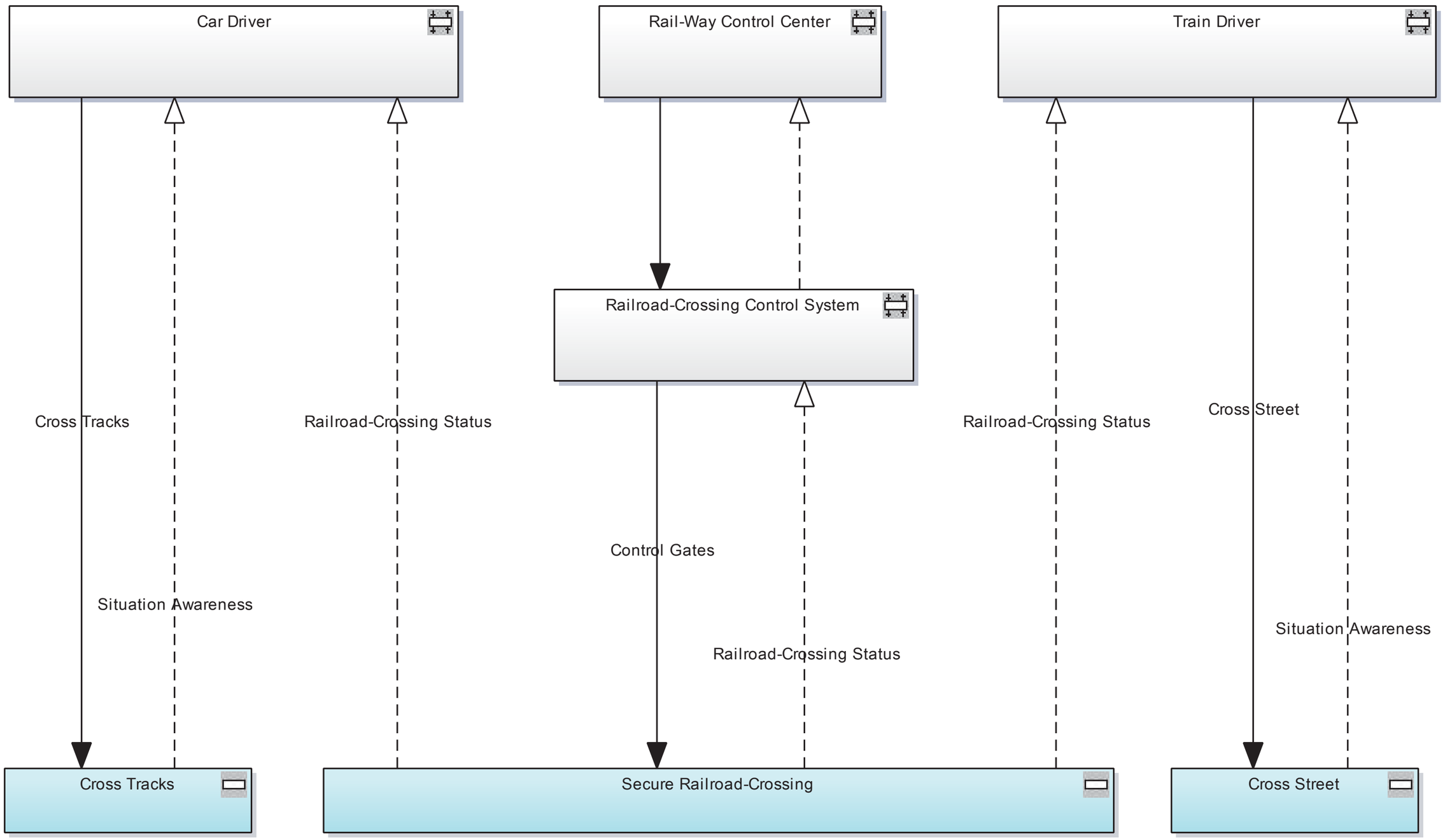
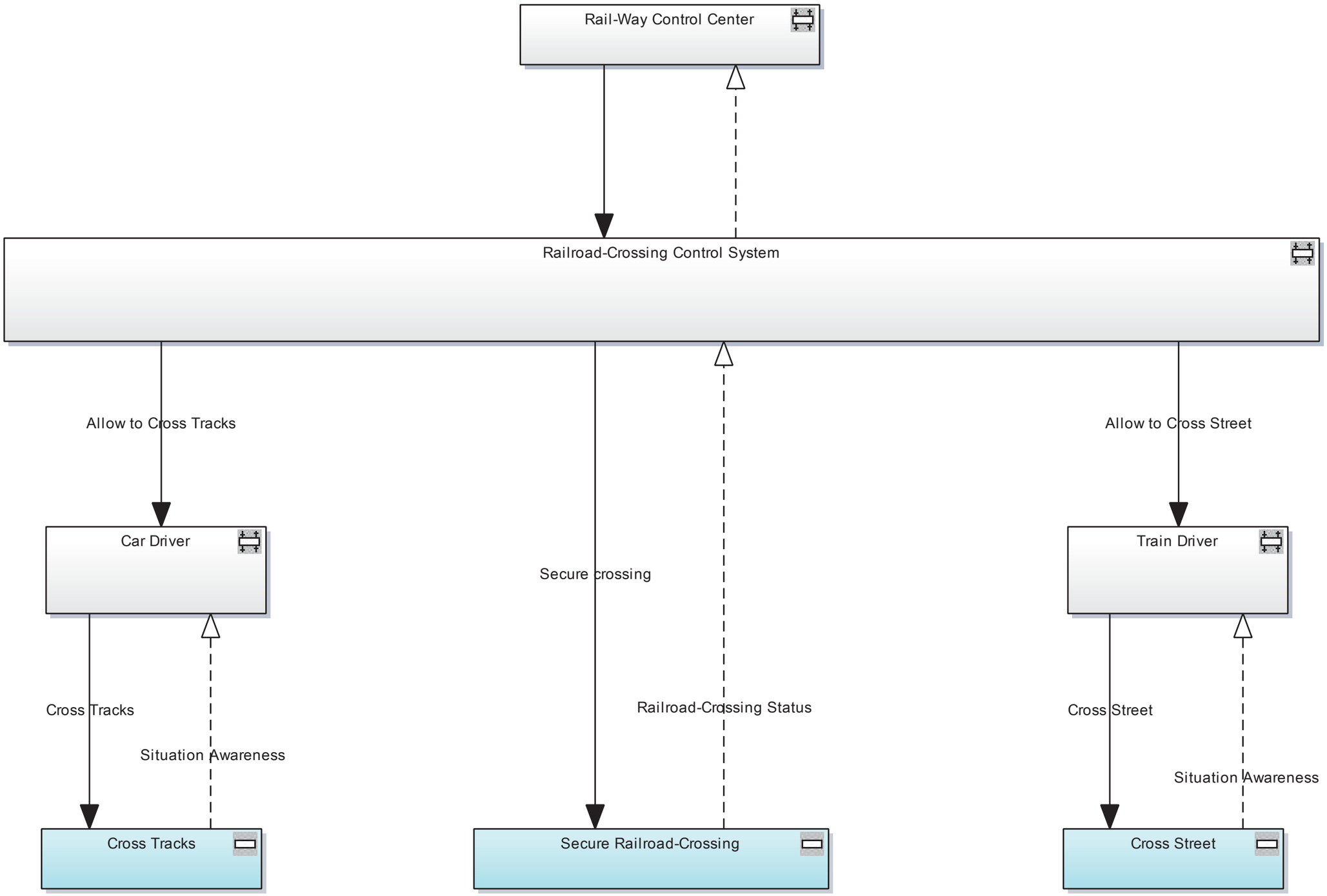
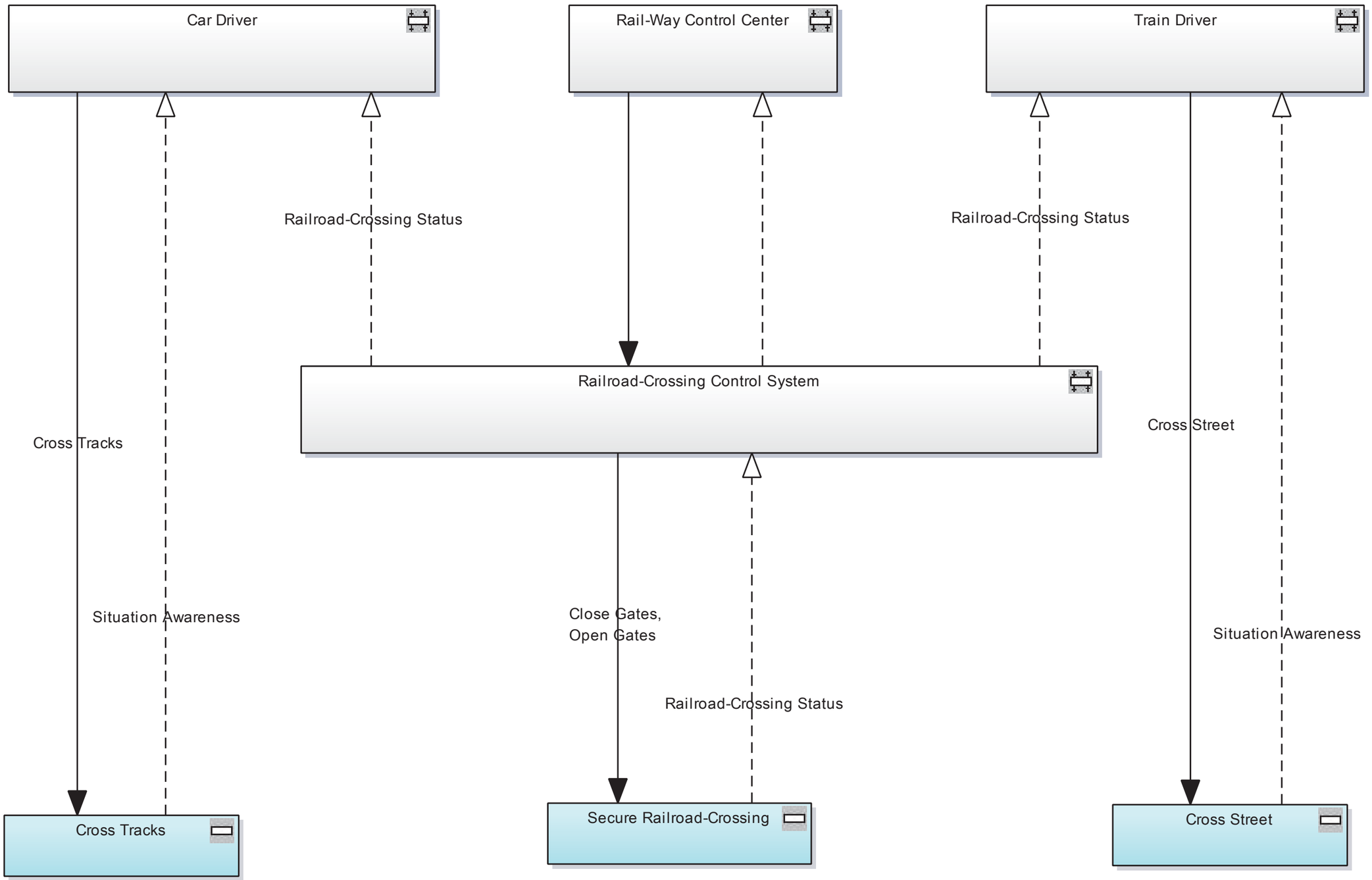
Tutorial – Hierarchical Control Structure (group activity)



