CHALMERS

D
Växel: Frammåt
Hastighetsläge: Snabb

Remote Controlled Truck

Proof of concept for designing a remote system for a Volvo truck

Pontus Carlsson
Sebastian Nilsson

Department of Signals and Systems
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden

EX028/2014

Remote Controlled Truck

PONTUS CARLSSON, SEBASTIAN NILSSON

Master's Thesis EX028/2014
Departments of Signals and Systems
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone: + 46 (0)31-772 1000

Cover:
Controller designed to remotely control the truck

Departments of Signals and Systems
Göteborg, Sweden 2014

Abstract

This thesis presents the concept to remote control a full sized truck. The safety aspects are the main issue with controlling such a vehicle. The work follows the ISO-26262 standard and results in functional safety requirements. Since the proposed application is a low-speed implementation, the highest automotive safety integrity level requirement is that the truck is not allowed to drive faster than 10 km/h and that the truck's interface which the remote system connects to must follow the desired setpoint. Requirements with lower level of automotive safety integrity level are for example that the system must detect loss of or incorrect setpoints or that the system shall not allow deactivation or activation if the parking brake is not applied. A second aspect of a remote system that is taken into account is the wireless communication between a remote controller and the vehicle. The recommendation here is that Line-of-sight propagation frequencies should be used since there is no benefit for this application to remotely control a vehicle outside visibility from the operator. From 30 MHz to 10 GHz is the proposed frequency span. Licensed spectrum is recommended to avoid disturbances in the so called "junk frequencies" like 2.4 GHz and the preferred technology is spread spectrum with frequency hopping modulation to get a robust communication. In the project a remote controller was designed as a proof-of-concept to show that it is actually possible to remotely operate a truck.

KEYWORDS: Remote, Controlled, Truck, ISO-26262, Autobox, Communication, Functional safety.

Sammanfattning

Detta examensarbete presenterar ett koncept för att fjärrstyra en fullskalig lastbil. Säkerhetsaspekterna är den huvudsakliga frågan när denna typ av fordon skall styras. Arbetet följer ISO-26262 standarden och resulterar i funktionella säkerhetskrav. Eftersom den tilltänkta applikationen är en låghastighetsimplementation är kraven med högst riskklassifiering att lastbilen inte tillåts att färdas snabbare än 10 km/h, och att lastbilens gränssnitt som fjärrsystemet är anslutet till måste följa den begärda referensen. Krav med lägre riskklassifiering är till exempel att systemet måste upptäcka när referensen förloras/är felaktig eller att systemet ej får tillåta aktivering eller avaktivering om parkeringsbromsen inte är tillslagen. En annan aspekt av fjärrstyrning som behandlas är den trådlösa kommunikationen mellan en fjärrkontroll och fordonet. Rekommendationen här är att fri-sikt-frekvenser bör användas eftersom det inte finns någon fördel att fjärrstyra fordonet när de inte är synligt för operatören. Från 30 MHz till 10 GHz är det rekommenderade frekvensspannet. Licensierade frekvenser är att föredra framför ”skräpfrekvenser” som $2,4$ GHz och den föreslagna tekniken är bandspridning med frekvenshoppsmodulering för att få en robust kommunikation. I projektet designas en fjärrkontroll som ett bevis på att konceptet fungerar och att det är möjligt att fjärrstyra en lastbil.

Nyckelord: Fjärrstyrd, Lastbil, ISO-26262, Autobox, Kommunikation.

Preface

Acknowledgments

We would like to thank:

Martin Fabian

Henrik Wiberg

Martin Ryd

Carl-Johan Hoel

Cpac System employees for supporting us

Göteborg, October 26, 2014

Sebastian och Pontus

CONTENTS

1 INTRODUCTION

1.1 Background

Volvo Trucks are, as a part of their research in customized systems, investigating the possibility of remote control of heavy vehicles. With the introduction of electronic steering the infrastructure for cost effective remote control is already in place. Remote controlled truck is an already commercialized product with an existing market. The product aims to make it easier for the operator and the driver of the vehicle to do specialized work. The operations could be for example asphalt or concrete trucks with chute that distribute their load over a longer distance and therefore have to move at the same time. Also, trucks with special machines mounted on them, like machines that make holes for guardrails by roads, would ideally be remotely controllable from outside the vehicle. The idea with this thesis is to do this specifically for a Volvo truck and take advantage of that the actuators are all controlled “by-wire”.

The primary purpose of remote controlling a truck is to avoid repetitive stepping out and in of the truck which may be both laboursome and inefficient. In many cases the truck driver uses functionalities on the truck that can only be used from outside the truck. This system would allow the driver to stay outside the truck for a longer period of time and make adjustments to the truck position at the same time as some other work is being done. Some possible applications are listed below:

- Concrete truck with small crane. Theam (2014)
- Asphalt paving truck with small chute
- Safety barrier installation
- Remote control of the truck from an aerial work platform. This is useful, for example, when replacing street lighting
- Safety hazardous situations where being present inside the truck is not favorable
- Maneuvering in tight situations where being outside the truck is advantageous

1.2 Purpose

The thesis has two purposes.

1. Creating a set of requirements and specifications that an implementation like this would need to fulfill.

2. Demonstrate by a proof-of-concept on a physical system. This demonstration does not necessarily show all the requirements, but the most important ones.

1.3 Problem formulation

To remotely control a machine is not a big task, but remote control of a 60 tonnes truck in a safe and reliable way is another deal. The goal of the thesis work is to define how a system like this would work and how to implement it with concern for safety and reliability. The work will be ended with a practical demo on a truck to validate assumptions and to verify that satisfying results can be reach with the current resources.

1.4 Scope and limitations

- For practical reasons the demonstration of a proof-of-concept will be done using an Autobox system which allows the truck to be extended with new software. The Autobox would not be included in systems sold to customers. Instead, all the functions implemented by us on the Autobox would be included in already present ECUs or a new ECU.
- A Safety analysis according to ISO-26262 will be done.

2 NOTATION

ADC	Analog to Digital Conversion
ASIL	Automotive safety integrity level, classification level for ISO-26262
Autobox	Embedded system box that is fairly easy to program. Used to connect development products together
Bodybuilder	Platform for additional hardware, eg concrete mixer or a crane connected to the vehicle
CAD	Computer-Aided Design
CAN	Controller area network
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DRC	Design Rule Check
DSSS	Direct Sequence Spread Spectrum
EDC	Electrical Rule Check
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FTA	Fault Tree Analysis, a method to expand a failure and locate possible causes
FSR	Functional Safety Requirements
LCD	Liquid Crystal Display, Display technology
LOS	Line-of-sight (propagation)
Operator	The person controlling the remote controller
PCB	Printed circuit board, holds electronic components and connects them with conductive tracks
PHA	Preliminary Hazard Analysis
PTS	Swedish Postal and Telecom Agency
RMS	Rate Monotonic Scheduling, Scheduling technique for threads in a RTOS
RTOS	Real Time Operating System
SPI	Serial Peripheral Interface, Full duplex serial communication technique
THSS	Time Hopping Spread Spectrum
VDS	Volvo Dynamic Steering, a system which makes steer-by-wire available on a Volvo truck
VRU	Vulnerable road user
WCET	Worst case execution time
WCRT	Worst case response time
XBee	Radio module incorporating the ZigBee protocol
ZigBee	Energy conservative standard for wireless communication

3 METHOD

3.1 Verification

System testing will be done throughout the project to minimize time spent implementing on the truck. In the planning we call this "system-on-table testing" since the system modules are connected on a table where programming and testing can be done with less hassle compared to on-field testing. The benefit with system-on-table testing is that bugs related to system integration are found earlier and have therefore less impact on the project.

3.2 Functional safety

Since the theses is within an automotive application hazard analysis and safety concept will follow the ISO-26262 (2011) Road vehicles – Functional safety. Worth mentioning is that ISO 26262 is not yet fully ready to be applied to vehicles over 3500 kg but it is being extended to also cover large vehicles like trucks in the near future. Satisfying ISO 26262 now serves as a premise to satisfy the same standard when the truck extension takes effect.

The standard is a modification of IEC 61508, and is a standard way of designing systems that include electrical and/or electronic (E/E) systems. The standard can be applied to the products whole lifecycle, but this thesis will only focus on the concept and functional level phases.

The concept level phase contains in short these steps:

1. Define an item that is going to be designed.
2. Do a preliminary hazard analysis (PHA) of the defined item.
3. Define safety goals, what is not to happen to avoid hazards.
4. Create/Define "Function safety requirements", functions that can be assigned to some part of the item, an external or a new part that make sure that the safety goal is fulfilled.

The item definition is a step where critical components such as actuators, sensors and/or controllers are specified and connected. The other steps uses the item definition as a specification on how the system is supposed to work.

Hazard analysis contains classifying the hazards in a specific way. Severity controllability and exposure to a specific situation in combination with a given hazard is ranked as shown in tables 3.1, 3.2 and 3.3. Then by looking into table 3.4 an automotive safety integrity level (ASIL) can be determined. The highest possible ASIL level is determined by the letter D and the lowest level is A, QM stands for quality managed and means that the standard does not state any recommendations how to design to avoid possible hazards. Safety goals are then specified in such way that when fulfilled all ASIL classed hazards will be avoided. Each safety goal then get the highest ASIL level of the hazards it is covering.

The end result of the concept phase is functional safety requirements (FSR), which are requirements on a functional level that the system needs to fulfill in order to not violate any of the safety goals.

Table 3.1. Classes of severity

	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and Life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Table 3.2. Classes of probability of exposure regarding operational situations

	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Table 3.3. Classes of controllability

	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Table 3.4. ASIL determination

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

4 RESULTS

This chapter describes the sequence of steps in the order that the project went through them, starting with a System architecture phase where the functionality, solutions and design targets were evaluated. When the system architecture was in place, it was split into modules. When all modules were done, testing and verification followed, as seen in Figure 4.1.

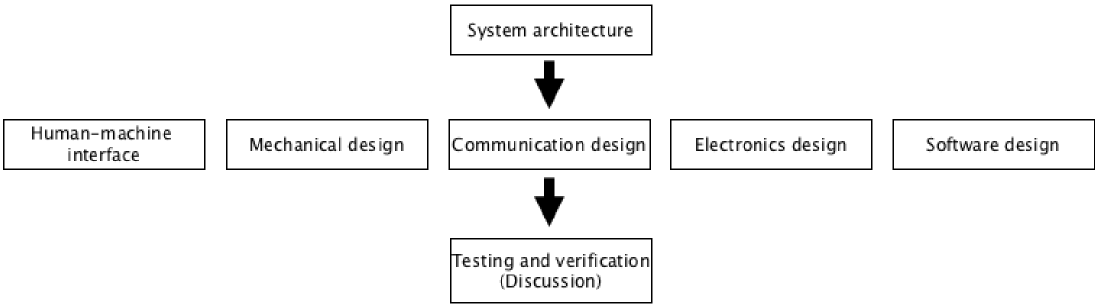


Figure 4.1. The sequence of steps in the project

4.1 System architecture

The functional model (represented by Figure 4.2) is a graphical representation of the desired functionality and the system. The purpose of the functional model is to describe functions, processes, and information and physical flows. The functional model aids discovery of information needs, identifies opportunities and gives a rough idea of how a product could be designed. A good functional model must not limit implementation and new solutions, that is, it must not specify solutions.

4.2 Safety concept according to ISO-26262

4.2.1 Item definition

The item being evaluated is the remote controller and the receiver. The truck and its controllers are added as external resources and are therefore assumed not to fail when hazard analysis is done. The signals in the definition are steering, breaking and acceleration. Which signal is sent where is shown in Figure 4.3.

