel\_Lane := newTravelLanes$
act4: $traffic\_level := trafficLevel$
act5: $Vehicle\_Speed := newVehicleSpeeds$
act6: $trafficReaded := FALSE$
act7: $trafficReadedCGMU := FALSE$
act8: $trafficReadedCIGC := FALSE$

end

Event DetermineTrafficLevelFromVdMSensors ⟨ordinary⟩ $\widehat{=}$

refines DetermineTrafficLevel

any

observedTrafficLevel
observedVehicles
observedSpeeds
observedFrontPositions
observedTravelLanes
vdmSensors
sensorObservedVehicles
sensorObservedVehicleSpeeds
sensorObservedTrafficLevels

where

grd0: $vdmSensors = (VdM\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRUE\}]$
grd0_1: $vdmSensors \neq \varnothing$
grd0_2: $operating\_mode \in \{DEGRADED\_MODE\_I, DEGRADED\_MODE\_II\}$
grd1: $sensorObservedVehicles \subseteq vdmSensors \times Vehicle$
theo1: ⟨theorem⟩ $finite(sensorObservedVehicles)$
grd2: $Vehicle \neq \varnothing \Rightarrow sensorObservedVehicles \neq \varnothing$
grd3:
$\forall xx, yy \cdot (xx \in dom(sensorObservedVehicles) \land yy \in sensorObservedVehicles[\{xx\}]$
$\Rightarrow (Vehicle\_Front\_Position(yy) - Vehicle\_Length(yy)) \mathinner{..} Vehicle\_Front\_Position(yy)$
$\cap Sensor\_Coverage\_Rear(xx) \mathinner{..} Sensor\_Coverage\_Front(xx) \neq \varnothing)$
grd3_1: $\forall xx, yy \cdot ((xx \in vdmSensors \land yy \in Vehicle \land (Vehicle\_Front\_Position(yy) - Vehicle\_Length(yy)) \mathinner{..}$
$Vehicle\_Front\_Position(yy) \cap Sensor\_Coverage\_Rear(xx) \mathinner{..} Sensor\_Coverage\_Front(xx) \neq \varnothing) \Rightarrow$
$(xx \in dom(sensorObservedVehicles) \land yy \in sensorObservedVehicles[\{xx\}]))$
@grd4 updatedSensorObservedVehicles = (Sensor_Observed_Vehicle⩤sensorObservedVehicles)
grd4: $observedVehicles \subseteq Vehicle$
theo2: ⟨theorem⟩ $finite(observedVehicles)$
grd5: $trafficReadedCIGC = FALSE \Rightarrow observedVehicles = ran(sensorObservedVehicles)$
lecture du trafic
grd5_1: $trafficReadedCIGC = TRUE \Rightarrow observedVehicles = ran(sensorObservedVehicles) \cup$
$ran(((MtQ\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRUE\}]) \lhd Sensor\_Observed\_Vehicle)$

lecture du trafic
grd6: $sensorObservedVehicleSpeeds = (\lambda(xx \mapsto yy) \cdot (xx \mapsto yy \in sensorObservedVehicles) | Vehicle\_Speed(yy))$

grd7_0: $sensorObservedTrafficLevels \in vdmSensors \to TRAFFIC\_LEVEL$
grd7:
$\forall xx \cdot (xx \in dom(sensorObservedTrafficLevels)$
$\land sensorObservedTrafficLevels(xx) = NORMAL$
$\Rightarrow (((card(sensorObservedVehicles[\{xx\}]) * 100) / MAXIMAL\_TUNNEL\_OCCUPATION) <$
40
$\land (\forall yy \cdot (yy \in sensorObservedVehicles[\{xx\}] \Rightarrow sensorObservedVehicleSpeeds(xx \mapsto yy) \geq$
$40))))$
grd8:
$\forall xx \cdot (xx \in dom(sensorObservedTrafficLevels)$
$\land sensorObservedTrafficLevels(xx) = DENSE$
$\Rightarrow (((card(sensorObservedVehicles[\{xx\}]) * 100) / MAXIMAL\_TUNNEL\_OCCUPATION) <$
40
$\land (\forall yy \cdot (yy \in sensorObservedVehicles[\{xx\}] \Rightarrow sensorObservedVehicleSpeeds(xx \mapsto yy) \in$
$35 \mathinner{..} 39))))$

grd9:
$\forall xx \cdot (xx \in dom(sensorObservedTrafficLevels) \land sensorObservedTrafficLevels(xx) = SLOWED \Rightarrow (((card(sensorObservedVehicles[\{xx\}]) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall yy \cdot (yy \in sensorObservedVehicles[\{xx\}] \Rightarrow sensorObservedVehicleSpeeds(xx \mapsto yy) \in 25 \mathinner{..} 34))))$

grd10:
$\forall xx \cdot (xx \in dom(sensorObservedTrafficLevels) \land sensorObservedTrafficLevels(xx) = CONGESTION \Rightarrow (((card(sensorObservedVehicles[\{xx\}]) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall yy \cdot (yy \in sensorObservedVehicles[\{xx\}] \Rightarrow sensorObservedVehicleSpeeds(xx \mapsto yy) < 15))))$