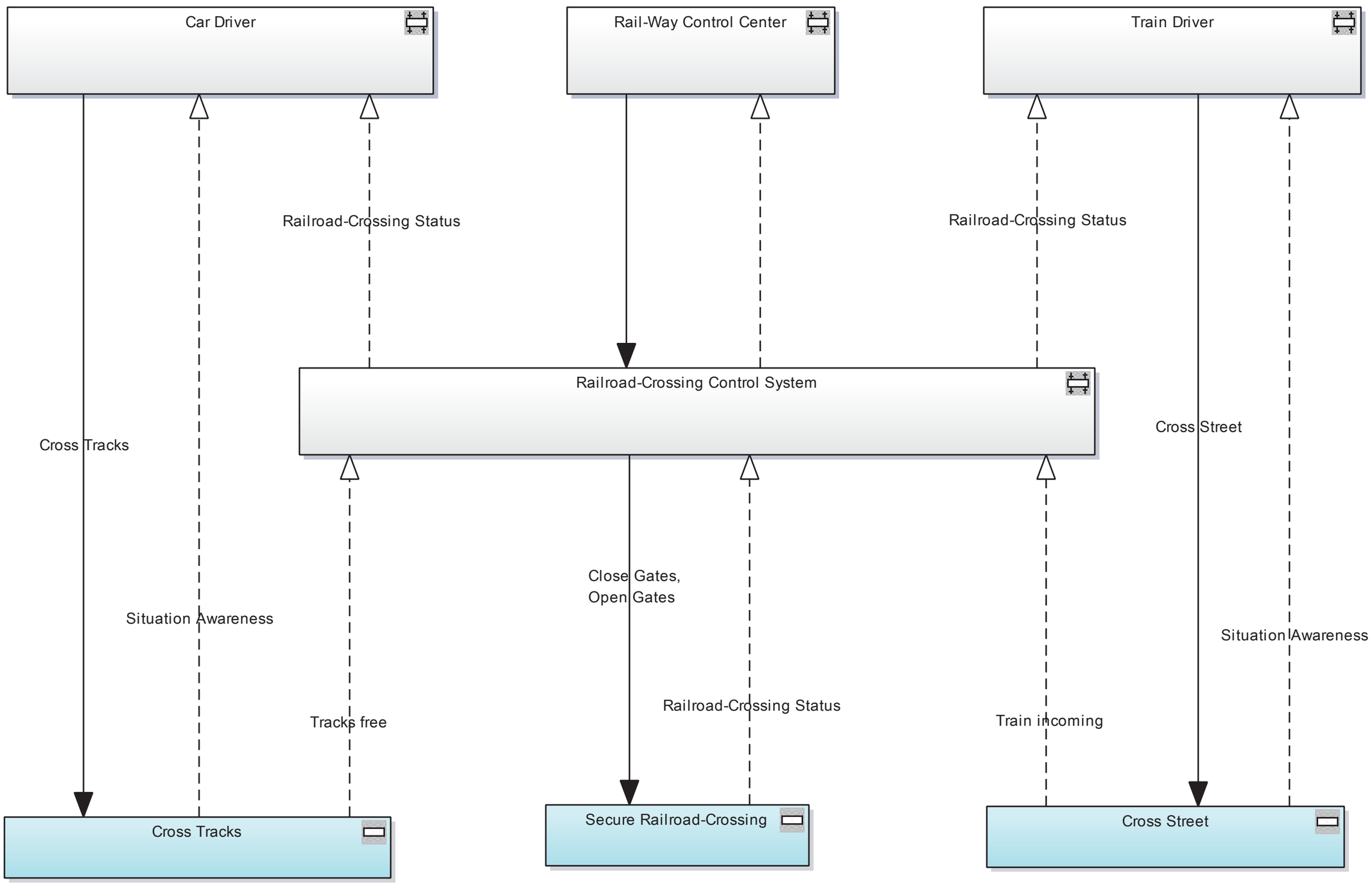
Tutorial – Hierarchical Control Structure (group activity)



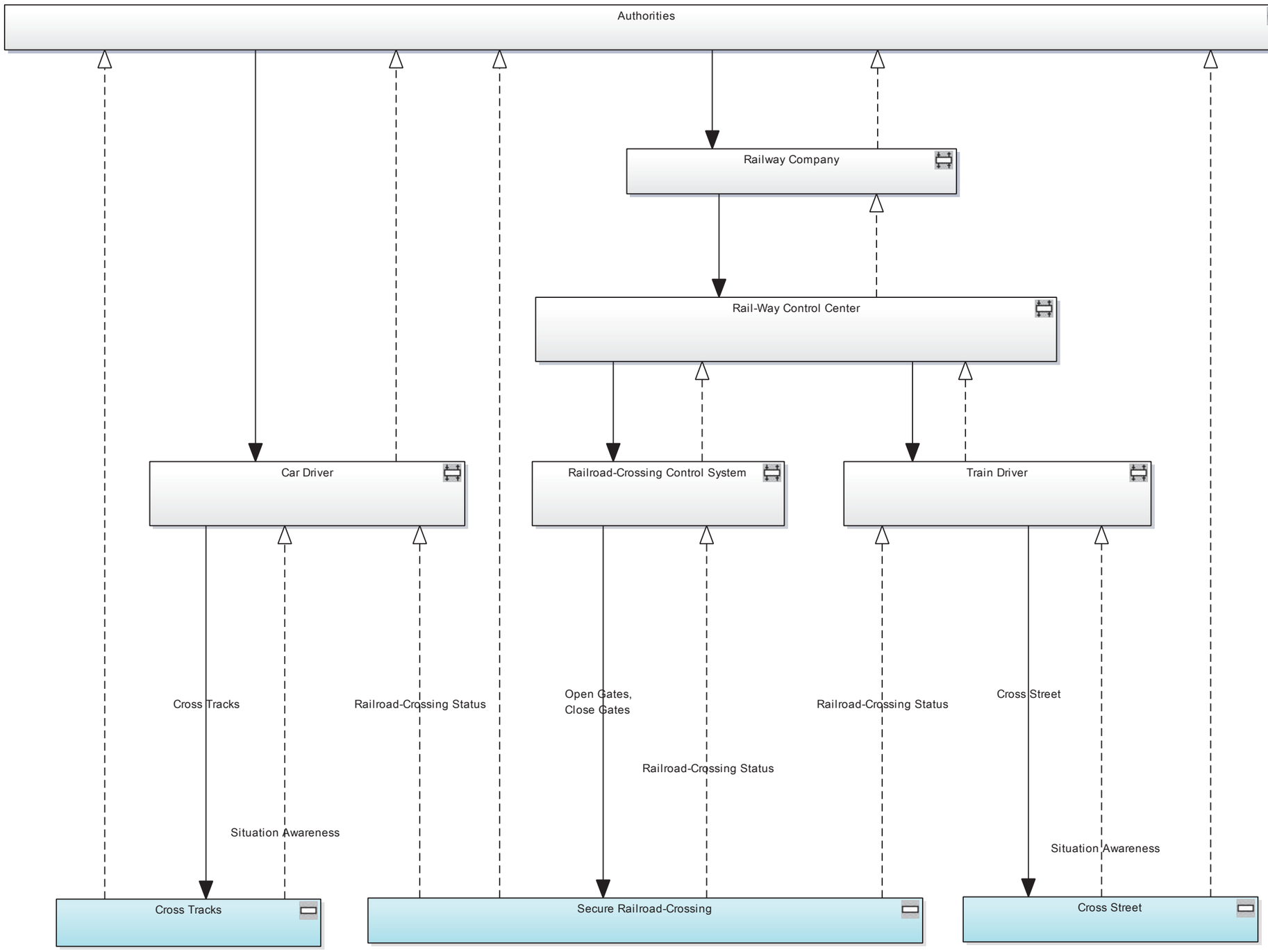
Tutorial – Hierarchical Control Structure (group activity)



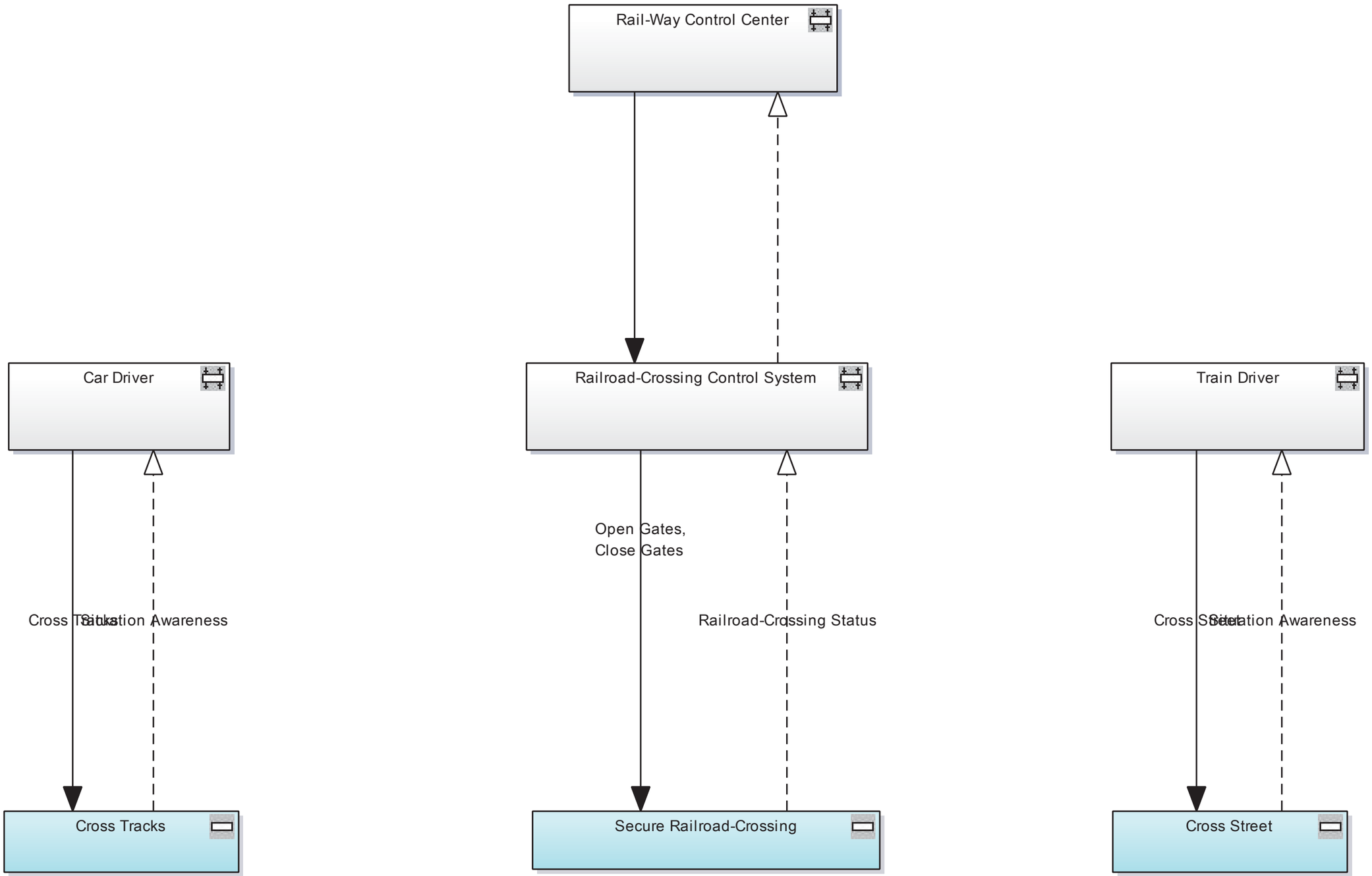
Tutorial – Hierarchical Control Structure (group activity)