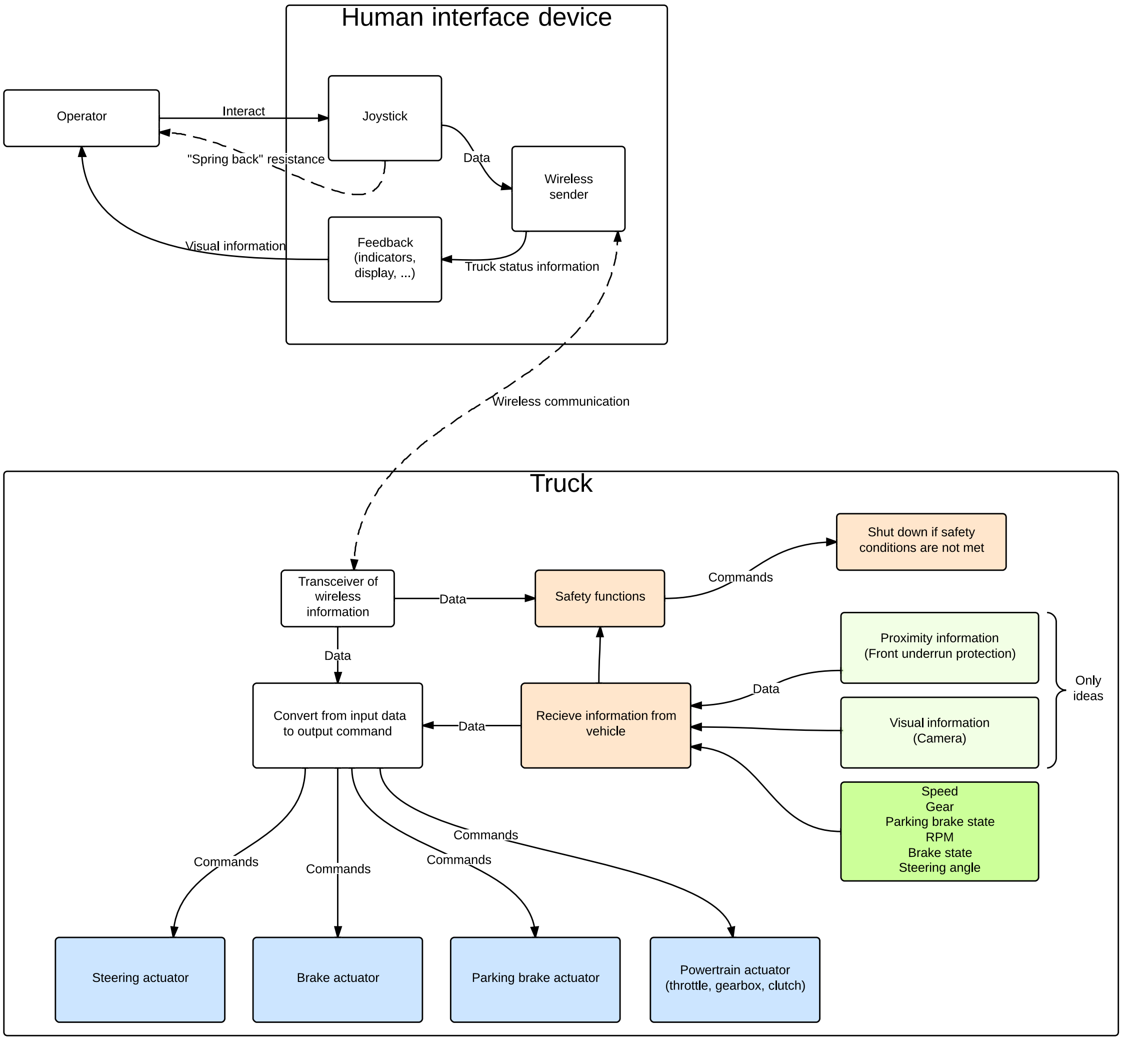


Figure 4.2. Functional model

Functions

The basic functionality of the remote control system is to be able to accelerate, brake and steer. Acceleration, braking and steering is continuously based on the operators physical input. The remote control system will receive physical inputs from the operator, as seen in Figure 4.3. The controller then interprets the signals and sends them to a receiver using wireless modules. The receiver receives the wireless signals and calculates an output for the truck interface. The interface is an external module that actually controls the trucks actuators. An assumption here is that the normal controls inside the truck does have priority over the remote system, meaning that if a driver inside the truck applies brake and an operator using the remote controller applies full throttle the truck will brake.

The physical sensors on the controller should work as described in Section 4.5, which explains how the operator can control the truck using a joystick and a steering knob.

Operation states

The system can be in two different states, activated or deactivated. When activated it is assumed that there is no driver in the driver seat, since the operator is using the remote control system instead. When deactivated the system should behave as a truck in normal operation and the operator will be driving the truck from the driver seat. This means that when the unlikely event occurs where the operator tries to use both the remote control and the trucks physical controls at the same time the truck will be in the deactivated state.

Foreseeable misuses

A foreseeable and reasonable misuse of the system is that the operator is driving the vehicle remotely and does not observe the path of the vehicle. This is taken into account as an operational situation in the hazard analysis.

4.2.2 Preliminary Hazard analysis

Preliminary Hazard Analysis according to ISO-26262 involves three different steps

1. Define operational situations
2. Define possible malfunctions
3. Combine situations with malfunctions to get hazards and evaluate the severity of each combination

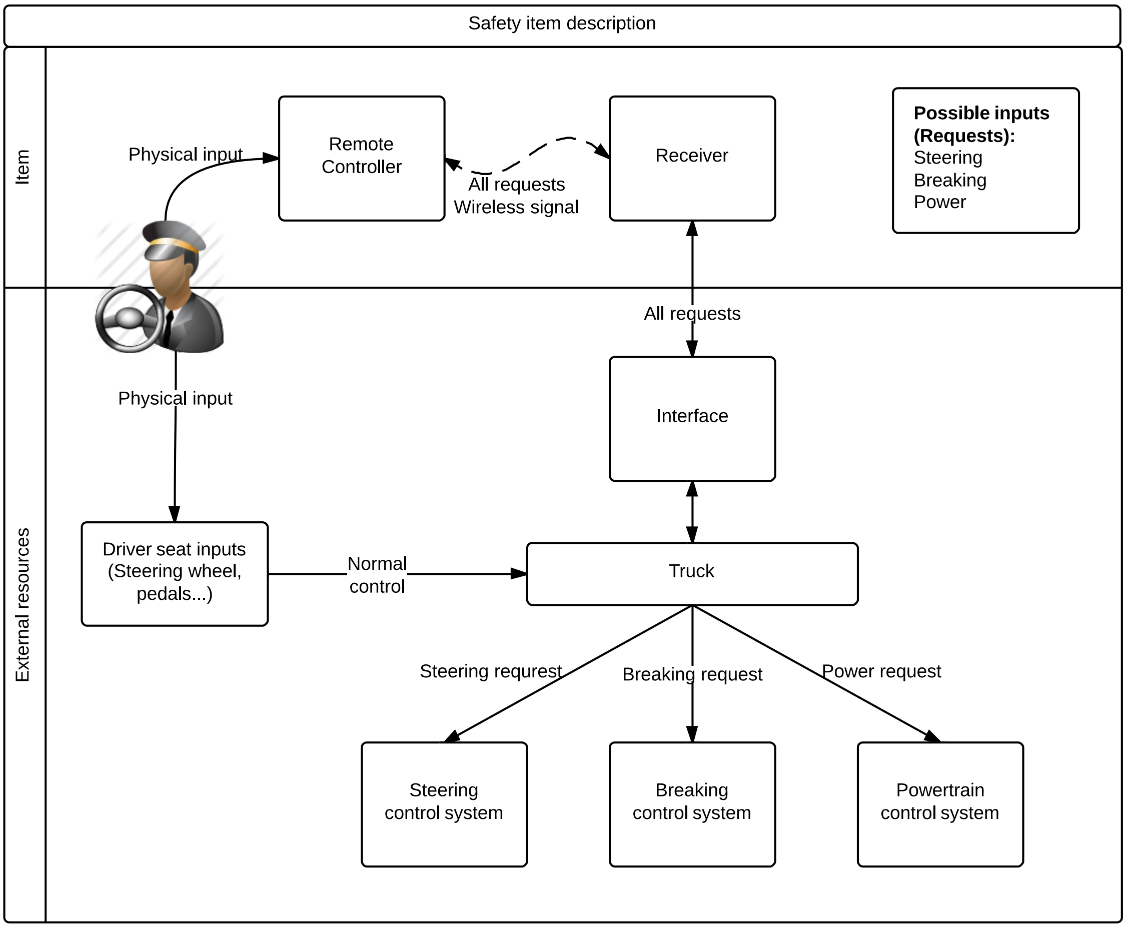


Figure 4.3. Item definition description

Table 4.1. Possible operational situations for a remote controlled truck

Driving on larger road at speed higher than 30 km/h
Driving on smaller road at speed higher than 30 km/h
Driving on smaller road or enclosed area at speed between 10 and 30 km/h
Driving on smaller road or enclosed area at speed below 10 km/h
Manoeuvre heavy situations.
Parking brake activated, zero speed
The operatior drives the vehicle wihtout watching its path at speeds lower than 10 km/h, this is a forseeable misuse.

Table 4.2. Possible malfunctions in analysis for a remote controlled truck

The truck receives a steering request that the operator did not issue
The operator requests steering but the truck does not receive the request
The operator requests steering, the truck gets the request delayed X timeunits
The truck receives a braking request that the operator did not issue
The operator requests braking but the truck does not receive the request
The operator requests braking, the truck gets the request delayed X timeunits
The truck receives an acceleration request that the operator did not issue
The operator requests acceleration but the truck does not receive the request
The operator requests acceleration, the truck gets the request delayed X timeunits
Unintended activation of remote system, since steering then tries to center and braking is applied it will be a combination between unintended steering and unintended braking. Also the driver is in the driving seat since the system was, prior to failure, deactivated. We then have double requests to controllers which makes this failure hard to control.
Unintended deactivation of remote system, all requests are lost

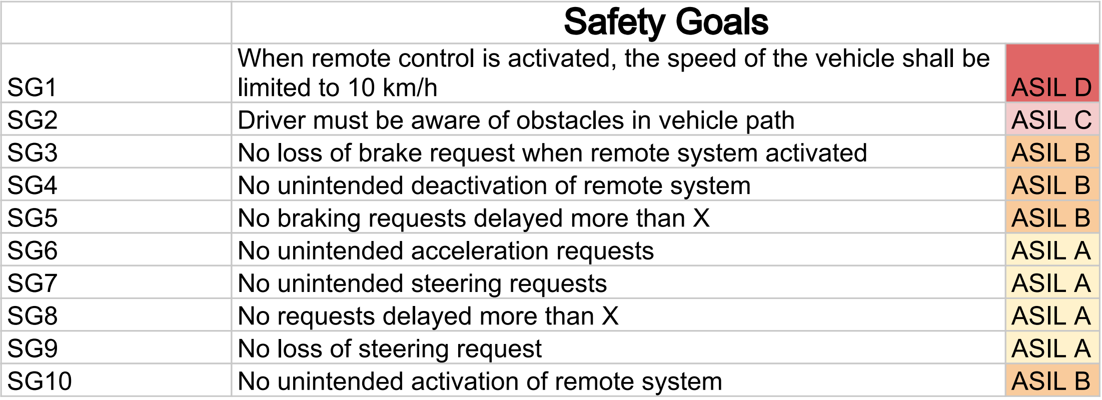
The hazard analysis results in safety goals, which must not be violated to avoid hazards.

The operational situations are defined as in Table 4.1. Each situation is defined with speed in mind, since the application is a low speed product. The lower the speed the less severe any hazards will be and therefore the safety goal will have lower ASIL. All of those scenarios have medium (E3) to high (E4) exposure rate over a vehicles full life-cycle.

The operational situations might have variants like poor vision, bad road conditions, slopes and so on. All those cases will be more unlikely to occur but might make it less controllable, therefore this will probably not create any new hazards with higher ASIL than the usual case without more extreme variants. Therefore variants are not explicitly added in this analysis, instead each situation contains all variants and can be altered depending on the hazard it is combined with.

The possible malfunctions would be that the physical signals given by the operator in some way does not affect the vehicle or that the state of the system changes unexpectedly. In each malfunction it is assumed that the control system on the vehicle still works as intended, meaning that if the operator loses breaking ability it is still possible to break from the drivers seat inside the vehicle. The operational situations are then combined with the malfunctions and evaluated by severity exposure and controllability. The full table can be found in Appendix F.

The result is a list of safety goals, top level requirements, listed in Figure 4.4.



	Safety Goals	
SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	ASIL D
SG2	Driver must be aware of obstacles in vehicle path	ASIL C
SG3	No loss of brake request when remote system activated	ASIL B
SG4	No unintended deactivation of remote system	ASIL B
SG5	No braking requests delayed more than X	ASIL B
SG6	No unintended acceleration requests	ASIL A
SG7	No unintended steering requests	ASIL A
SG8	No requests delayed more than X	ASIL A
SG9	No loss of steering request	ASIL A
SG10	No unintended activation of remote system	ASIL B

Figure 4.4. Safety goals for remote controlled truck, result from Section 4.2.2

4.2.3 Functional safety requirements

The safety goals are the top level requirements that must be fulfilled. Those can be branched down to functional safety requirements (FSR) using fault tree analysis (FTA). This analysis allows for new functions to be implemented in order to detect or hinder the safety goals from being violated. To do this the original item definition is a bit vague and needs to be extended in order to verify that each fault is caught when doing the FTA. The FSR is shown in Figure 4.6 and the FTA can be found in Appendix F.

If any of the FSR are violated, the system is placed in a safe state where in all cases full brakes are applied and the system is deactivated. To recover from the safe state, the system needs to be reinitialized by entering the truck to restart the system.

Each FSR must be allocated to an element in the item definition. The given element then has the role to make sure that the FSR is followed with the given ASIL. The FSR also states a new element named setpoint monitor which some requirements were allocated onto. The setpoint monitor can be seen in the extended Figure 4.5 of the item description. This element will monitor the signals going between the receiver and the truck.