grd11: $observedSpeeds = observedVehicles \lhd Vehicle\_Speed$
lecture de la vitesse des vehicules

grd12: $observedFrontPositions = observedVehicles \lhd Vehicle\_Front\_Position$
lecture du trafic

grd13: $observedTravelLanes = observedVehicles \lhd Vehicle\_Travel\_Lane$
lecture du trafic

grd14: $observedTrafficLevel \in TRAFFIC\_LEVEL$

grd15: $observedTrafficLevel \in ran(sensorObservedTrafficLevels)$

grd16:
$observedTrafficLevel = NORMAL \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) \geq 40)))$
determination du niveau de trafic

grd17:
$observedTrafficLevel = DENSE \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) < 40 \land (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) \in 35 \mathinner{..} 39)))$

grd18:
$observedTrafficLevel = SLOWED \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) \in 25 \mathinner{..} 34)))$

grd19:
$observedTrafficLevel = CONGESTION \Rightarrow (((card(observedVehicles) * 100)/MAXIMAL\_TUNNEL\_OCCUPATION) > 40 \land (\forall xx \cdot (xx \in observedVehicles \Rightarrow observedSpeeds(xx) < 15)))$

then

act1: $Observed\_Vehicle := observedVehicles$

act2: $Observed\_Vehicle\_Speed := observedSpeeds$

act3: $Observed\_Vehicle\_Front\_Position := observedFrontPositions$

act4: $Observed\_Vehicle\_Travel\_Lane := observedTravelLanes$

act5: $observed\_traffic\_level := observedTrafficLevel$

act6: $trafficReadedCGMU := TRUE$
@act7 Sensor_Observed_Traffic_Level := Sensor_Observed_Traffic_Level⩤sensorObservedTrafficLevels

act7: $Sensor\_Observed\_Traffic\_Level := (\{TRUE \mapsto (((MtQ\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRUE$
$Sensor\_Observed\_Traffic\_Level) \cup sensorObservedTrafficLevels, FALSE \mapsto sensorObservedTrafficLevels\})($
$TRUE))$
@act8 Sensor_Observed_Vehicle := (vdmSensors⩤Sensor_Observed_Vehicle)∪ sensorObservedVehicles

act8: $Sensor\_Observed\_Vehicle := (\{TRUE \mapsto (((MtQ\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRUE\}]) \lhd$
$Sensor\_Observed\_Vehicle) \cup sensorObservedVehicles, FALSE \mapsto sensorObservedVehicles\})(bool(trafficReaded$
$TRUE))$
@act9 Sensor_Observed_Vehicle_Speed := ((vdmSensors × VEHICLE)⩤Sensor_Observed_Vehicle_Speed)∪ sensorObservedVehicleSpeeds

act9: $Sensor\_Observed\_Vehicle\_Speed := (\{TRUE \mapsto ((((MtQ\_Sensor \lhd Is\_Sensor\_Detection\_Available)^{-1}[\{TRUE$
$VEHICLE) \lhd Sensor\_Observed\_Vehicle\_Speed) \cup sensorObservedVehicleSpeeds, FALSE \mapsto$

$sensorObservedVehicleSpeeds\})(bool(trafficReadedCIGC = TRUE))$

act10: $trafficReaded := bool(trafficReadedCIGC = TRUE)$

end

Event CommunicateTrafficLeveltoTrafficSignalController ⟨ordinary⟩ $\widehat{=}$

refines RegulateTrafficLevel

any

trafficLevel

where

grd0: $trafficLevel \in Sensor\_Observed\_Traffic\_Level[VdM\_Sensor]$

then

act0: $tsc\_observed\_traffic\_level := trafficLevel$

end

Event ApplyAppropriateTrafficSignalProgram ⟨ordinary⟩ $\widehat{=}$

refines SuperviseTrafficLevel, RegulateTrafficLevel

any

trafficSignalProgram

where

grd0: $trafficSignalProgram \in Traffic\_Light\_Color \to \mathbb{N}$

a partir de la table d'association entre niveau de trafic et plan de feux, il sera possible de specifier le plan de feux correspondant a chaque etat du trafic

then

act0: $Traffic\_Signal\_Program := trafficSignalProgram$

end

Event SuperviseTrafficLevelinNormalMode ⟨ordinary⟩ $\widehat{=}$

refines SuperviseTrafficLevel

when

grd0: $operating\_mode = NORMAL\_MODE$

then

skip

end

Event SuperviseTrafficLevelinDegradedMode1 ⟨ordinary⟩ $\widehat{=}$

refines SuperviseTrafficLevel

when

grd0: $operating\_mode = DEGRADED\_MODE\_I$

then

skip

end

Event SuperviseTrafficLevelinDegradedMode2 ⟨ordinary⟩ $\widehat{=}$

refines SuperviseTrafficLevel

when

grd0: $operating\_mode = DEGRADED\_MODE\_II$

then

skip

end

END