Tutorial – Hierarchical Control Structure (group activity)



Tutorial – Hierarchical Control Structure (group activity)



Tutorial – STPA Step 1 Template

Control Action		Group / Page	

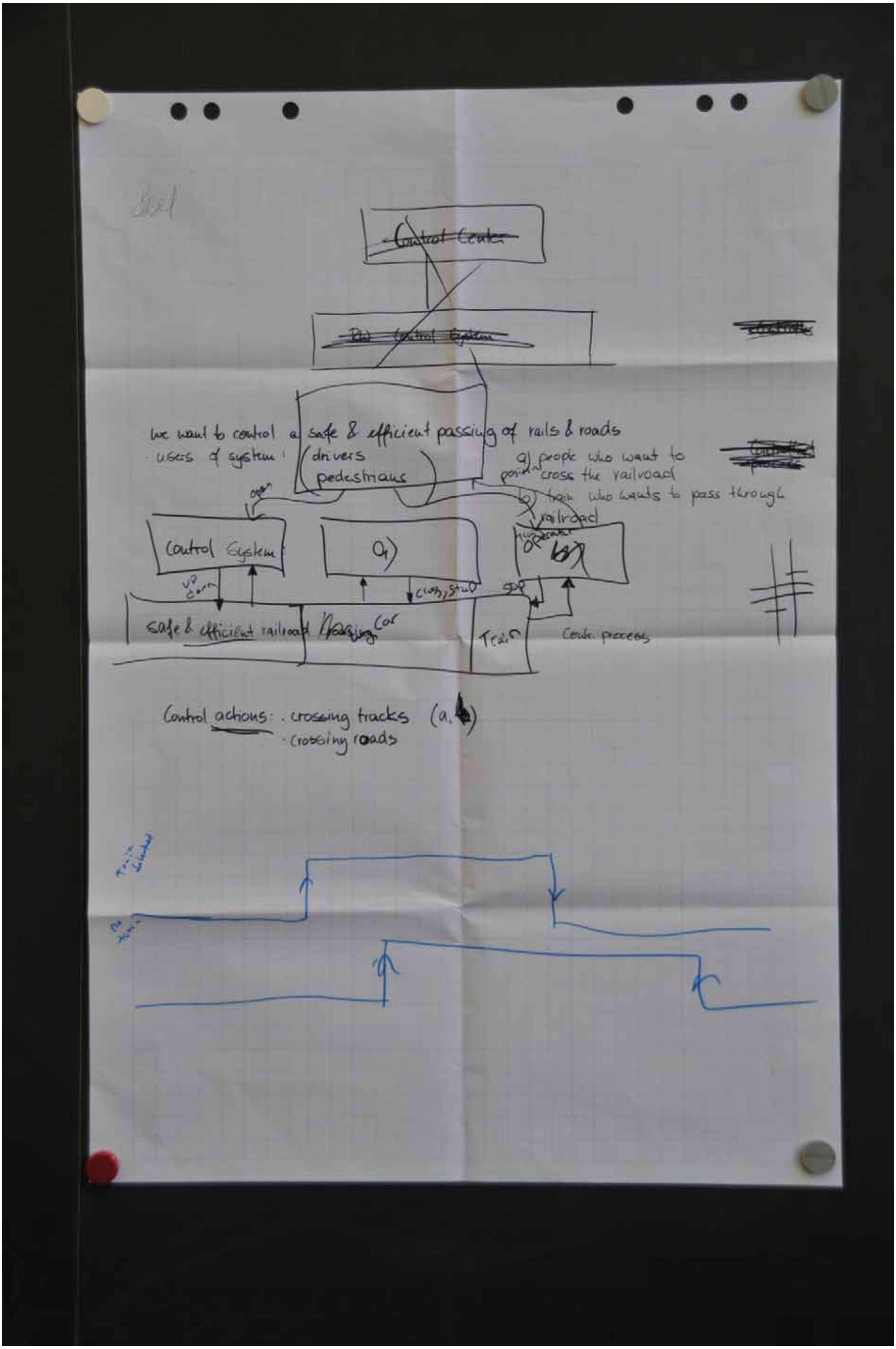
Keyword	UCA / Comments	Safety Constraints / Requirements

Tutorial – STPA Step 2 Template

UCA		Group / Page	

Control Loop Element	Scenario / Causal Factors	Safety Constraints / Requirements


Basel


Control Center
Control System
we want to control a safe & efficient passing of rails & roads
· users of system: drivers
pedestrians
a) people who want to cross the railroad
b) train who wants to pass through railroad
open
Control System
a)
b)
up
down
close, stop
stop
safe & efficient railroad
Train
Contr. process
Control actions: . crossing tracks (a.)
· crossing roads

ESW European STAMP Workshop

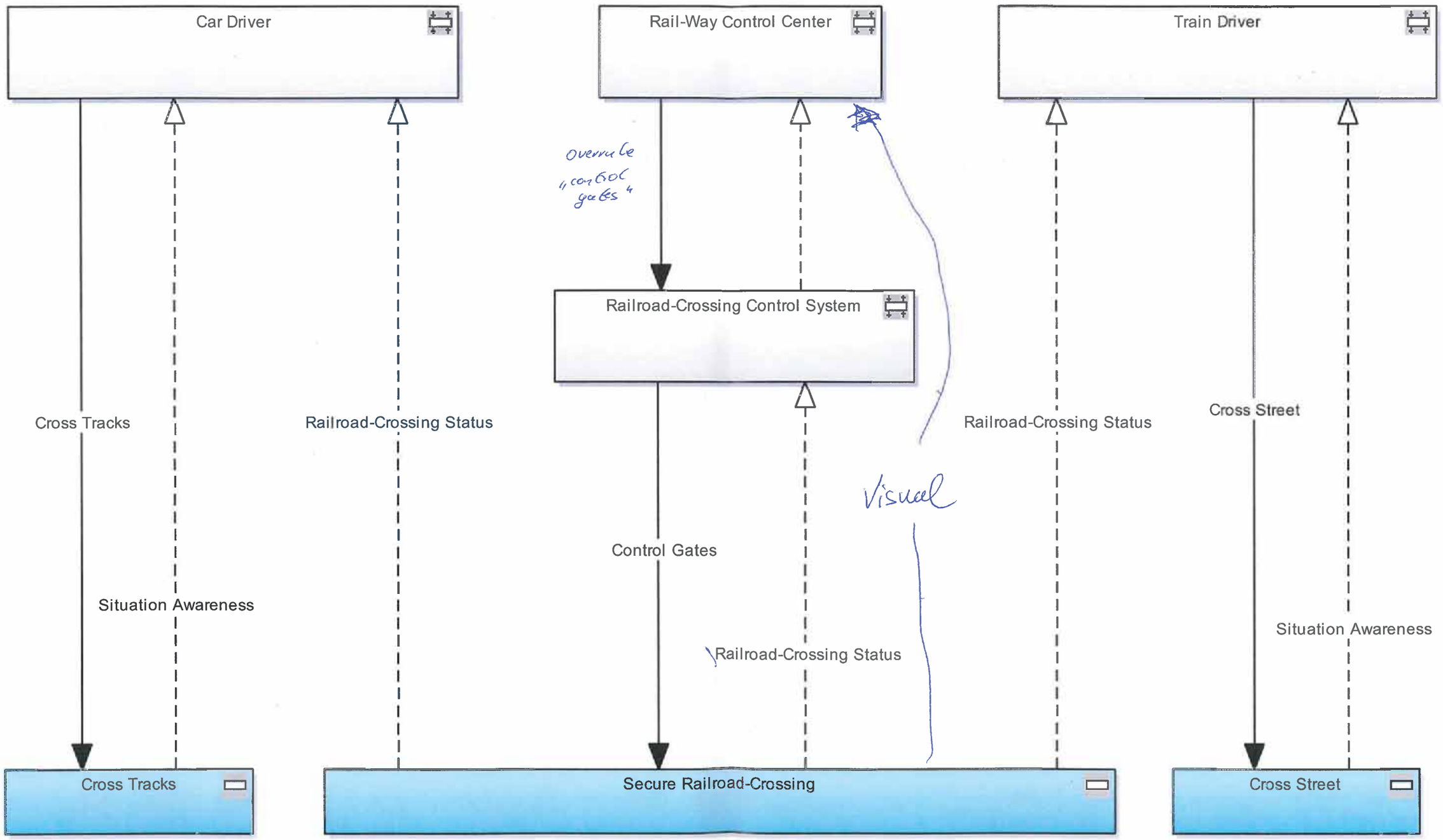
Control Action	up / down (contrd system)	Group / Page	

Keyword	UCA / Comments	Safety Constraints / Requirements
down not provided when expected	close not provided when train passes	gate shall be moved down before train approaches & stay down during passing
down open provided when not expected	if open is provided when train approaches then vehicles can go on tracks & collide	gate ~~shall~~ not be opened when train passes
down provided too early	for train no issue for cars this might be hazardous, e.g. whilst being on trains	

Basel

Tutorial – Hierarchical Control Structure (group activity)