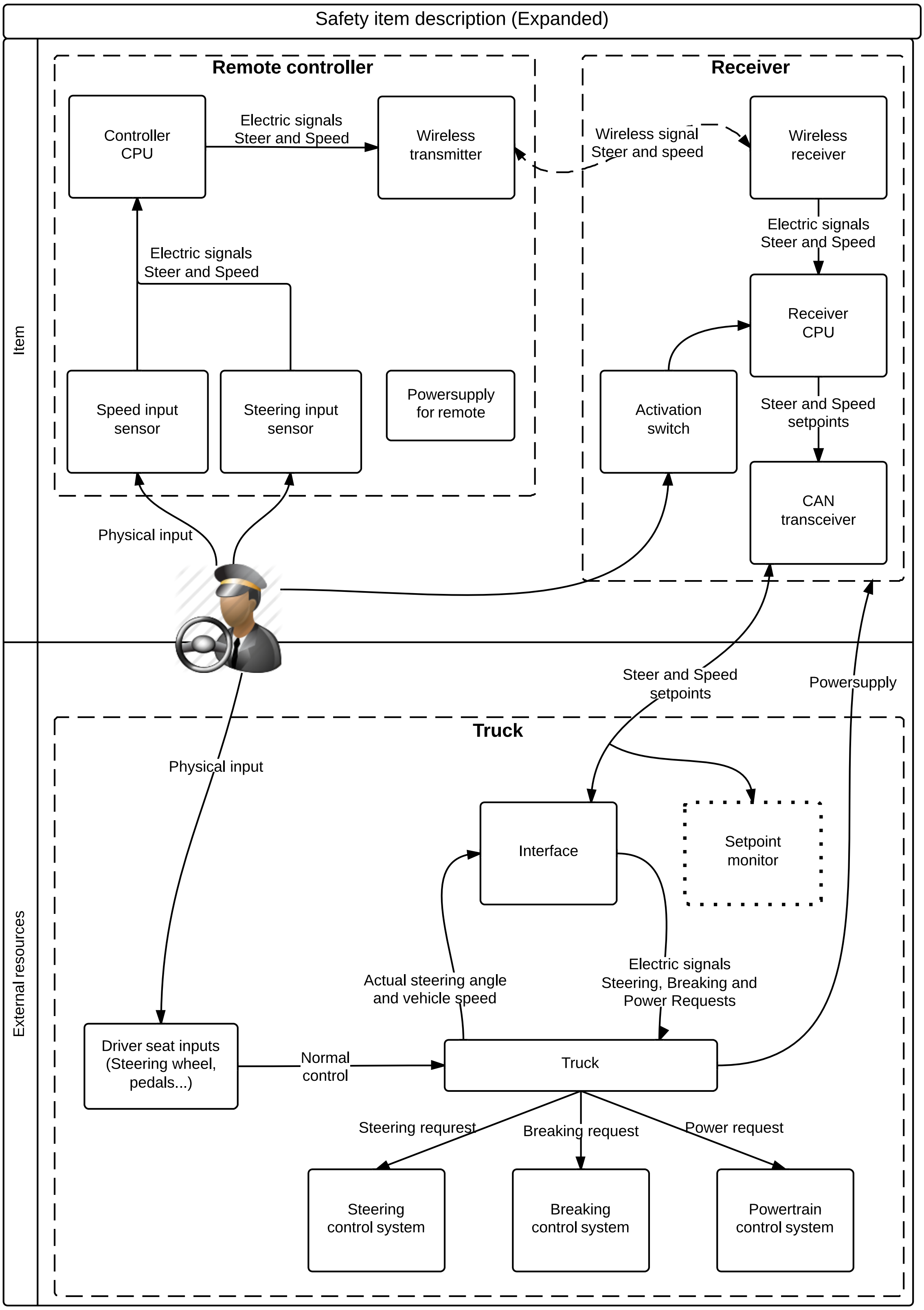
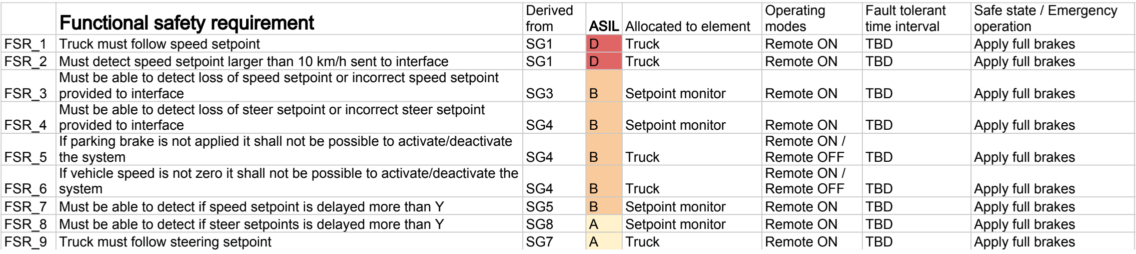


Figure 4.5. Item definition, expanded in more detail



	Functional safety requirement	Derived from	ASIL	Allocated to element	Operating modes	Fault tolerant time interval	Safe state / Emergency operation
FSR_1	Truck must follow speed setpoint	SG1	D	Truck	Remote ON	TBD	Apply full brakes
FSR_2	Must detect speed setpoint larger than 10 km/h sent to interface	SG1	D	Truck	Remote ON	TBD	Apply full brakes
FSR_3	Must be able to detect loss of speed setpoint or incorrect speed setpoint provided to interface	SG3	B	Setpoint monitor	Remote ON	TBD	Apply full brakes
FSR_4	Must be able to detect loss of steer setpoint or incorrect steer setpoint provided to interface	SG4	B	Setpoint monitor	Remote ON	TBD	Apply full brakes
FSR_5	If parking brake is not applied it shall not be possible to activate/deactivate the system	SG4	B	Truck	Remote ON / Remote OFF	TBD	Apply full brakes
FSR_6	If vehicle speed is not zero it shall not be possible to activate/deactivate the system	SG4	B	Truck	Remote ON / Remote OFF	TBD	Apply full brakes
FSR_7	Must be able to detect if speed setpoint is delayed more than Y	SG5	B	Setpoint monitor	Remote ON	TBD	Apply full brakes
FSR_8	Must be able to detect if steer setpoints is delayed more than Y	SG8	A	Setpoint monitor	Remote ON	TBD	Apply full brakes
FSR_9	Truck must follow steering setpoint	SG7	A	Truck	Remote ON	TBD	Apply full brakes

Figure 4.6. Functional safety requirements, results from the fault tree analysis

4.3 Design targets

The functional model and the safety concept generates a set of design targets (Table 4.3). The values for each target are based on the the safety concept and reasonable assumptions from what can be expected from modern wireless devices.

Table 4.3: Design targets

Target	**Value**	**Comment**
Joystick to receiver lag	$x[ms]$	Testing needs to be done.
Maximum steering angle velocity		Limit for safety reasons. Testing at max speed
Maximum steering angle acceleration		Limit for safety reasons. 25 [Nm] is max torque produced by VDS
Maximum speed	$10[km/h]$	From hazard analysis
Joystick to actuator lag	$< 50[ms]$	Steering response.
Truck remotely controlled	True	Fulfilled when able to steer, break and accelerate by using a remote controller
Remote time to live	$> 12[h]$	Remote time to live per battery charge. One working day + battery degrading time (33%)
Battery charge time	$< 8[h]$	For a second battery pack to charge while the first one is in use
Signal range	$> 100[m]$	Driving the vehicle from longer distances is not really useful
Loosing connection	less than once a month	When following all other requirements as range and battery lifetime
Remote updaterate	$> 100[hz]$	Toycar $50 \cdot 2 = 100[hz]$
Startup time	$< 1[s]$	Time from starting remote system until it is ready

Continued on next page

Target	Value	Comment
Communication reconnect time (after lost)	$< 0.5[s]$	Half of the startup time
Maximum acceleration	$1[m/s^2]$	$\sim 2,8[s]$ to full speed $10[km/h]$
Maximum deacceleration non fail mode	$2[m/s^2]$	$\sim 1,4[s]$ to halt from $10[km/h]$

4.4 Solution model

The solution model is similar to the functional model with the important difference that it specifies the most important design decisions, see Appendix A.

There are three programmable units in the design. The remote, the receiver and the Autobox. The Autobox coding is done in Matlab Simulink which is a very powerful tool for doing signal processing and control logic. The model (Simulink code) is merged with a model already existing in the Autobox. The existing model takes simple inputs references, e.g. steering angle or speed reference and returns information (e.g. vehicle speed). The references are followed as quickly as possible and therefore a smooth trajectory reference has to be generated out from the input signals to get a comfortable control behavior.

In order to use the powerful tools available, a decision was made to do most signal processing inside the Autobox model. This means that the remote and receiver simply just forward the signals from the controller to the Autobox. The weakness is that in order to do good signal processing, the original samples are needed. The raw signal often requires more bandwidth than a filtered signal and since the wireless communication probably is the bottleneck, this is going to limit the possible sample speed and resolution. The strengths is that it is simple to do filtering and then simulate the design to verify that it works as intended.

The receiver is just a stupid transceiver, receiving messages from the XBee module and forwarding it to the CAN bus and vice versa in the other direction.

The controller has a more sophisticated design where it has a watchdog thread that verifies that the communication is working as intended and checking battery status. It also has a screen to display visual information to the driver like error messages and vehicle information. The controller sends the sampled inputs to the receiver with maximum practical rate.

4.5 Human-machine interface

Human-machine interaction should always be considered when designing a product that in any way needs input from a human. Design targets for the interface are:

- Out of range indication. Make sure that the operator knows if the controller is out of range from communication with the truck.
- Battery status. Make sure that the operator gets notified when the battery is close to empty.
- Show warning messages from the truck. When a warning message is received the operator needs to confirm the message. This attempts to avoid missing serious warnings.

Our focus when designing the controller was on functionality:

- If the user lets go of the joystick the truck should calmly deaccelerate and stop.
- A certain angle on the joystick corresponds to a certain velocity. The alternative to this approach would be to let the joystick regulate the throttle and brake power. The idea is to make it easy for the user to regulate speed. Keeping the joystick at the same angle should correspond to a certain constant velocity.
- Two main modes for velocity regulation exist; work mode and transportation mode. If the truck just needs to be transported (for example from one broken streetlight to another) then the transport mode limits the velocity to 10 km/h. When work mode is activated the maximum velocity is 5 km/h. Basically the truck should not go any faster than walking pace when in work mode.
- A switch will be used to select between the transportation and work modes.

Three main alternatives to the behavior of the velocity joystick are proposed:

1. Forward means either forward or backward acceleration depending on the state of a directional switch. The advantage is that when reversing, the operator will most probably walk besides the truck looking in the truck's backward direction, therefore making a joystick push forward logical.
2. The joystick works similar to a plane throttle. Pushing the joystick forward will mean forward motion in the forward mode and brake in the backward mode. Pushing the joystick backward will mean backward motion when in backward mode and brake when in forward mode. Here a directional switch is also necessary to change between backward mode and forward mode.

3. Full brake is when the joystick is in the centre. Pushing the joystick backwards will make the truck reverse. Pushing it forwards will make the truck go forward. If the operator requests an opposite motion to the truck direction (for example applying full reverse when the truck is moving forward) then the truck will only brake to a standstill. The operator will need to release the joystick back to the centre before an opposite motion is possible. This functionality is to make sure that during an emergency brake, the truck will not stop and then start moving in the opposite direction. This alternative does not require a mode switch as the other two alternatives.

Modes are often frowned upon in interface design since they are likely to produce so called mode errors. A mode error is when the user expects a certain behavior, but because of the device being in a certain mode, gets a different behavior. A mode error is very likely to occur in alternative 1 since opposite behaviors depend on a mode switch. Alternative 3 is overly complex and the user might have a problem with expectation of the behavior of the truck. Alternative 2 is the chosen alternative even though it includes a mode switch. The user might still make a mode error by not remembering if the truck is in forward or backward mode, but the consequence will simply be that the truck does not move. Since safety is a main design target this solution is chosen.

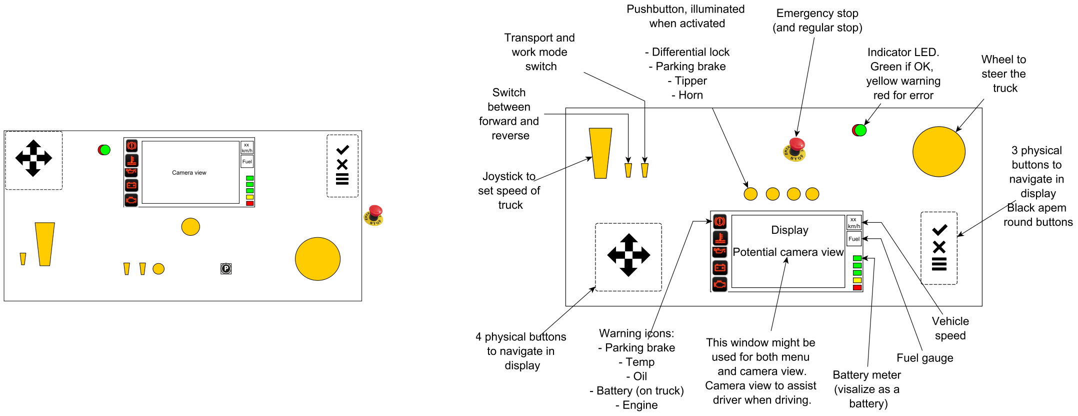
4.6 Steering behavior

Progressive steering where the steering is fine close to equilibrium and coarse close to the extreme angles is desired. The idea is to allow fine adjustments to a straight forward motion, and at the same time allow the operator to make full steering angles possible. Both linear and progressive steering should be tested. A deadzone close to the steering centre (spring equilibrium) is introduced to avoid unintended drift. Both mechanical imperfections and limited sensor precision might cause varying angle readings when the steering is in centre. When returning the wheel to centre, any values that are unlikely to be from the user should be removed. By introducing a deadzone, values close to the equilibrium are removed and unintended drift is avoided.

4.7 Layout

Designing the layout of the interface is an iterative process. The final layout is shown in Figure 4.7 (left).

Ergonomics testing was done with a very basic cardboard box, see Figure 4.8. The most important results from this test was the decision to move the steering knob and the velocity joystick further away from the operator to give a more relaxed posture. The emergency switch was moved to always be visible and the display was

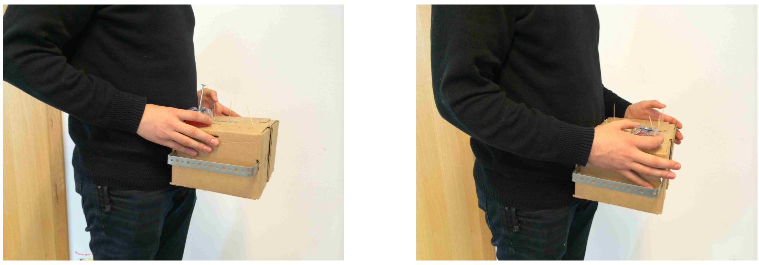

Camera view
xx km/h
Fuel
Pushbutton, illuminated when activated
- Differential lock
- Parking brake
- Tipper
- Horn
Emergency stop (and regular stop)
Transport and work mode switch
Indicator LED. Green if OK, yellow warning red for error
Wheel to steer the truck
Switch between forward and reverse
Joystick to set speed of truck
3 physical buttons to navigate in display
Black apem round buttons
Display
Potential camera view
4 physical buttons to navigate in display
Warning icons:
- Parking brake
- Temp
- Oil
- Battery (on truck)
- Engine
This window might be used for both menu and camera view. Camera view to assist driver when driving.
Battery meter (visalize as a battery)
Fuel gauge
Vehicle speed

(a) Early sketch for the control layout

(b) Final layout of the controller with steering knob and joystick moved further up

Figure 4.7. Final layout compared to the early sketch

put further away from the operator's focus.



(a) Early layout

(b) Final layout

Figure 4.8. Layout before the cardboard test and after

Information being presented on the display should aid the operator with relevant data that ease mental processing for executing a task Bohgard et al. (2008). In our case the most important information being shown on the screen is the current status of the truck and if it is safe to operate. It should show if the truck is in reverse, if it is in transport or work mode and important vehicle variables (fuel, battery, and warnings).

The controls should be designed to be accessible, easy to identify and understandable. The user's mental model should correspond well with the behavior of the controls. Bohgard et al. (2008) In essence, the controls should be designed with the target that the user should be able to control the truck without reading the manual. The mental model for controlling a truck is that a round knob is used for steering and an one-axis joystick is throttle and brake. This is the main reason for using a knob instead of another joystick for steering.

4.7.1 Functions that are not part of the proof-of-concept

Some functions were considered to be out-of-scope for the proof-of-concept design. These might be interesting for further research:

- Fisheye camera on one or multiple positions with a feed to the control display. The main reason that camera view on the controller was not considered was because the operator might focus on the screen instead of just looking at the truck. It might be useful though, if treated as a complement to regular vision observation.
- Dead-man's switch as a fail-safe to stop the truck during a potentially dangerous situation, for example if the operator loses consciousness or drops the control. It is not implemented in the proof-of-concept design since the primary purpose of the prototype testing is to show the feasibility of remotely controlling a heavy vehicle.
- Extra functionality by controlling Body Builder functions (such as tipper, lift, asphalt chute, . . .) or regular truck functions (such as horn and lights). It is not part of the proof-of-concept due to the same reason as the dead-man's switch.

4.8 Mechanical design

In order to get the layout and functions described in Chapter 4.5 onto a mechanical prototype, a CAD system was used to aid in visualizing the construction before manufacturing and assembly. This chapter describes the design.

4.8.1 Design targets

The target of the mechanical design is basically to support other components:

- Implement assembly for steering angle sensor (steering mechanics)
- Fasteners for holding the body together, battery, buttons, switches and the joystick
- Provide the operator with an ergonomic working posture
- Fulfill the interface layout
- It will also be designed with robustness in mind.

Optimization for material use, weight and touch-and-feel design is considered to be out of scope.

4.8.2 Implementation of interface design

The result from the human-machine design consideration of Chapter 4.5 was implemented into a CAD system with straight lines and symmetry in mind. The layout from Figure 4.7b was visualized in the CAD as seen in Figure 4.9.

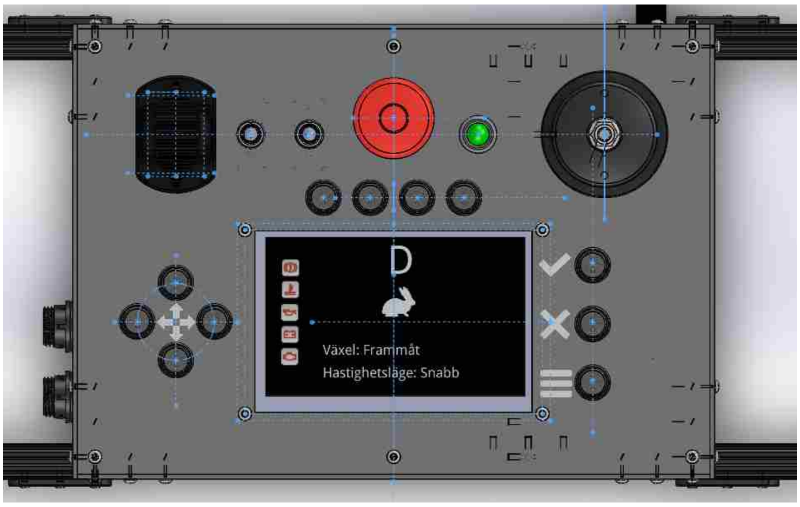


Figure 4.9. CAD interface drawing

4.8.3 Spring-back for steering knob

An engineering challenge was to design the mechanics for the steering knob. The steering knob needed to have a spring-back to centre when released and finding a potentiometer with this functionality was more difficult than expected. Therefore the spring-back functionality had to be implemented in the mechanical design. The targets for the steering mechanics and a brief implementation description is presented below:

- Spring-back to centre with variable spring force
    - Implemented by replacing the spring in the assembly
- Stop at end points in both directions
    - Implemented with a beam and a circular plate. Both the beam and the plate have screws that collide at the end points. See Figure 4.10:
- Interface the angle sensor
    - Implemented by a threaded rod and supportive beams. Bearings are used to keep the threaded rod in position. (A better solution would probably have been just drilling a hole and ignoring the friction it would impose)

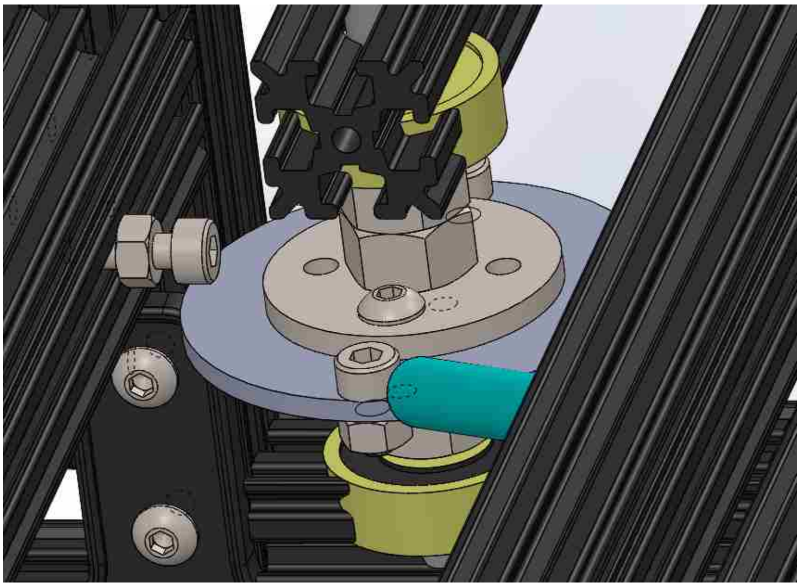


Figure 4.10. Steering end point stop implementation

4.8.4 Manufacturing

By using standardised components when possible, we have limited the number of manufactured components. For example in the steering mechanics (see Figure 4.10) an assembly of washers, nuts, screws and a threaded rod made the design less complex and easy to manufacture. Components that still needed manufacturing was the circular plate (holding the stop screws and the spring) and the steering knob. Manufacturing and assembly is described more thoroughly in Appendix D. Drawings for milling and drilling operations are presented in Appendix C.

4.9 Communication design

To allow wireless communication between the remote and the truck a practical approach to selection of wireless technologies is necessary. This section will mainly focus on recommendations for a potential commercial product and not on the proof-of-concept prototype. Decisions to take include:

- Licensed vs unlicensed spectrums
- Propagation mode (type of transmission)
- Spread spectrum modulation technique, including:
  - Choise of frequency band
  - Noise and interference robustness considerations

4.9.1 Licensed vs unlicensed spectrum

The unlicensed spectrums are so called “junk frequencies” that commercial users are unlikely to want. The 2.4 GHz band is an example of such a frequency. It is shared with Bluetooth, Wifi, Zigbee, RC hobby devices to name a few. It is also subject to interference from microwave ovens which explains why the signal has problems penetrating trees, heavy snow or anything that contains water (since a portion of the signal is absorbed as heat into water, just like in a microwave oven).

For a commercial product our recommendation would be to use a dedicated frequency which would require permissions from the agency in the regions where the device will be used (i.e. FCC for the US or PTS for Sweden). Selection of an exact frequency band is considered out-of-scope for this project, since it would require interaction with one or more agencies, but a recommendation for a frequency range will be put forward. Our recommendation for a commercial product being presented in the following sub-chapters, will therefore consider the physics and not the politics of frequency selection.

4.9.2 Propagation mode (type of transmission)

“A signal radiated from an antenna travels along one of three routes: ground wave, sky wave, or line of sight (LOS)” Stalling (2005). Figure 4.11 illustrates this. LOS propagation provides the lowest wireless communication distance due to the earth’s curvature, but the potential distance is still far greater than what we are trying to achieve. The earth’s curvature will not matter since we are not trying to achieve any greater distances than 100 m. There would be no benefit of using anything other than LOS propagation as far as the distance target is considered.

Since LOS propagation does not operate below 30 MHz Stalling (2005), only frequencies above this will be considered to make sure reception is limited to LOS communication. By only considering LOS communication, avoidance from disturbances far from the source is achieved. Other factors then become far more important to consider:

- Data throughput. The higher the frequency the greater the possible data rate.
- Omnidirectionality; that is, the signal propagates in all directions from the antenna. At high frequencies omnidirectionality becomes more difficult. Since the truck and the remote control are movable omnidirectionality is important.
- Attenuation increases with rainfall which is especially noticeable for frequencies above 10 GHz.
- Interference from other sources. Microwave transmissions are growing in popularity and interference robustness is therefore important.

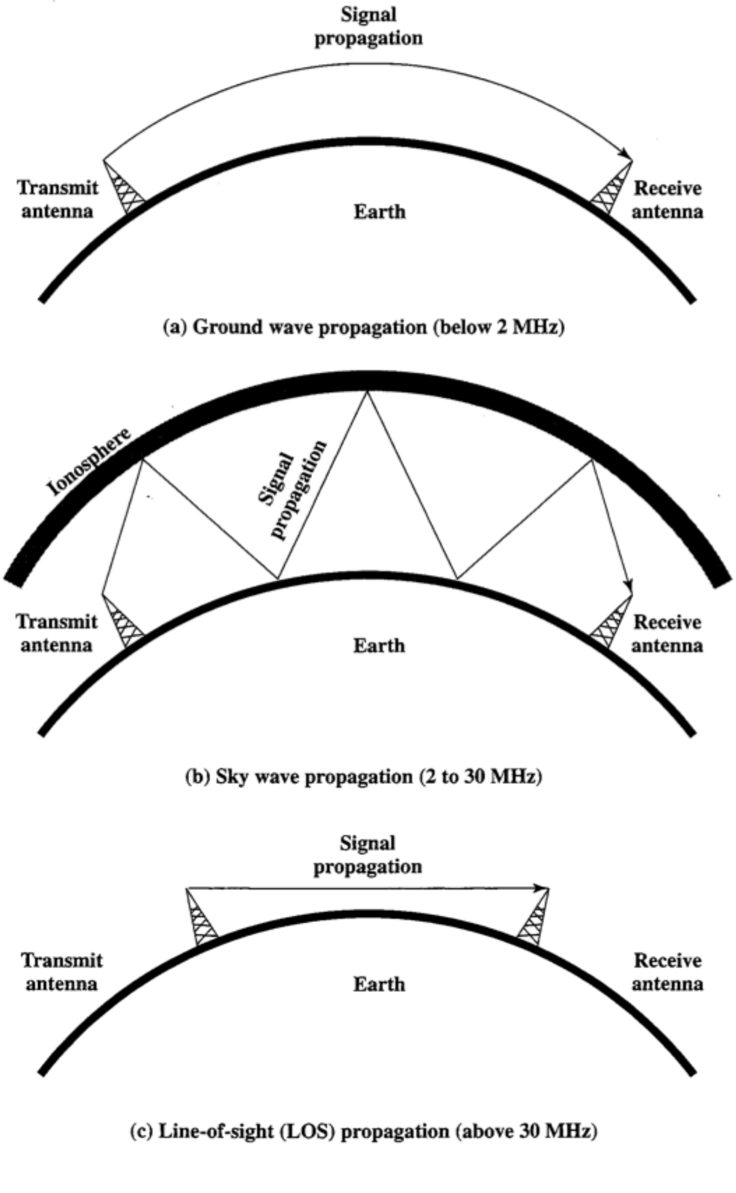


Figure 4.11. Wireless propagation modes, Stalling (2005)

4.9.3 Spread spectrum modulation properties

Spread spectrum technology shows its strength primarily in license free spectrums where the frequency band is shared among many users. However the technology also provides other advantages:

- Transmission security
- Resistance to interference from other radio sources
- Redundancy
- Resistance to multipath and fading effects Schwartz (2005)

Robustness is one of the main attributes searched for and therefore spread spectrum with its inherent robustness is from this point forwards the chosen approach.