Group Model



Tutorial – STPA Step 1 Template

ESW European STAMP Workshop

Control Action	cross tracks	Group / Page	Basel

Keyword	UCA / Comments	Safety Constraints / Requirements
Provided/too late	Hazardous if provided when train is approaching	The car Driver shall Crosses Tracks if and only if Railroad Crossing Status is secure and no train visible.
Stop too soon	Driver does not provide control Cross Tracks while on the Tracks (Car is on the tracks) He started crossing and stopped on the tracks	The Driver needs to cross the tracks to the other side. The Driver shall not intermediately stop on the track
not provided	Hazardous if not provided when train is not approaching and road is clear	The Driver needs to verify that he has clearance to get to the other side.
→ Driver stops at closed driver crosses by a second train.	gates and one train passes. After this, the tracks early (before barriers opens) in order to save time, and is hit	barriers remains closed, but
→ Gate on other side of tracks from driver closes befor the other gate and traps driver inside		


Thun

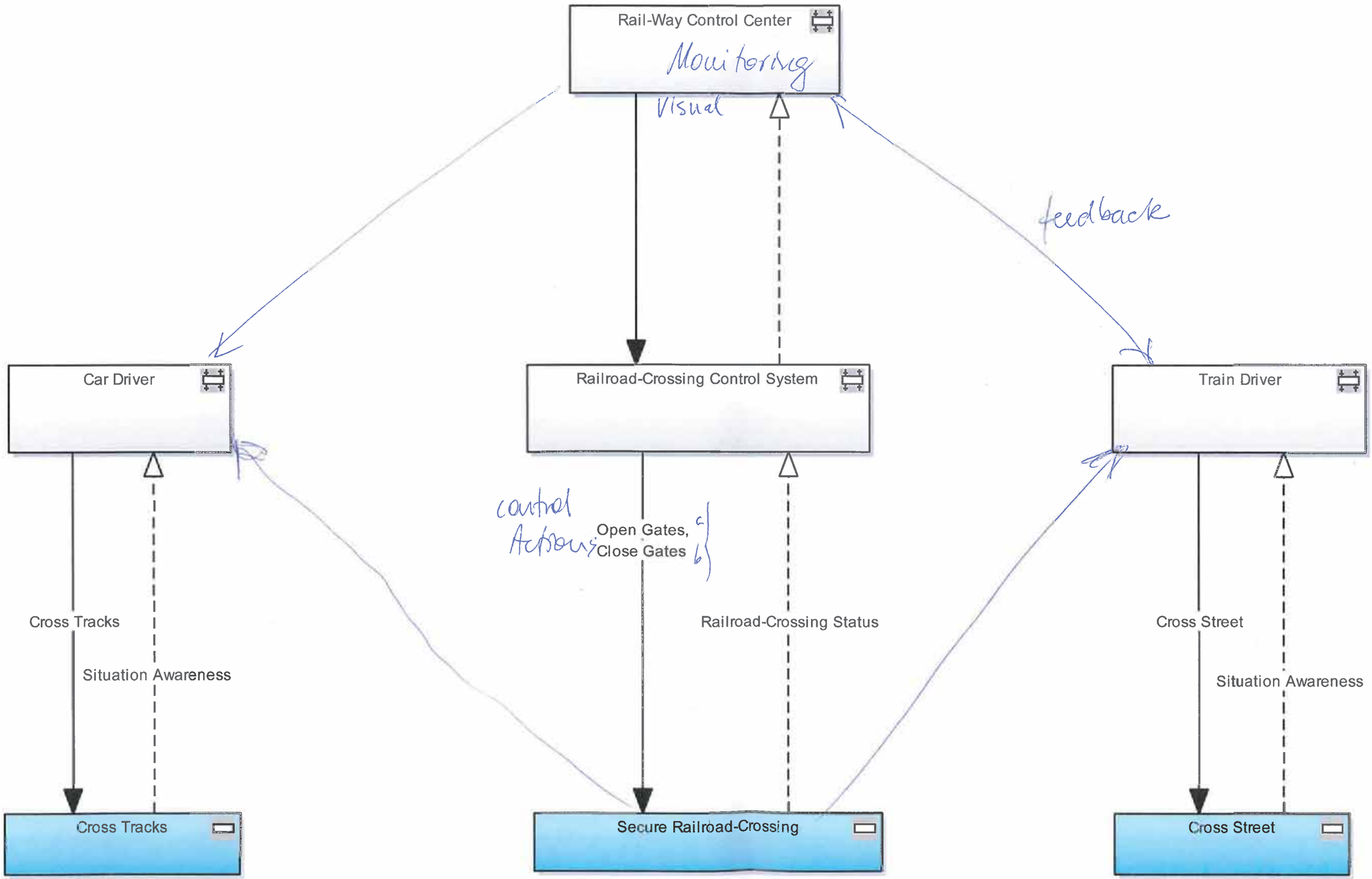
Tutorial – STPA Step 1 Template

ESW European STAMP Workshop

Control Action	~~Open Gates~~ / Close Gates	Group / Page	Thun

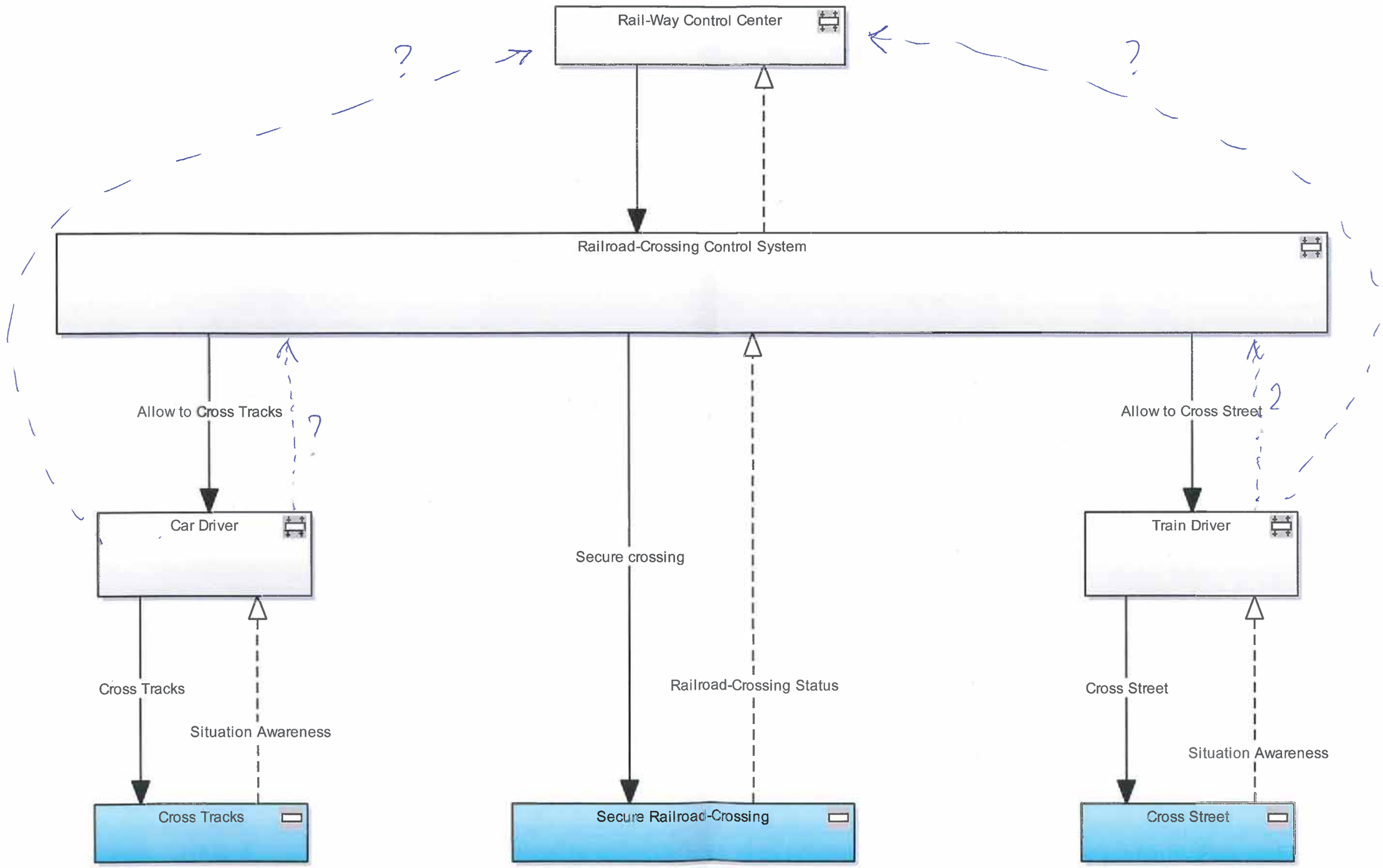
Keyword	UCA / Comments	Safety Constraints / Requirements
I not provided when expected	Gate is not closed when train is approaching lead to a Hazard	Sensor needs to inform Control System that train is approaching – Detection of incoming train
II provided when not expected	Gate B closed, but no train is coming leads to no direct Hazard unless this leads to change to peoples behav. Question of the scope of the analysis	Signal from train tracks
III provided too early	Similar to II ? How early? Needs to be defined Expectation of user?	Are red/green lights giving the same/right signals at the gates? This has to be synchronized.
IV provided too late	If Close Gate B provided too late when a train is approaching we have a Hazard. People/cars on the train tracks when train comes	What if two trains approach at the same time? a) from same side b) from opposite side
V stopped too soon	We need to define what "too soon" means Train needs to pass completly before gate opens again.	