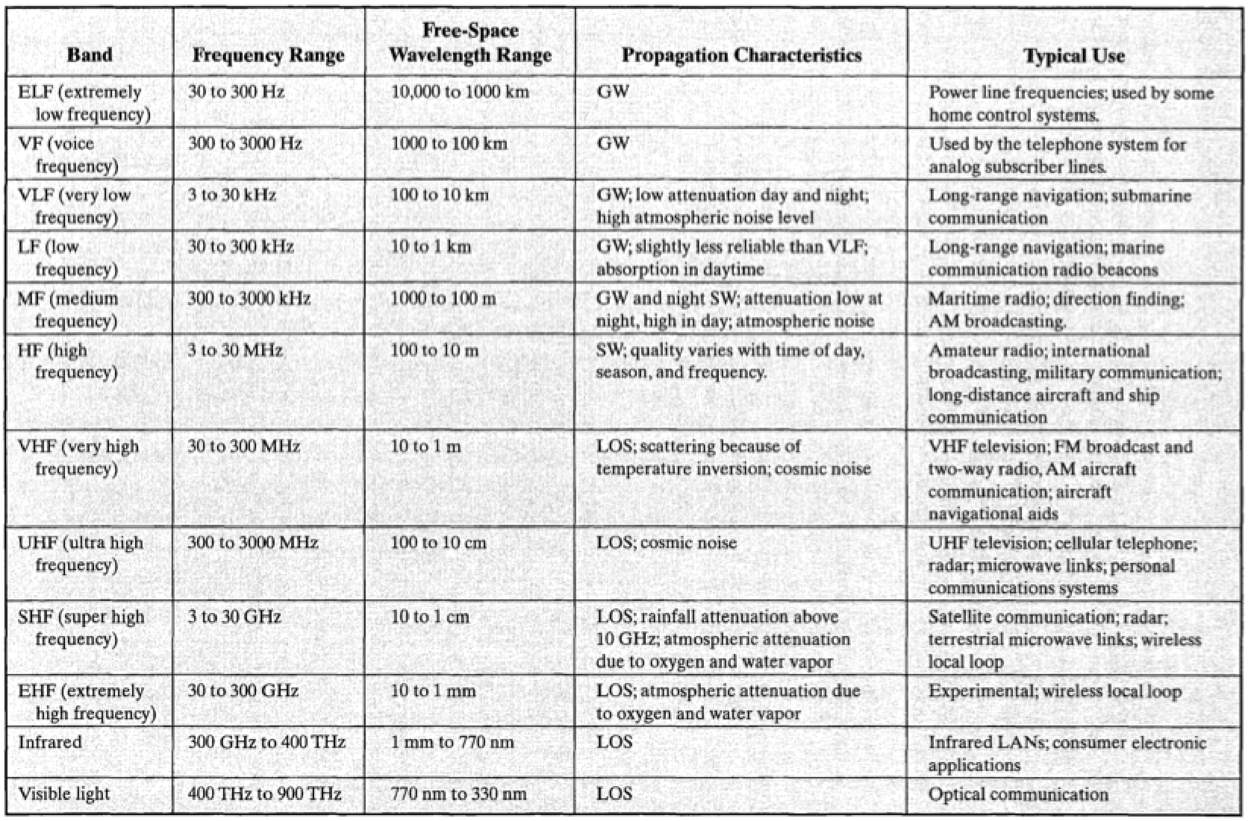
Choice of frequency band

Choosing a frequency spectrum above 30 MHz will limit transmission to LOS, and distant transmitters will not interfere with each other due to to reflection from the atmosphere. The greatest issue with choosing a frequency spectrum is a political one due to the growing popularity of microwave transmissions. Agencies make sure that the spectrum areas do not overlap and interfere with each other and therefore strict regulations are put in place Stalling (2005). The scope of this report includes choosing a range of possible spectrums. The Nyquist formula indicates that doubling the bandwidth doubles the data rate (with all other variables being equal). But higher data rates are also more affected by noise, so the error rate increases with higher data rates (for a given noise level). The maximum channel capacity obeys the equation: $C = B \cdot \log_2(1 + \text{SNR})$ Where SNR is signal-to-noise ratio which is the ratio of the power in the signal to the power of the noise. B is the bandwidth and C is the maximum channel capacity. Simply put, the wider the bandwidth, the more noise is admitted to the system. As B increases, SNR decreases Stalling (2005)

Since LOS communication is preferred, only frequencies above 30 MHz are considered, and choosing a spectrum comes down to choosing with these parameters in mind:

- Range and robustness. The lower the frequency the greater the range.
- Bandwidth. The higher the frequency the greater the bandwidth (which means greater data rates).
- Environmental factors, that is cosmic noise and attenuation due to water.

From Figure 4.12 and 4.13 some spectrums can be ruled out. Optical communication (visible light) and infrared both incur a too high risk of drowning in interference. The EHF band is ruled out since it is experimental and the benefits of high data rate are overkill. The SHF band (above 10 GHz) has the same disadvantage as the EHF band with attenuation from water. Since the application of this device is for outdoor use, it would make no sense to chose a band with these inherent risks. The conclusion is to chose a frequency in the range from 30 MHz to 10 GHz (ie, the UHF band and the lower part of the SHF band up to 10 GHz).



Band	Frequency Range	Free-Space Wavelength Range	Propagation Characteristics	Typical Use
ELF (extremely low frequency)	30 to 300 Hz	10,000 to 1000 km	GW	Power line frequencies; used by some home control systems.
VF (voice frequency)	300 to 3000 Hz	1000 to 100 km	GW	Used by the telephone system for analog subscriber lines.
VLF (very low frequency)	3 to 30 kHz	100 to 10 km	GW; low attenuation day and night; high atmospheric noise level	Long-range navigation; submarine communication
LF (low frequency)	30 to 300 kHz	10 to 1 km	GW; slightly less reliable than VLF; absorption in daytime	Long-range navigation; marine communication radio beacons
MF (medium frequency)	300 to 3000 kHz	1000 to 100 m	GW and night SW; attenuation low at night, high in day; atmospheric noise	Maritime radio; direction finding; AM broadcasting.
HF (high frequency)	3 to 30 MHz	100 to 10 m	SW; quality varies with time of day, season, and frequency.	Amateur radio; international broadcasting, military communication; long-distance aircraft and ship communication
VHF (very high frequency)	30 to 300 MHz	10 to 1 m	LOS; scattering because of temperature inversion; cosmic noise	VHF television; FM broadcast and two-way radio, AM aircraft communication; aircraft navigational aids
UHF (ultra high frequency)	300 to 3000 MHz	100 to 10 cm	LOS; cosmic noise	UHF television; cellular telephone; radar; microwave links; personal communications systems
SHF (super high frequency)	3 to 30 GHz	10 to 1 cm	LOS; rainfall attenuation above 10 GHz; atmospheric attenuation due to oxygen and water vapor	Satellite communication; radar; terrestrial microwave links; wireless local loop
EHF (extremely high frequency)	30 to 300 GHz	10 to 1 mm	LOS; atmospheric attenuation due to oxygen and water vapor	Experimental; wireless local loop
Infrared	300 GHz to 400 THz	1 mm to 770 nm	LOS	Infrared LANs; consumer electronic applications
Visible light	400 THz to 900 THz	770 nm to 330 nm	LOS	Optical communication

Figure 4.12. Frequency bands table Stalling (2005)

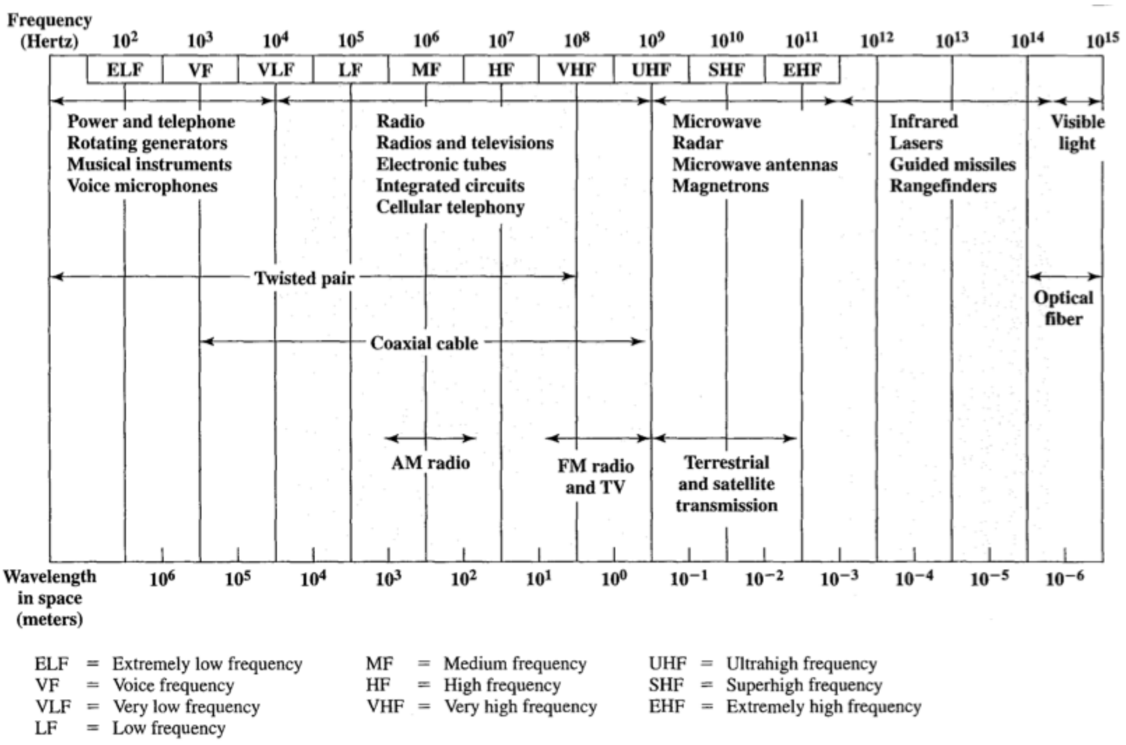


Figure 4.13. Electromagnetic Spectrum for Telecommunications Stalling (2005)

Spread spectrum modulation techniques

Simply put, *spread spectrum* means spreading a signal over a frequency spectrum. For example, the common 802.11b standard for wireless communication uses the 2.4 GHz band between 2.4000 and 2.4835 GHz. Each channel on this band is 22 MHZ wide. The same signal can be sent over multiple channels to increase robustness.

Spread spectrum systems are broadly classified by IIT (2014) as:

- Direct sequence spread spectrum (DSSS) systems
- Frequency hopping spread spectrum (FHSS) systems
- Time hopping spread spectrum (THSS) systems.
- Hybrid systems, which are combinations of any of the above.

Two main spread spectrum modulation techniques will be evaluated; Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS).

Both FHSS and DSSS are good at dodging interference from conventional sources (that is signals on a narrow frequency band). Focus in this chapter is to compare the technologies with only a brief description of the low level functionalities. The signal in FHSS is broadcast over a seemingly random series of radio frequencies, as shown

Table 4.4. Spread spectrum modulation techniques merits and demerits

Spread spectrum modulation	Merits	Demerits
DSSS	• Simpler to implement • Low probability of interception • Can withstand multi-access interference reasonably well	• Code acquisition may be difficult • Susceptible to Near-Far problem • Affected by jamming
FHSS	• Less affected by Near-Far problem • Better for avoiding jamming • Less affected by multi-access interference	• Needs FEC (Forward Error Correction) • Frequency acquisition may be difficult

schematically in Figure 4.14. The signal in DSSS spreads across a wider frequency band compared to FHSS. DHSS centers its communication on one frequency, and spreads out the same transmission on multiple channels (higher and lower than the center frequency). The width of the frequency band is proportional to the number of bits used, for example a 10 bit code is spread across a frequency band that is 10 times greater than a 1-bit code Stalling (2005). Practical merits and demerits of the two technologies is presented in Table 4.4.

If multiple FHSS transmitters operate on the same band, it is likely that one or more of them will hop to the same frequency causing interference and retransmission or discarding of data. A DSSS system on the other hand handles interference better since the same data is transmitted on multiple channels simultaneously, but this is only true up to a certain point where high interference will drop throughput to nearly zero. In high interference conditions FHSS has higher performance since it is more likely that at least one channel is relatively noise free. Also, in a FHSS system the transmission energy will only be spent on one channel at a time, and not be spread out on multiple channels as in a DHSS system. In essence, FHSS degrades more gracefully and is more predictable in the presence of interference arcelect (2014). Robustness and graceful degradation are considered more important than data throughput, and therefore FHSS is our recommended technology.

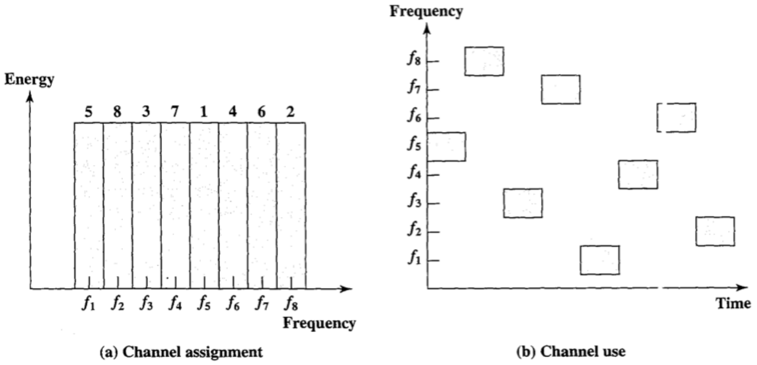


Figure 4.14. Every channel in the designated frequency band uses the same amount of energy during transmission, as shown on the left figure. But only one channel is active at a time, as shown in the example of a hopping scheme in the right figure. Stalling (2005)

4.9.4 Basis for choice of communication devices for proof of concept

The proof-of-concept prototype does not necessarily need to follow every design target as a commercial product. To implement the wireless communication we will limit the choices to unlicensed frequencies and easily accessible circuit components. The evaluated systems should have a range of 100 m. Communication between more than two nodes (i.e. mesh network) will not be necessary. For security concerns, pairing a remote with only one truck is also preferable. Reliability and development time was chosen as the most important criteria when choosing the wireless solution. Higher reliability and lower development time will be achieved by:

- In-house developed protocol for communication will not be preferred compared to a ready-made protocol.
- Error checking built into the communication protocol.

A quick market survey revealed a huge number of possible implementations of wireless communication that fulfills all our requirements. Rather arbitrarily we choose to inspect the following:

1. Xbee
2. Xbee pro
3. Bluetooth
4. Nordic
5. Wifi

Table 4.5. Weights for each category

Importance (1-10)	
10	Range
5	Power consumption
2	Price
10	Time to working prototype
10	Error checking in protocol

Table 4.6. Evaluation matrix of different wireless solutions

Scale (-5 to 5)					
Xbee	Xbee pro	Bluetooth	Nordic	Wifi	General RF
0	2	-2	-3	0	-3
0	-3	-2	3	-3	3
0	-2	0	3	-3	3
0	0	-2	-2	-3	-2
0	0	0	0	0	-2
=	=	=	=	=	=
0	1	-50	-29	-51	-49

6. General RF

The XBee is the reference system and by comparing all the other alternatives to this using the weighted categories in Table 4.5, the best alternative can be selected. A higher weight means that the category is more important. In Table 4.6 the solutions are compared and the summation at the bottom shows the best solution. A positive number indicates that it is better than the reference, and a negative value indicates that it is worse.

4.9.5 Discussion and decision of wireless communication for proof-of-concept

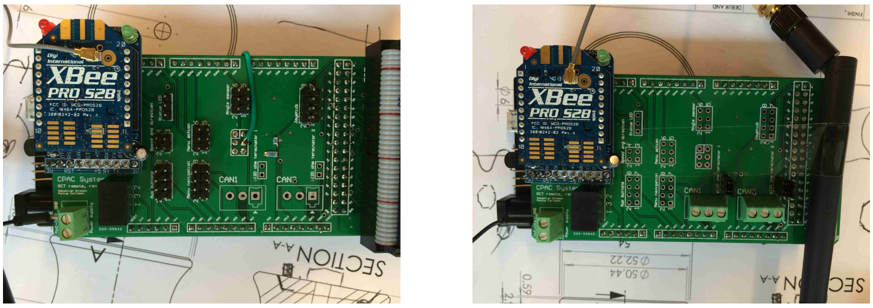
Xbee Pro Series 2 will satisfy our requirements. The solution incorporates IEEE 802.15.4 and less development time will be spent with developing a reliable communication since reliability functions are included into the protocol. The protocol implements full handshake between transmitter and receiver. For avoiding collisions with other wireless devices it has a CSMA/CA feature.

4.10 Electronics design targets

Once the communication device and technology has been chosen, these need to be integrated into an electronic system. Two Electronic Control Units (ECUs) will handle the communication; one in the remote controller and one in the receiver (in the truck). Design targets for the ECUs for both of these are listed below. Also listed are brief descriptions of how the design target was met.

- Micro controller for reading sensors and handle communication
  - Atmel SAM3X8E ARM Cortex-M3 on a Arduino Due board
- Incorporate wireless communication
  - XBEE Pro S2B is the chosen solution (see Table 4.6)
- CAN bus communication on the receiver device
  - MCP2551 CAN tranceiver which is fully compatible with the CAN bus connection on the micro controller.
- Voltage regulation from a battery or generator to appropriate voltage necessary for sensors and the micro controller. The controller ECU should also be energy conservative since it will run from battery.
  - A buck converter (Recom R-785.0-0.5) is used instead of a linear converter. The reason is to reduce power consumption since linear regulators waste energy by dissipating excess power as heat. The buck converter has a efficiency of 97%.
- The PCB should be easy to assemble and connect
  - Reasonably small components and spacing between components for manual soldering are used.
- Robustness from noise and vibrations are important. The PCB has to remain robust in an automotive environment.
  - Ground planes on both sides of the PCB minimize spurious ground voltage differences. The main usage of the ground planes is to provide a low impedance return path for high-frequency currents.
  - Decoupling capacitors help stabilize the voltage delivered to active digital devices by providing a local source of charge if the power suddenly drops.

Two boards are necessary; one in the remote and one in the truck. Both boards will need power supply, radio communication module, processor. The PCB in the remote will need sensor reading (ADC and SPI). The PCB in the truck will need CAN communication. Apart from these previously mentioned features, the boards will resemble each other more than they differ. In an effort to minimize work, two board layouts were combined on the same PCB. This means that conductive tracks for both applications are put into the same layout. During assembly, only the components belonging to either variant is put onto the board. For example the sensor and LCD connectors to the controller PCB, and CAN transceivers and CAN connectors to the receiver PCB. A side by side of the boards can be seen in Figure 4.15.



(a) Controller

(b) Receiver

Figure 4.15. PCBs for the controller and the receiver compared

General PCB design guidelines

Surface mounted components are space efficient and easy to solder by hand if chosen correctly. The component standardized package size 2012 (2.0 mm x 1.25 mm) is chosen since they are large enough to be reasonably easy to solder, but still small enough for the board to accommodate the necessary components. Choosing smaller components would make some parts of the soldering much more difficult. Ground layers were placed on both the top and the bottom of the board. This is a general design recommendation when doing PCBs since it makes the board less sensitive for disturbances. It also makes sense in the way that almost all components need to have a ground connection.

When designing PCBs certain capabilities of the factory doing PCB manufacturing has to be taking into consideration. In our case for example, no traces (ie connections between two points) can be below 8 mil (0.2 mm) and no holes can be less than 0.25 mm in diameter. These limitations are derived from tolerance specifications on the machines used for etching and drilling.

ECAD design

Altium Designer, *Altium Designer* (2014), was used to design the circuit boards. Simulations in the software is extensive but the most necessary tools are EDC and DRC:

EDC (Electrical Rule Check) can identify violation of certain electrical rules:

- Checks if every component on the circuit board has the minimum amount of pins routed (for example power supply and ground).
- Checks electrical errors (for example if two outputs are connected).
- Consistency check to make sure that the schematics and the board layout include the same components.

DRC (Design Rule Check) checks the designed board against the constraints of the board manufacturer. Our constraints towards the manufacturer are primarily:

- Distances from any routing to the edge of the board or to drilled holes including vias (ie. conductive holes between two layers on a board providing electrical connection between a trace on one layer to a trace on another layer).
- The size of the routing is important since manufacturers will not be able to print under a certain dimension with enough precision to avoid routes being connected by mistake. In our case the distance between routes has to be minimum 8 mils.
- Routing analysis to inspect route networks, for example to see which components has a 3.3V power supply and if routes are overlapping.

4.11 Software design

There are three programmable devices in the design, two Arduino micro controllers and one Autobox. The Arduinos were programmed in C++ using a real-time operating system. The Autobox was programmed with code generated from Matlab/Simulink. This chapter describes the code in more detail.

4.11.1 Software design architecture

The Simulink model shown in Figure 4.16 reads CAN messages for the sampled inputs from the controller and sends them to the filter. The filter outputs references of speed and steering angle to an existing model done by Volvo Group. The Simulink model also sends out CAN messages with information about the truck so the driver gets feedback on speed and possible fault signals. The watchdog subsystem in Figure 4.16 sends out an integer value that is incremented for each CAN message. The watchdog thread in the remote controller then replies with the exact same value.

By monitoring the returned value and verifying that it is not static (that the value is actually changing over time) the model knows that the communication works. If it stops working, the model calls for full brake and the vehicle will stop.

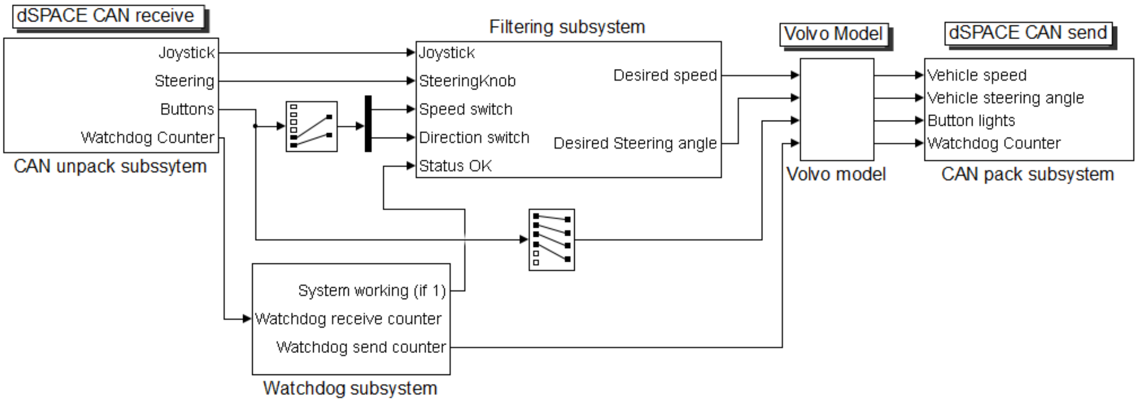


Figure 4.16. Autobox simulink model

The software is derived from the functional model from Figure 4.2 and is coded in C++ assisted with Arduino libraries. A realtime operating system is used to run multiple threads concurrently. The receiver code represented in Figure 4.17 is very basic, two threads running in parallel where one receives the incoming CAN messages and sends a XBee message to the remote controller, and the other receives XBee messages and sends CAN messages to the truck. The remote controller represented in Figure 4.18 is more complex with 5 threads running. Each thread is periodic with the frequency shown in Table 4.7. By measuring the time from start to finish on each thread running alone, an estimation of the worst case execution time can be made. The worst case execution time when just one thread is running can be used with different scheduling techniques to determine if a system is feasible or not. The resolution of the timer in the cpu is $8\mu s$. Therefore the last digit in the execution time is rounded up by $0.01ms$.

The frequencies are somewhat ad-hoc, the buttons thread contains low-pass filtering of analog inputs and by doing this 20 times as fast as the actual use of the signal a smoother signal can be achieved. The wireless module has a practical send rate at 20 Hz. Therefore the send task will have a frequency of 20 Hz. When receiving a package, a delay of $\approx 5ms$ is acceptable meaning that the thread needs to poll and check if a message is available 200 times a second. The screens execution time allows only 2 frames per second to be generated. The watchdog thread should be a few

Table 4.7. Threads period and worst case execution time

Thread	Frequency [Hz]	Period [ms] p_i	Worst Case Execution time [ms] e_i
Buttons	500	2	0.17
Input	20	50	2.10
Receive	200	5	0.08
Screen	2	500	290.3
Watchdog	100	10	0.02

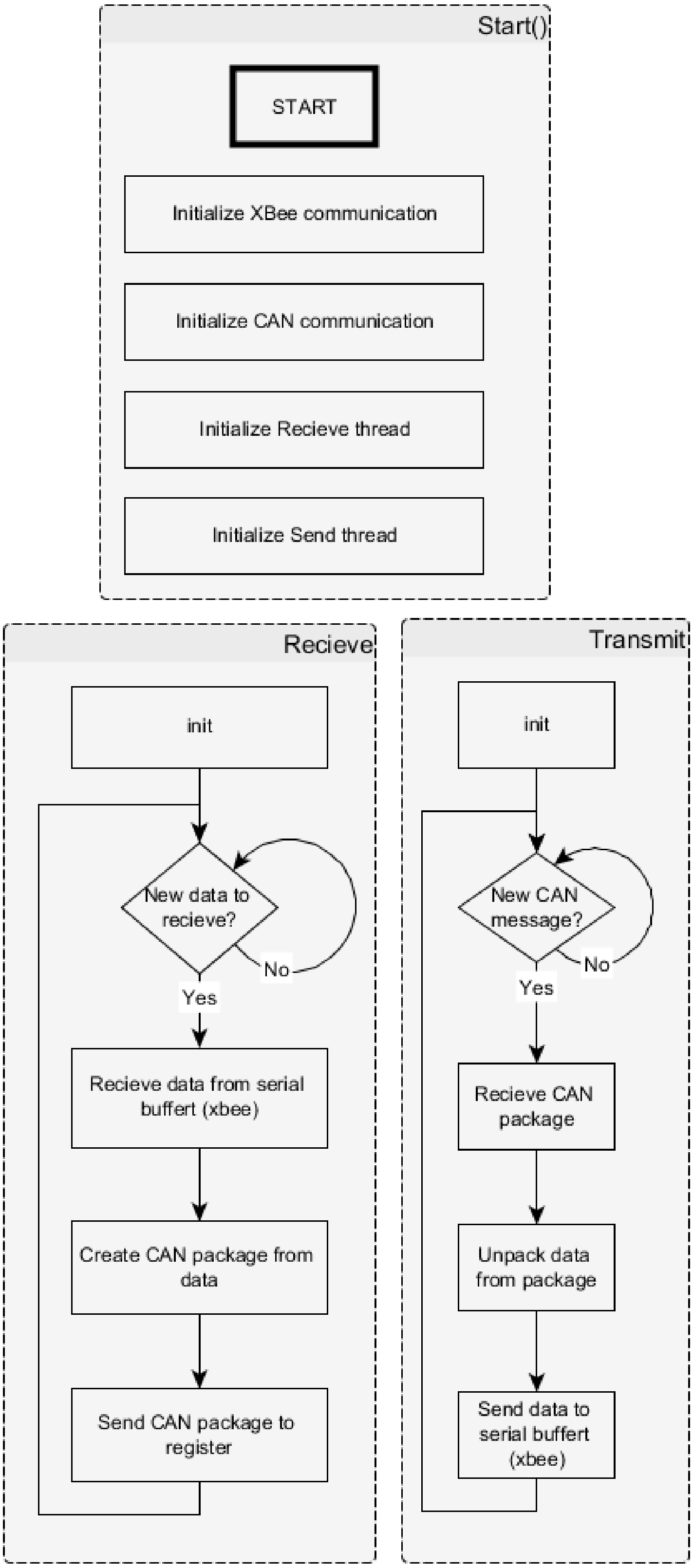

Start()
START
Initialize XBee communication
Initialize CAN communication
Initialize Recieve thread
Initialize Send thread
Recieve
init
New data to recieve?
No
Yes
Recieve data from serial buffert (xbee)
Create CAN package from data
Send CAN package to register
Transmit
init
New CAN message?
No
Yes
Recieve CAN package
Unpack data from package
Send data to serial buffert (xbee)