Tutorial – Hierarchical Control Structure (group activity)

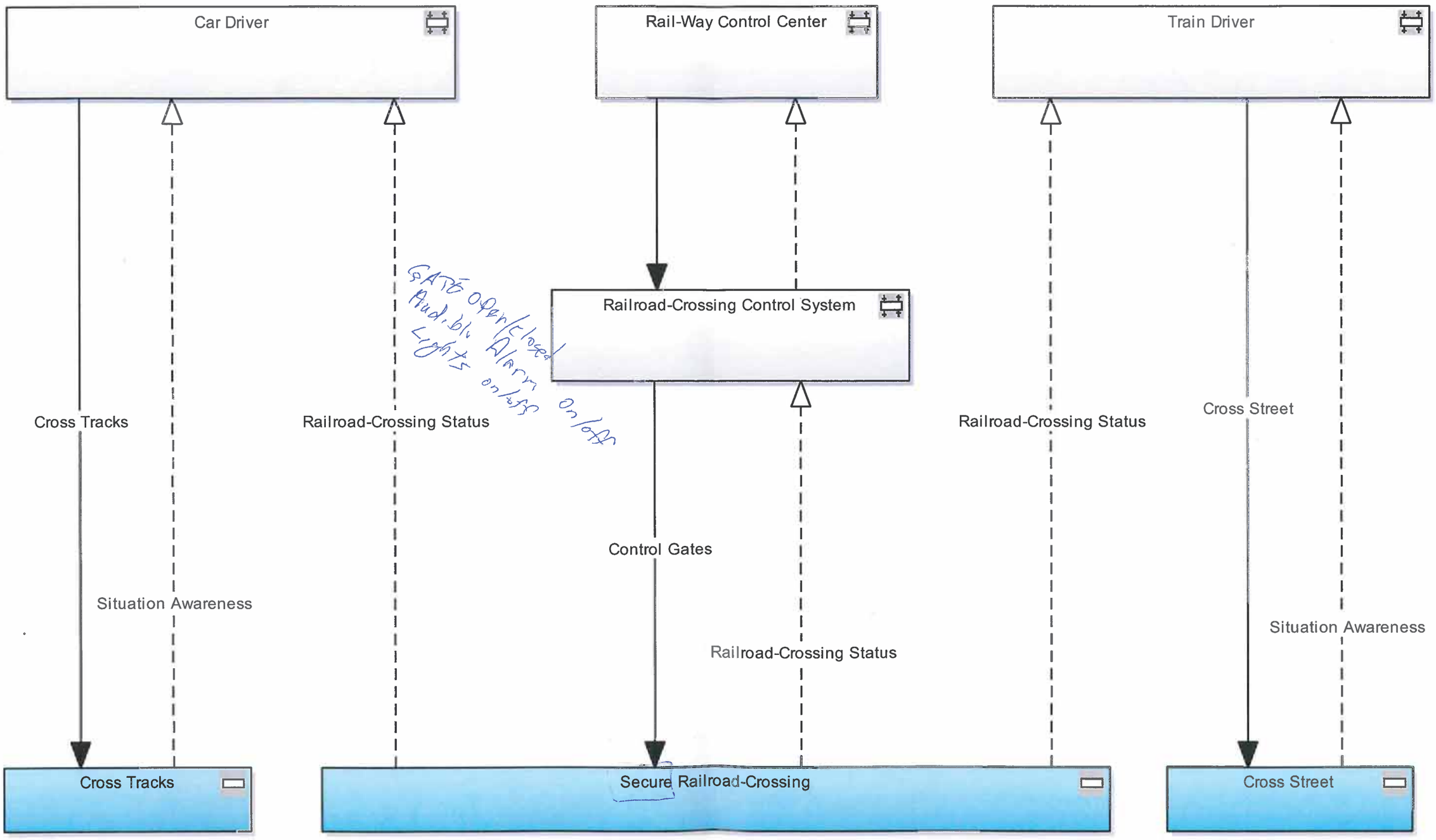


Lucerne

Tutorial – Hierarchical Control Structure (group activity)



Tutorial – Hierarchical Control Structure (group activity)

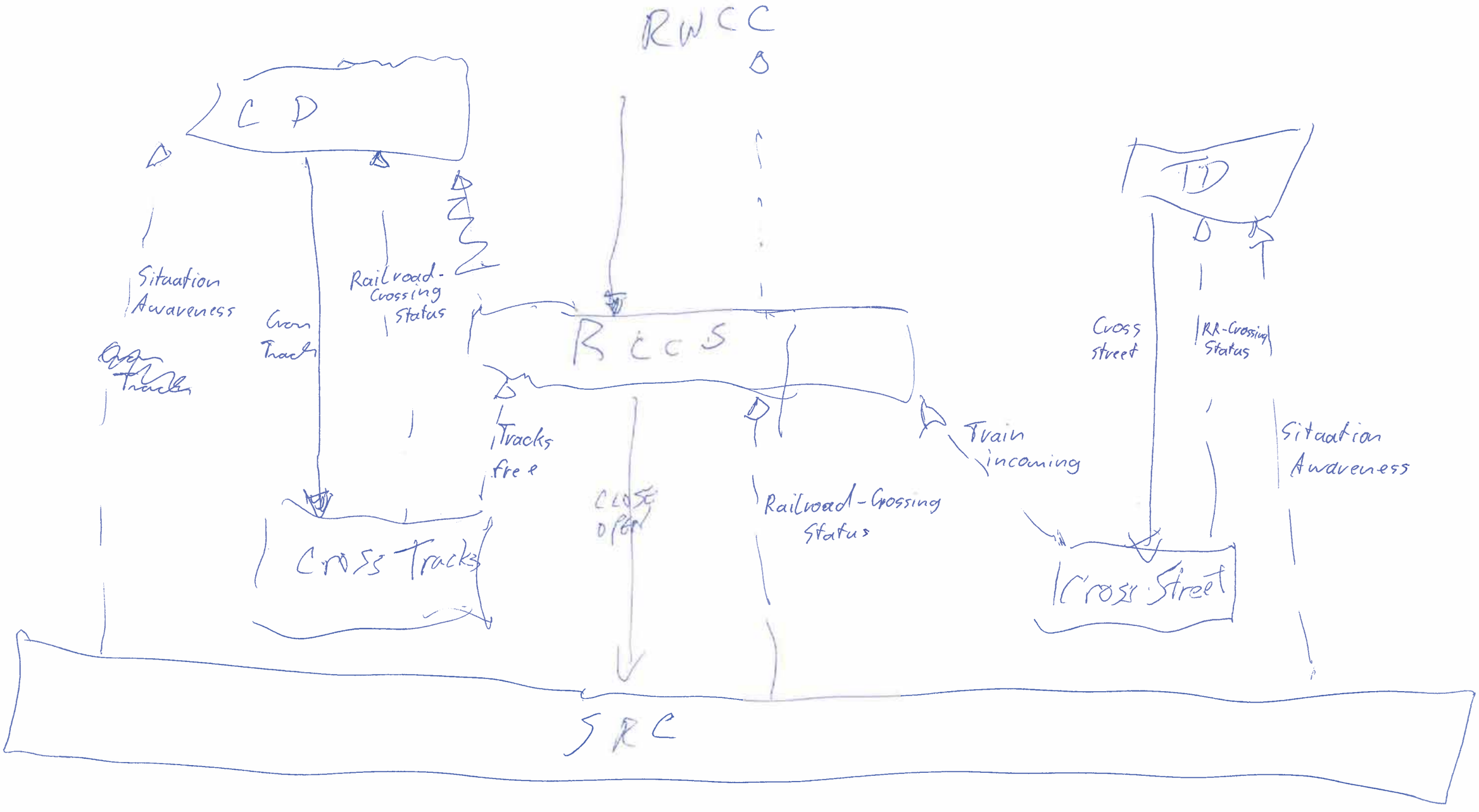


Tutorial – STPA Step 1 Template

ESW European STAMP Workshop

Control Action	Cross Tracks	Group / Page	Lucerne

Keyword	UCA / Comments	Safety Constraints / Requirements
not provided when expected	If the car driver is not provided the control action „Cross Tracks" when the	


RWCC
CD
TD
RCCS
SRC
Situation Awareness
Railroad-Crossing Status
Cross Tracks
Tracks
Tracks free
Train incoming
Railroad-Crossing Status
Cross Tracks
Cross Street
Cross street
RR-Crossing Status
Situation Awareness

Tutorial – STPA Step 2 Template

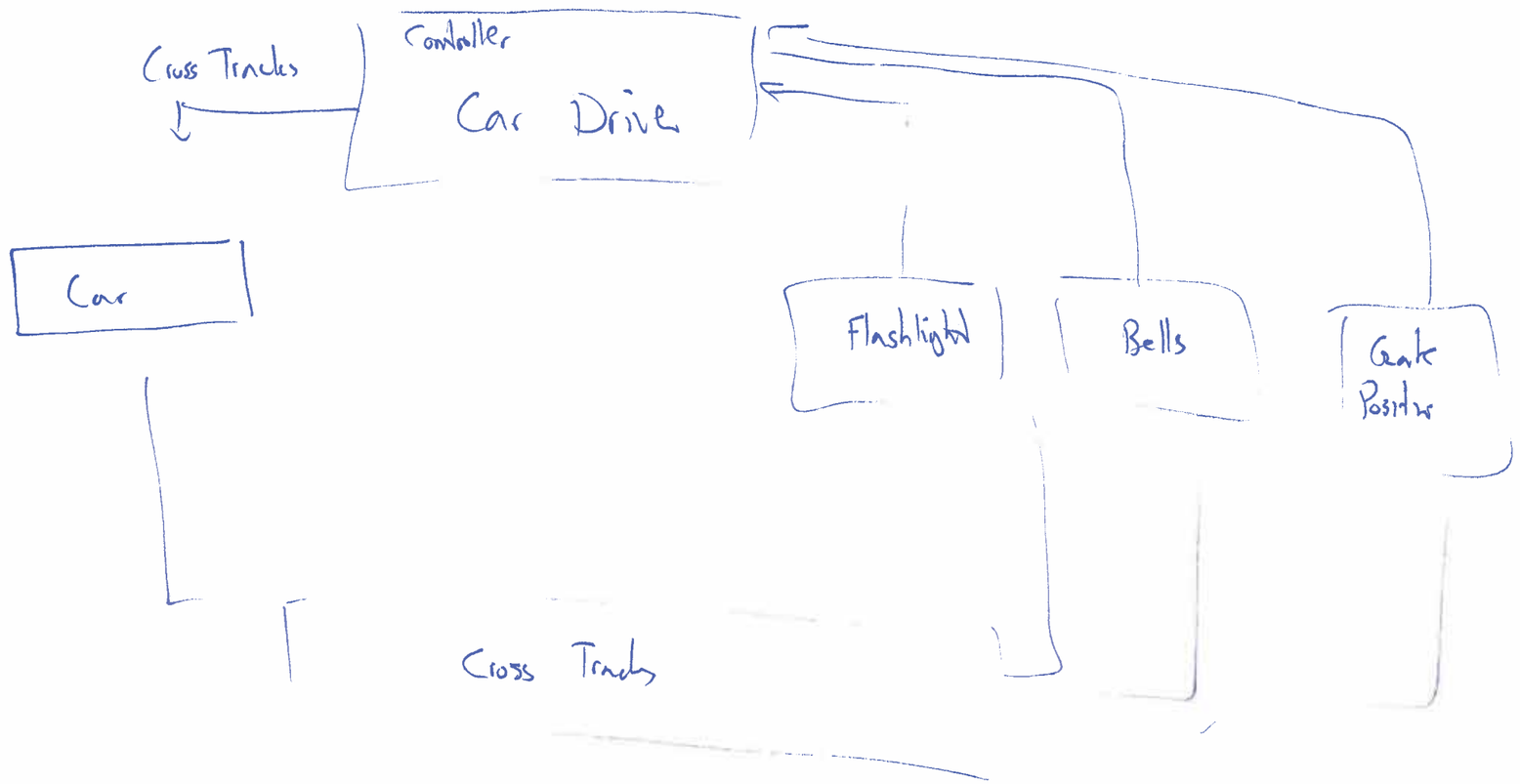
ESW European STAMP Workshop

UCA	Cross track	Group / Page	Lucerne

Control Loop Element	Scenario / Causal Factors	Safety Constraints / Requirements
NOT Provided	If cross tracks is not provided (By car driver) when train is not incoming then . . .	
Provided when not Required	if ct is provided when train incoming then could impact train	
too early	crash	
too late	ok	
too Soon	crash on track	
too Long	ok	