Figure 4.17. Receiver architecture

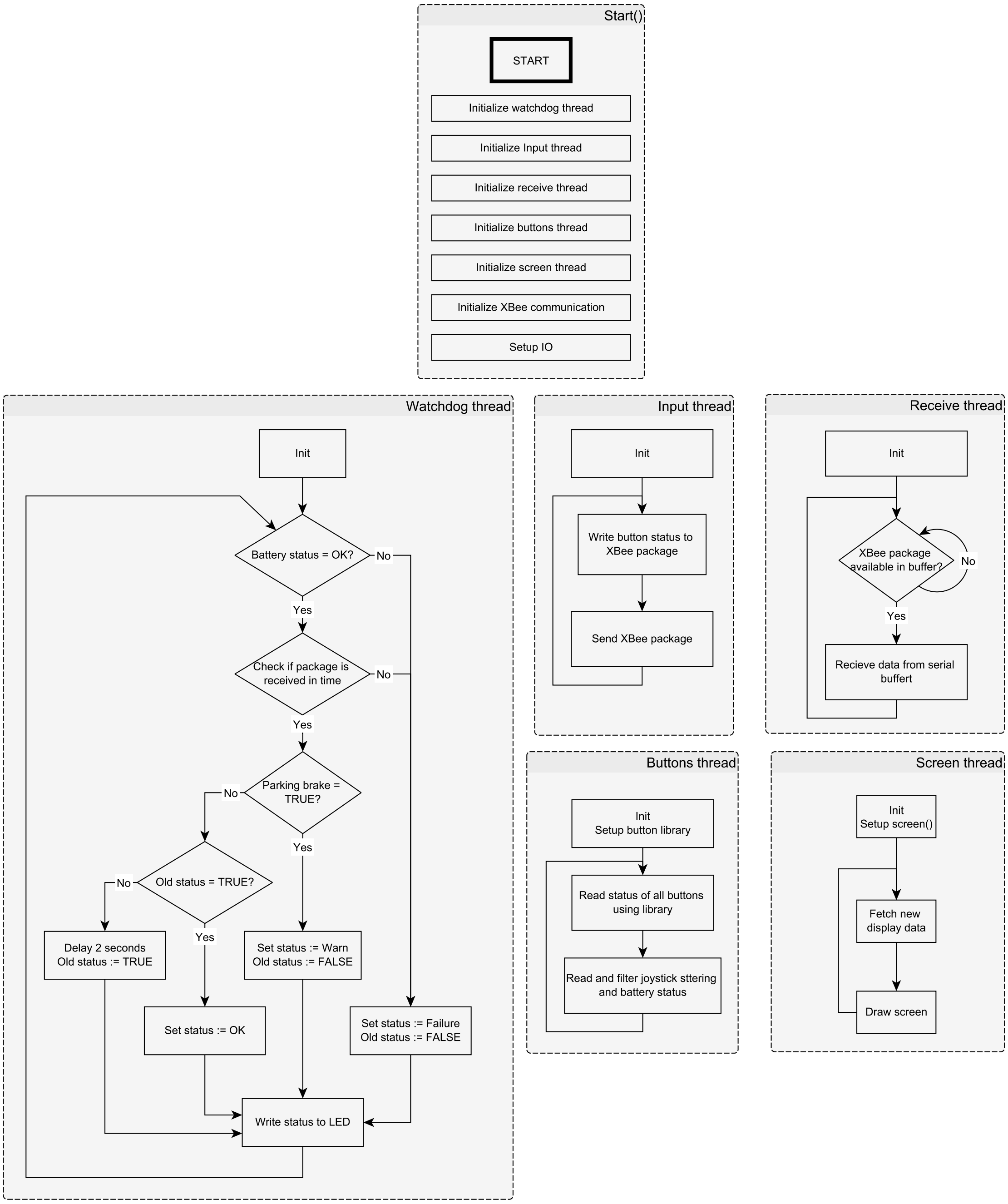


Figure 4.18. Controller architecture

times faster than the actual communication which is the send rate 20 Hz, therefore 100 Hz is reasonable.

4.11.2 Schedulability

In the controller a real time operating system (RTOS) is needed to be able to do multiple tasks in what looks to be real time. To be able to schedule the threads, the RTOS needs some information about the threads running. Each task can have a:

- Release time: When the thread wants to start.
- Start time: Thread gets time to run
- Execution time: Total cpu time the thread needs to finish
- Preemption: Time when the RTOS pauses the thread to run another more important task
- Resumption: Task restarts after being preempted
- Finish time: Time when task finishes
- Response time: Equal to the finish time minus the release time
- Deadline: Time when task must be done

Those times are visualized in Figure 4.19. This information is important for a RTOS scheduler to make correct decisions when a given thread should have CPU time. There is a difference in execution time and response time which is important to understand. The execution time is the time when the thread actually executes, and the response time is the time when the thread would like to execute, meaning that when a thread gets preempted by another thread, it only affects the response time and not the execution time. The worst case execution time is therefore the longest time a single thread running alone will take.

The RTOS scheduler cares about three things when deciding to execute a task. What processor to run the task on, in what order the tasks are executed and the start time of each task. Depending on what kind of scheduler is implemented in the RTOS the execution will be either static or dynamic or a mix of these. A fully-static scheduler have everything decided before it starts, meaning that each cpu will know beforehand what thread should be executed at a given time. A fully-dynamic scheduler, on the other hand, decides what thread should run at each timestep. Also, a scheduler can be preemptive or non-preemptive, meaning that if it is preemptive it has the ability to preempt a thread (pause the thread) for another higher priority thread to run. Non-preemptive scheduling does not have that ability. Lee and Seshia (2011)

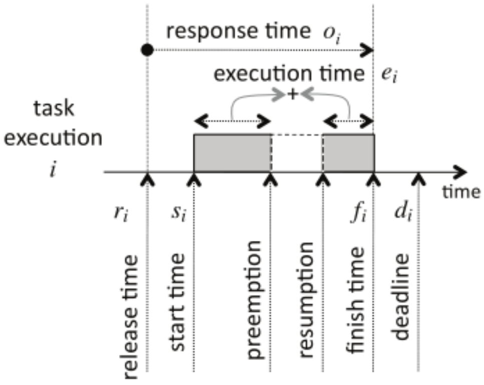


Figure 4.19. Scheduling times

In short, there are two parameters that the programmer can design the threads for, the period between each release time and the deadline for each task. Often threads will run periodically meaning that the time between each release time will be the same. Depending on what the thread is doing, it could be more or less critical that the thread is executed close to its release time. A thread doing sampling is an example of a thread that in almost all cases needs to execute with the same timing each time to minimize sample jitter. If no deadline is given, it is assumed to be the same as the period, meaning that the task has to finish before the next release time. A reason to specify an earlier deadline is if the task's period is longer than the desired maximum delay of some output from the task. The deadline has to be larger or equal to the execution time and smaller or equal to the period.

FreeRTOS *FreeRTOS* (2014) is the RTOS implemented and it has a preemptive fully-dynamic priority-based scheduler, and tasks with the same priority are executed using a round-robin method. A task with lower priority will be preempted when a task with higher priority is released. If two tasks have the same priority the RTOS switches between them with a predefined frequency to let them run simultaneously. FreeRTOS does not support deadlines.

Rate Monotonic Scheduling

By using rate monotonic scheduling (RMS) the priority of each thread can be decided. The priority is ranked by each task's period, the shorter the period the higher the priority. Table 4.8 shows the priorities for the implemented threads. The schedule was introduced by Liu and Layland (1973) and assumes the following:

- Only periodic tasks
- Deadline is equal to tasks period ($d_i = p_i$)
- Execution times are known (e_i)

- No sharing between threads
- Tasks may not suspend themselves
- Each task should have a unique priority
- Switching between tasks takes zero time, “ideal”.

The deadlines are met for a rate monotonic scheduling if Equation 4.1 is true. Where n is the number of threads being scheduled, e_i is the worst case execution time and p_i is the period.

$$\sum_{i=1}^{n} \frac{e_i}{p_i} \leq n \left(2^{1/n} - 1\right) \tag{4.1}$$

By putting into (4.1) the values from Table 4.7, as shown by (4.2) all deadlines are met with a small margin. The assumption that the RTOS is “ideal” is not correct in practice, therefore a too small margin might make the schedule infeasible. The result from (4.2) has less than 2% margin which is not enough to guarantee a feasible scheduler in practice.

$$\sum_{i=5}^{i=1} \frac{e_i}{p_i} \approx 0.7256 \leq 5 \left(2^{1/5} - 1\right) \approx 0.7435 \tag{4.2}$$

Scheduling by thread importance

Since some tasks are more important from a safety critical point of view, the priority can be based on this. The problem might then be that some tasks do not meet their deadline. This can be verified by calculating the worst case response time and verify that it is lower than the deadline.

Sampling inputs and sending them to the receiver is the most important task and therefore it has the highest priority. The screen has no relation to safety which makes it the lowest priority. To make sure that the button, send and receive tasks are running correctly, the watchdog thread must have lower priority than these, this has to do with the way that the watchdog thread is implemented. This priority layout does have the advantage that if for some reason the execution times increases the watchdog will stop working before the more important threads which means that the system will detect the fault.

Worst case response time

The worst case response time is calculated using generalized rate monotonic analysis Årzén et al. (2012). The calculation assumes that the lowest priority thread will be preempted by higher priority threads, and by summation of worst case execution time for each thread multiplied by their periods a worst case response time can be calculated.

$$r_i = e_i + \sum_{\forall j \in hp(i)} \left\lceil \frac{r_i}{p_j} \right\rceil e_j \tag{4.3}$$

The set $hp(i)$ contains tasks with higher priority than task i. r_i is a function of itself and calculation is done recursively until r_i becomes static or larger than the deadline for the current thread. If the deadline is not met by this calculation the schedule is infeasible. This can be used to show that a specific scheduling technique is feasible.

$$r_i^{n+1} = e_i + \sum_{\forall j \in hp(i)} \left\lceil \frac{r_i^n}{p_j} \right\rceil e_j \tag{4.4}$$

Table 4.8 shows the worst case response times calculated by Equation 4.4. By this analysis each thread in both priority layouts meet their deadline with fairly good margin. The analysis done in (4.2) is only possible when using rate monotonic scheduling and can not be applied to any arbitrary priority layout.

Table 4.8. Thread priority depending on rate monotonic scheduling and task importance, where the deadline is equal to the period

Thread	Period [ms]	Priority RMS	wcrt	Priority by importance	wcrt
Buttons	2	1	0.2	1	0.2
Receive	5	2	0.3	3	2.6
Watchdog	10	3	0.3	4	0.2
Input	50	4	2.6	2	2.5
Screen	500	5	339.8	5	339.8

4.11.3 Filtering

The reference output generated from the Simulink model directly affects the vehicle. If slow braking is desired, simply setting the reference to zero will not work, since it makes the truck halt with full braking power. The reference has to be filtered and smoothed in order to achieve the desired behavior. This has to be done without building in too much delay into the filtering.

A quick engineering idea was to simply take an integrator in a feedback loop and saturate the control signal in the loop with a variable saturation. By this, controlling the speed of convergence between the reference speed and the joystick value is possible. See Figure 4.20.

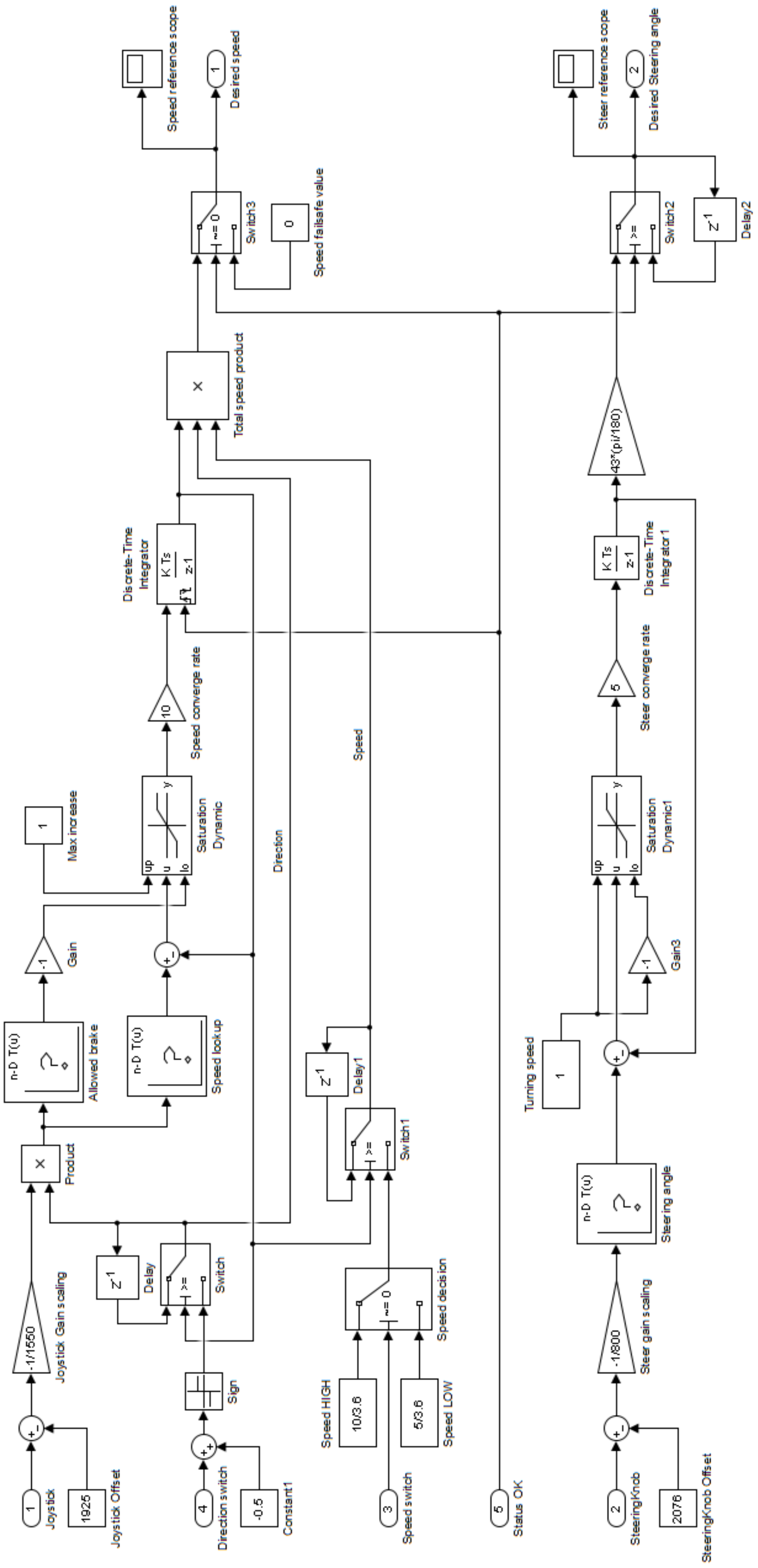


Figure 4.20. Simulink smoothening filter

Verify stability

The filter used in Figure 4.20 is a saturation in series with an integrator. Stability can be proved using the circle criterion. If a nonlinearity is bound within two linear functions the coefficients for those bounds can be used to prove stability Torkel Glad (2000). By drawing a Nyquist diagram of the linear system and a circle between $-\frac{1}{k_1}$ and $-\frac{1}{k_2}$. Where k_1 is the coefficient of the lower bound and k_2 is the coefficient of the upper bound, the system is stable if the linear system does not enter this circle Assuming that the saturation's lower limit is negative and its upper limit is positive, the Nyquist diagram will be as in Figure 4.21. The circle has its bounds between $-\infty$ and -1 and therefore we have a stable system.