Locarno

Locarno


Cross Tracks
Controller
Car Drive
Car
Flashlight
Bells
Gate Positn
Cross Tracks

Tutorial – STPA Step 2 Template

ESW European STAMP Workshop

UCA		Group / Page	Locarno

Control Loop Element	Scenario / Causal Factors	Safety Constraints / Requirements
UCA1:	- Flashlight broken - Gates not closed, stay open - Driver ignores	- Automatically detect when flashlight broken

UCA	~~Cross tracks~~ Cross tracks	Group / Page	Locarno / #2

~~Control Loop Element~~ Keyword	~~Scenario / Causal Factors~~ UCA / Comments	Safety Constraints / Requirements
~~not~~ provided when unexpected (lights flashing, gates down)	Cross tracks when lights are flashing or gates are closed → possible collision = UCA 1	
provided but not completed ~~in time~~ (before ~~train~~ arrives, gate closes)	possible collision if crossing is not completed before gate closes. = UCA 2	
provided too early (before gates open again)	possible collision if crossing is provided before gate opens again	
provided too late (after gates close or are closing)	possible collision if car crosses after the gates are closed	
stopped too soon	possible collision if the car stops on the railroad track and a train is approaching	
applied too long	possible collision if the car is driving too slow across the tracks and a train is approaching before the car vacates the tracks.	

Tutorial – STPA Step 1 Template

ESW European STAMP Workshop

Control Action	Cross street	Group / Page	Locarno 13

Keyword	UCA / Comments	Safety Constraints / Requirements
not provided when expected / required provided when not expected.	.... If ~~close gate~~ is provide and ~~people~~ obstacle still on the track	

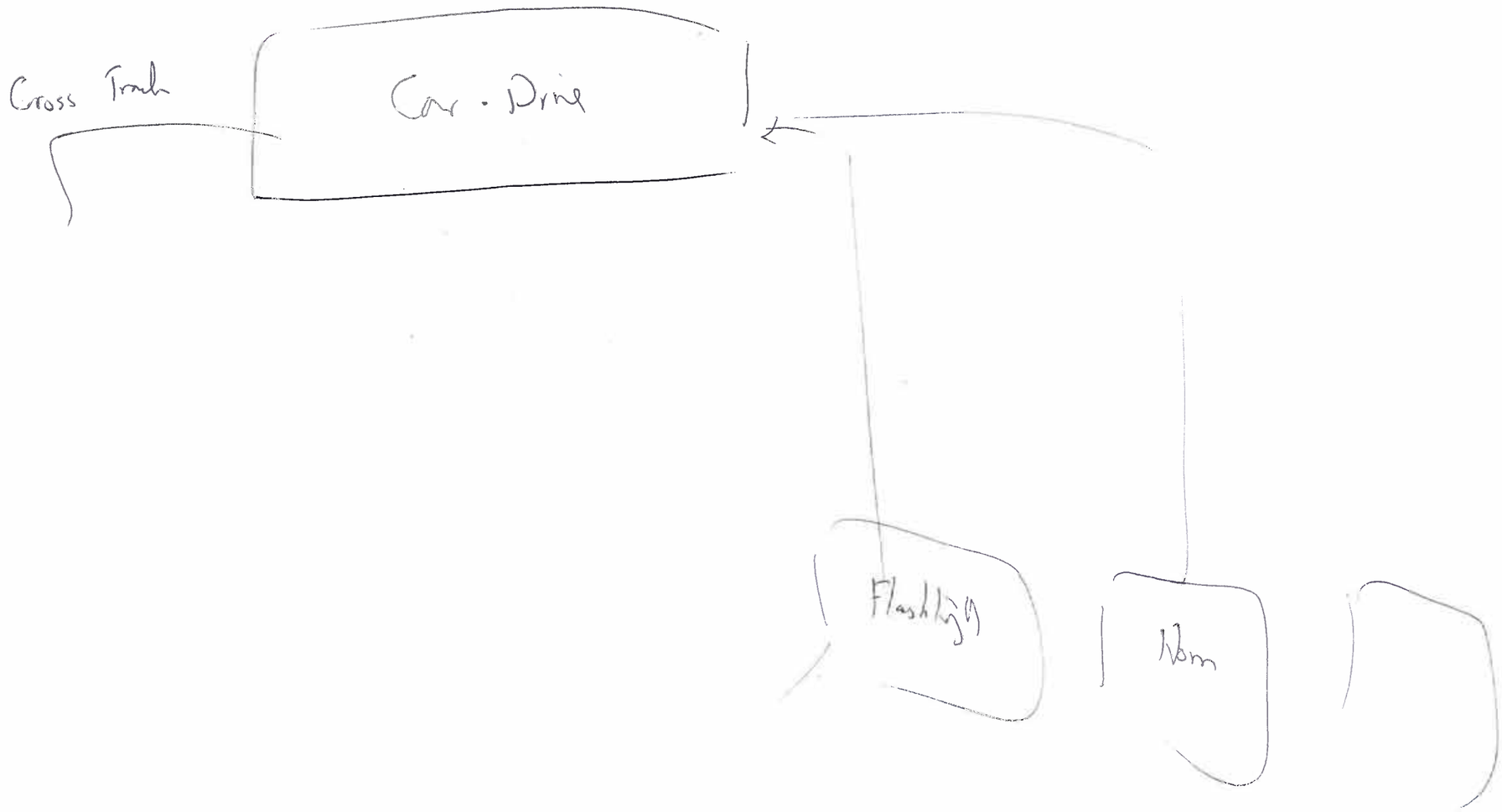
Tutorial – STPA Step 1 Template

ESW European STAMP Workshop

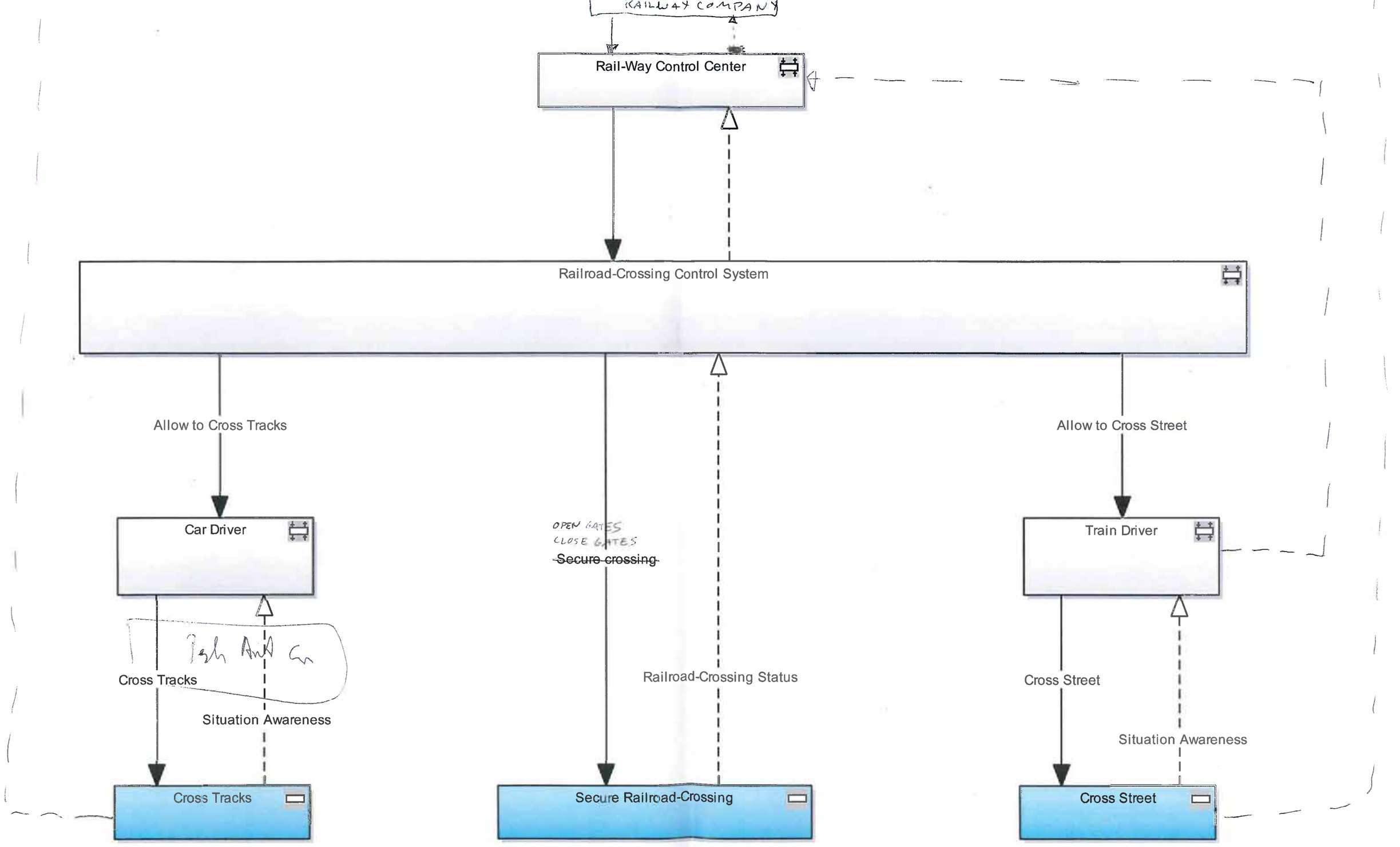
Control Action	~~Secure crossing~~ Cross Street.	Group / Page	Locarno / 1

Keyword	UCA / Comments	Safety Constraints / Requirements
not provided when expected / required	— — if train drive cross street. when car on the tracks that the train if	


Vevey


Cross Track
Car . Drive
Flashlight
Horn

Tutorial – Hierarchical Control Structure (group activity)



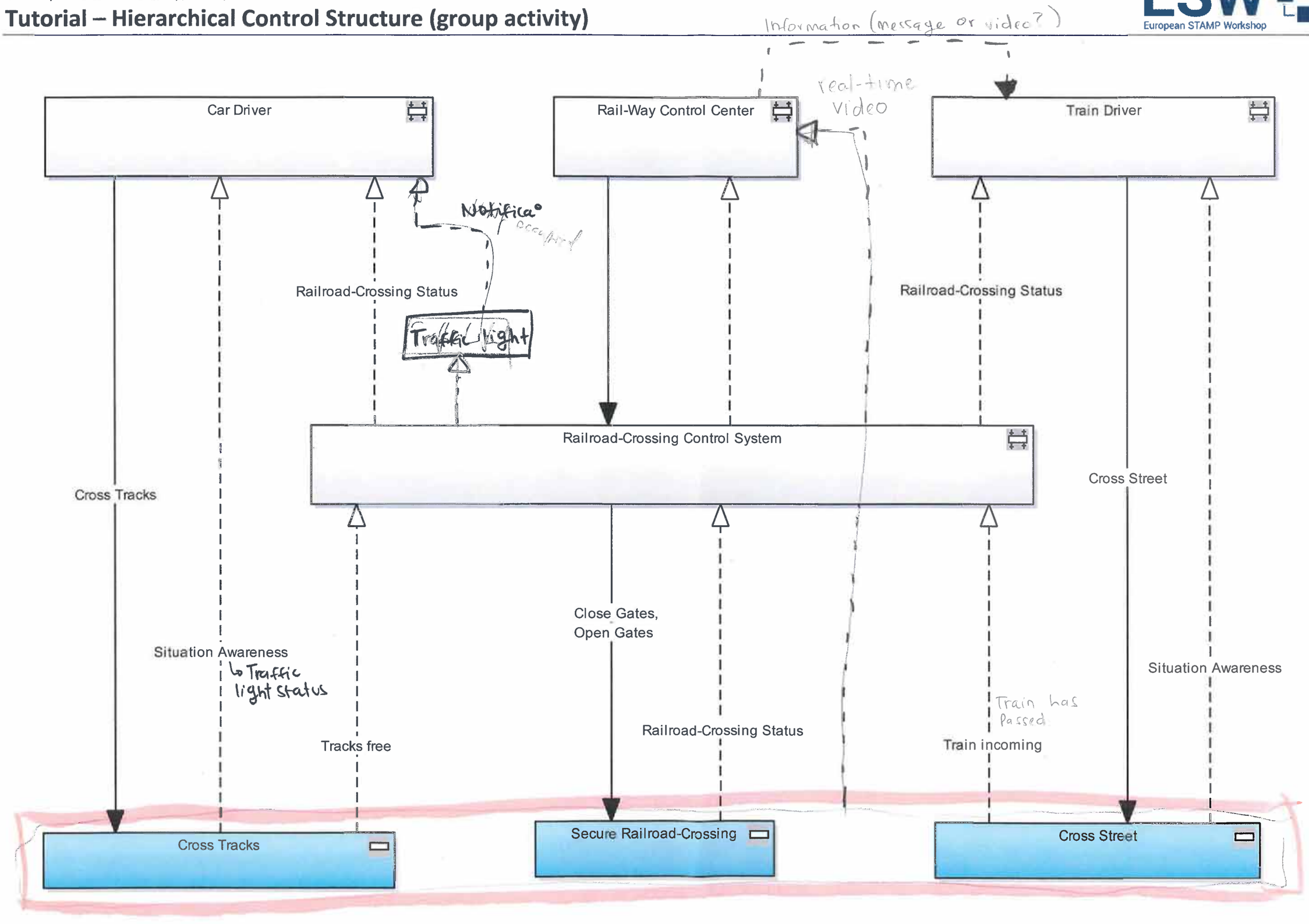

Bienne

Tutorial – STPA Step 1 Template

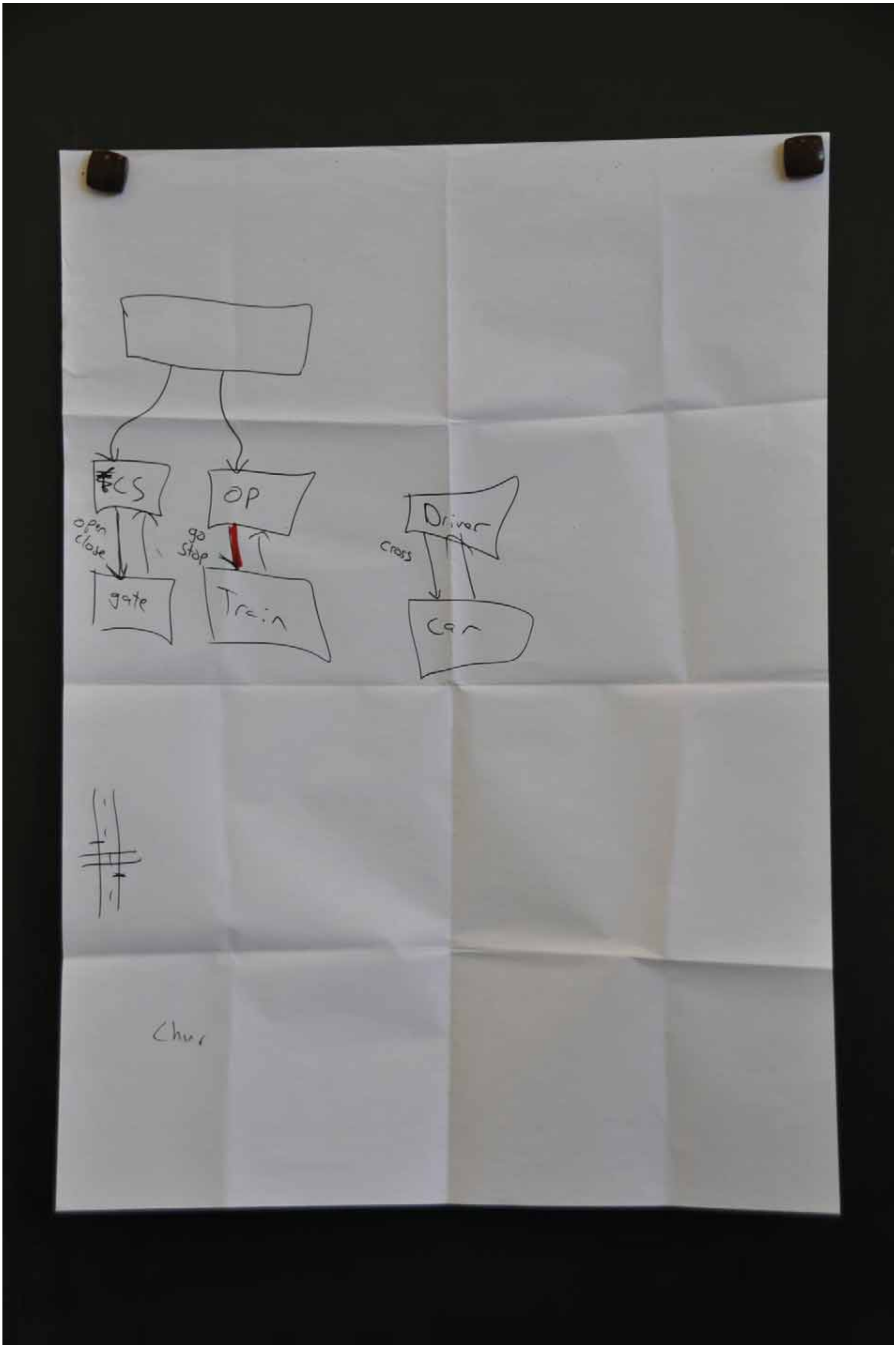
Control Action		Group / Page	

Keyword	UCA / Comments	Safety Constraints / Requirements
	"Close gate" not Provided when a train is approaching. "Close gate" Provided too late when a train is approaching "Close gate" Provided too early when a ~~train~~ Vehicle is ~~approaching~~ crossing. "Close gate" Provided when not required. "Open gate" Provided too early before an approaching train has ~~is~~ crossed. The "Open gate" and "close gate" commands are provided in the wrong order. (asynchronously)	

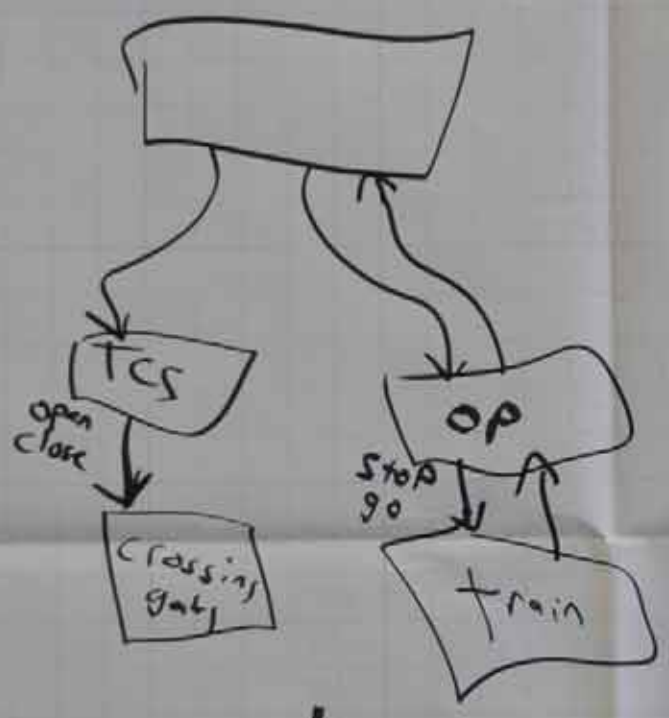
Tutorial – Hierarchical Control Structure (group activity)

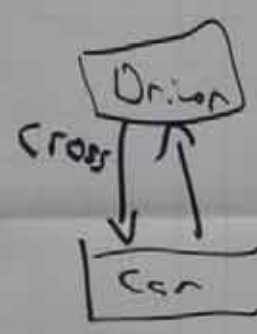



Chur

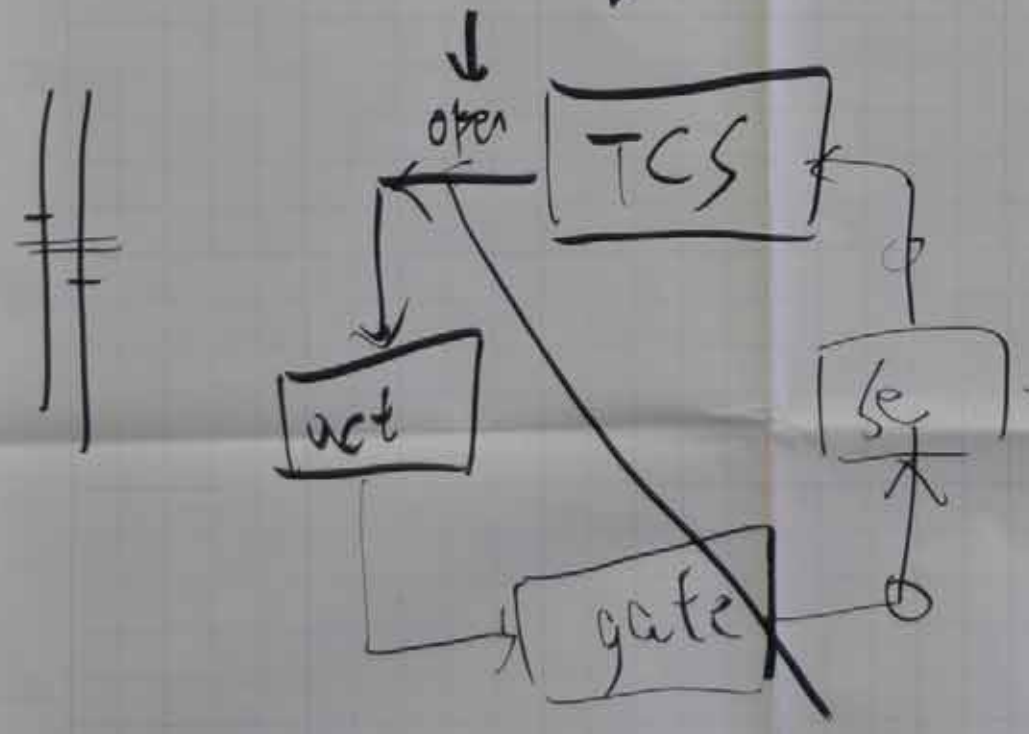

CS
OP
Driver
open
close
go
Stop
cross
gate
Train
Car

Chur





1. wrong a/g
2. Prerorce
3. Loss of feedback
4. sensor
5.



ESW European STAMP Workshop

UCA	TCS	Group / Page	Chw

Control Loop Element	Scenario / Causal Factors	Safety Constraints / Requirements
Traffic control system crossing gate actions: -open -cross	~~If not open when expected in~~ • If ~~not~~ provided when a train is coming then collision • If provided too early then cars cross the street when not allowed • ~~same like too early~~ If provided too late when a train is approaching then people can cross without it is open • If stopped too soon .... (nothing) • If applied too long .... (nothing)	• When a train is coming, the gates should be closed • Keep the gates closed until the train is 30s away • ~~Keep~~ the gates ~~closed~~ while the train is • Close the gates when the train arrives to a „save distance"

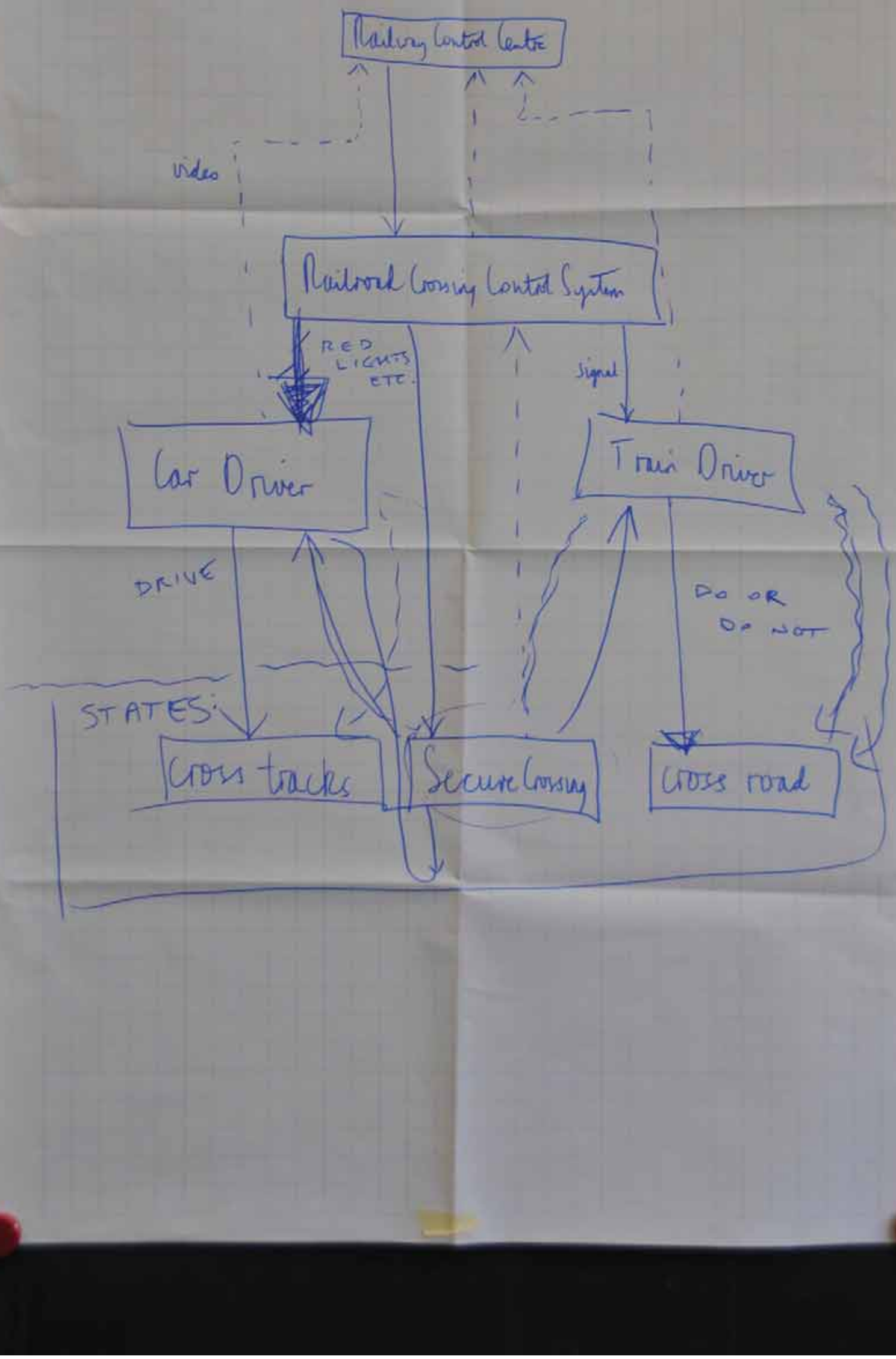
Tutorial – STPA Step 1 Template

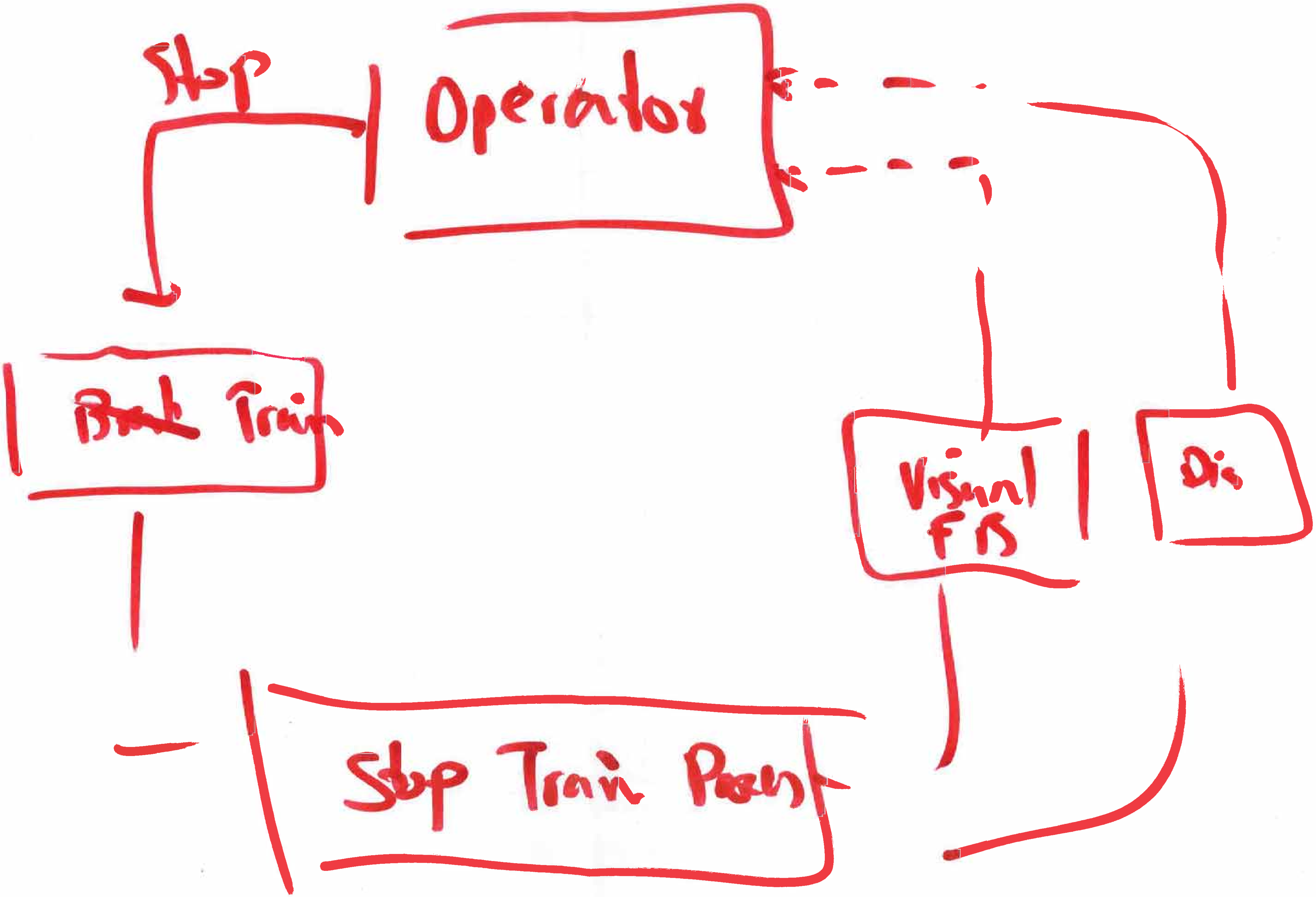
Control Action	Stop	Group / Page	

Keyword	UCA / Comments	Safety Constraints / Requirements
Not provided when expected	~~at the right time~~ If Stop is not provided when expected, then it might collide with people or vehicles	Stop has to be provided at time
provided when not expected	if Stop is provided when not expected, then the train might be late in schedule.	No hazard (from safety perspective)
	if Stop is provided when not expected, then it can lead to another train hitting it by the back	


Genève

Genève


Railway Control Centre
Video
Railroad Crossing Control System
RED LIGHTS ETC.
Signal
Car Driver
Train Driver
DRIVE
DO OR DO NOT
STATES:
Cross tracks
Secure Crossing
Cross road



Stop
Operator
Brak Train
Visual FIS
Dis
Stop Train Prest

Tutorial – Hierarchical Control Structure (group activity)