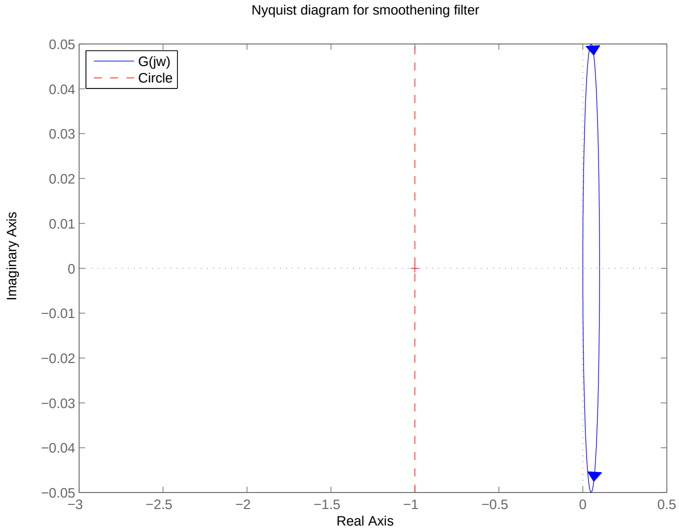
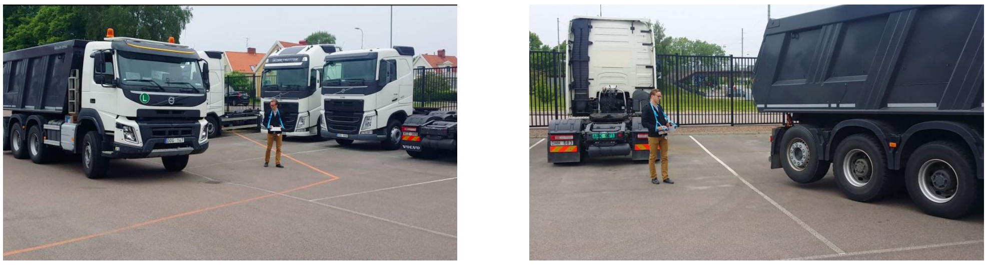


Figure 4.21. Circle criterion for the designed filter, showing stability

4.12 Testing of proof-of-concept

Testing of the proof-of-concept controller was done with satisfying result. The whole process from interaction on the controller to actuation on the truck worked well enough for the concept to be proven possible. The wireless communication between the controller and the receiver was robust. CAN bus communication between the receiver and the Autobox worked as intended, and the integration of our Simulink model into Volvo's Autobox model was successful. Signal filtering all the way from the controller to the actuator worked without any noticeable noise interference and the lag from the controller to actuation on the truck was not noticeable. Two test were done to check the basic functionality of the system:

1. Driving on a line and stopping at set intervals to emulate safety barrier installation. See Figure 4.22a (left)
2. Reversing into a parking space, see Figure 4.22b (right)



(a) Safety barrier installation

(b) Reversing into parking space

Figure 4.22. Testing of the proof-of-concept

Some things did not work as intended. The display and the LED indicator were too dim to be easily readable in outdoor conditions. Also the steering knob is a bit slippery. At the extreme positions the springback force is relatively high, and the steering knob needs to be held firmly for it not to slip. It might be a good idea to use nonlinear spring where the springback force is less in the extreme angles.

5 DISCUSSION

5.1 Safety analysis discussion

Remember the purpose of this work:

1. Creating a set of requirements and specifications that an implementation of a remote controlled truck needs to fulfill.
2. Demonstrate by a proof-of-concept on a physical system, to show that some, but not all, requirements could be fulfilled.

The safety analysis had the aim to state clear functional safety requirements that must be implemented in order to create a safe product. First thing to discuss is the safety goal "Driver must be aware of obstacles in vehicle path". This goal needs a more in-depth study that analyze how operators actually behave using the remote controlled product in order to break this goal down into requirements. Depending on how the operators behave, different safety functions may be required like external sensors around the truck to detect obstacles or camera views fed to the controller to aid the operator. A beeping sound emitted from the truck could also be used to warn bystanders that the operator might have less visual awareness (like a truck does when reversing). Maybe it is enough with warning messages from the controller to make the operator aware about the dangers.

Another factor that needs more data is the allowed delay and the update frequencies in the remote system. Some data about this was collected from other systems in Chapter 4.3 to determine good estimates of acceptable requirements. As those are estimations they need to be verified. The controller built in this project is a perfect platform to perform such tests on, adding delays into the system and having a test group to analyze when the delay is noticeable. Also the fault tolerant time needs to be decided, the actual time that can be allowed from when a fault occurs to when the accident actually happens. This time is critical and the system must be able to degrade or enter safe-state within this time. The requirement that the truck is not allowed to move faster than 10 km/h makes all the other requirements have lower ASIL level, since the hazards are not as fatal. In order to make a remote system that actually drives faster than this, a more detailed hazard analysis needs to be done. The number of FSR will increase and probably also the level of them.

5.2 Solution model for proof-of-concept

The solution model proves a good-enough approach to implementation of wireless control of a truck, but only as a proof-of-concept. Our recommendation is to still use Autobox, Simulink and the inhouse CAN bus modules for further development and testing until satisfactory functionality is reached. Therefore implementation of actual production grade components would need to take place.

5.3 Mechanical design and human-machine interface

Overall the mechanical design of the controller was good enough for the purpose of testing. The most important design flaw is the steering knob that would need further development. When the steering knob is released it has a stable oscillation around equilibrium. A wanted behavior is critical damping where no oscillations would occur close to equilibrium and releasing the steering knob would make it calmly return to the center. Overly-damped behavior could also be evaluated up to the point where the steering knob feels sluggish.

The beams on the side of the mechanical construction was a result of a rapidly created cardboard model, where the belts collided with the operators arms without the beams.

5.4 Communication

In order to reach the requirements with high enough update rate of 100 hz, the 20 hz that the XBee produces is not enough. Other hardware is required in order to lower the latency and increase the send-rate and still keep good robustness of packages sent.

5.5 Electronics design

Our designed PCBs are proven to work for the proof-of-concept testing but they do contain some design flaws. If further research is to be done new PCBs should be manufactured where the design flaws are fixed. See Appendix D for a full list of found design flaws with a description for how they were fixed in post PCB-assembly.

5.6 Software and scheduling

The Simulink code generated into compilable C code for the Autobox was a really efficient way to create and simulate desired behavior. In the remote controller a real time operating system was used in order to easily do multiple tasks concurrently. Without it the screen functionality would have been hard to implement. For the prototype, the scheduler is feasible using any of the two proposed scheduling algorithms. The preferred technique should therefore be the thread by importance scheduling since it also had the advantage of handling unexpected increase in execution time.

5.7 Filtering

The filter did successfully filter out the mechanical oscillations from the steering knob sensor and created a smooth convergence towards the reference without introducing any significant delays.

6 CONCLUSION

Design and implementation of a safe and reliable wireless controller for remotely controlling a heavy vehicle is possible. It is certainly possible to use the already present actuators for controlling the vehicle. In our case the primary actuators are the electronic motor steering and control of the complete powertrain. One conclusion that can be made from this thesis is that taking advantage of controlling actuators by-wire will open doors for new functionality that increases the effectiveness of trucks.

6.1 Functional safety requirements

Some of the FSR need extra research in order to determine allowed delay and how truck drivers would behave when actually using the remote control system. The following FSR can be directly applied to the remote system and includes the FSR that needs extra research:

- Truck/Interface must follow speed setpoint
- Must detect speed setpoint larger than 10 km/h sent to interface
- Must be able to detect loss of speed setpoint or incorrect speed setpoint provided to interface
- Must be able to detect loss of steering setpoint or incorrect steering setpoint provided to interface
- If parking brake is not applied it shall not be possible to activate/deactivate the system
- If vehicle speed is not zero it shall not be possible to activate/deactivate the system
- Must be able to detect if speed setpoint is delayed more than Y time units
- Must be able to detect if steering setpoint is delayed more than Y time units
- Truck must follow steering setpoint

6.2 Communication

The conclusion drawn from the communication chapter is a list of recommendations for a remote controlled system for trucks, as follows:

- Propagation mode should be Line-of-sight (LOS) propagation. There is no benefit in using ground wave or sky wave propagation since the distance is far to small.
- Omnidirectinal antennas are recommended.
- Licensed spectrum are recommended to avoid disturbances in the so called "junk frequencies".
- Frequency should be below 10 GHz to avoid unnecessarily high attenuation from rainfall.
- Spread spectrum modulation technology should be used for robust communication. Frequency hopping modulation is the recommended choice since it degrades with more predictability with increasing interferance compared to direct-sequence modulation.

7 FUTURE WORK

This thesis focuses on the concept of remote control of a heavy vehicle. Further research and work could be done to investigate areas either left unexplored or just being scratched on the surface by this thesis. This section lists some of our recommendations for further research.

7.1 Testing

Extensive testing could be done to make sure that the system fulfills industry requirements. Basically each application listed in the Background section of this report could be tested, such as:

- Run a test with a concrete truck with a small crane.
- Asphalt paving truck with small chute
- Safety barrier installation
- Remote control of the truck from an aerial work platform.
- Safety hazardous situations where being present inside the truck is not favorable.
- Maneuvering in tight situations where being outside the truck is advantageous.
- In general controlling extra functionality by controlling Body Builder functions (such as tipper, lift, asphalt chute, ...) or regular truck functions (such as horn and lights).

7.2 Human-machine interface

In our opinion, useful results could be gathered from evaluating different human-machine interfaces for controlling the truck.

- Test more layout alternatives. Relocate buttons, switches, the wheel and the joystick and try to find an intuitive and an ergonomic working position for the operator.
- Compare steering with both joystick and a steering knob. Perhaps also try alternative controls for the velocity control.

- Touch screen to change controller settings or control vehicle actuators might be useful.
- Warning sounds from the controller or the truck could be looked into. For example, evaluate if a warning beep should be sounded when controlling the truck remotely just like when the truck is reversing; both to make the operator aware that remote control is active but also to notice bystanders.
- Dead-man's switch was not used in the proof-of-concept but it should be present on a commercial product. Evaluating different solutions for this would be useful, (eg, compare accelerometer, conductive sensors and a simple switch to check operator presence).
- Fisheye camera on one or multiple positions on the truck with a feed to the control display could be evaluated, to see if it would make truck operation smoother or safer.
- Ergonomics in general was only evaluated from a simplistic point-of-view where an approximate ergonomic design was targeted.

7.3 Functional safety

The safety concept was bound to functional safety and did not include technical requirements on the hardware or software level. In order to construct a full concept built around the ISO-26262 standard this would be the next step.

7.4 Communication

Further testing can be done on the wireless communication, starting with testing the recommended setup from this report and then compare it to other setups. Testing over a range of frequencies should be conducted under different scenarios, for example, attenuation from rain and obstacles. To test worst case performance at least some of the tests should be done with multiple transceivers present to emulate multiple vehicles all being wirelessly controlled. For safety and security considerations encryption schemes should be implemented and tested as well.

Bibliography

Altium Designer (2014). URL: http://www.altium.com/en/products/altium-designer/overview (visited on 07/02/2014) (cit. on p. 30).

Bohgard, Mats et al. (2008). *Arbete och teknik på människans villkor*. Prevent. ISBN: 978-91-7365-037-3 (cit. on p. 17).

FreeRTOS (2014). URL: http://www.freertos.org/ (visited on 05/22/2014) (cit. on p. 36).

IIT, Kharagpur (2014). *Spread Spectrum and Multiple Access Technique*. URL: http://nptel.ac.in/courses/Webcourse-contents/IIT%20Kharagpur/Digi%20Comm/pdf-m-7/m7138.pdf (visited on 05/22/2014) (cit. on p. 25).

ISO-26262 (2011). *Road vehicles – Functional safety*. ISO 26262-x:2011. Geneva, Switzerland: International Organization for Standardization (cit. on p. 4).

Lee, Edward A. and Sanjit A. Seshia (2011). *Introduction to embedded systems: a cyber-physical systems approach*. English. Morrisville, NC: Lulu Enterprises. ISBN: 0557708575; 9780557708574. URL: www.summon.com (cit. on p. 35).

Liu, C. L. and James W. Layland (Jan. 1973). "Scheduling Algorithms for Multiprogramming in a Hard-Real-Time Environment". In: *J. ACM* 20.1, pp. 46–61. ISSN: 0004-5411. DOI: 10.1145/321738.321743. URL: http://doi.acm.org.proxy.lib.chalmers.se/10.1145/321738.321743 (cit. on p. 36).

Schwartz, Mischa (2005). *Mobile wireless communications*. New York: Cambridge University Press. ISBN: 0-521-84347-2 (cit. on p. 23).

Stalling, William (2005). *Wireless Communications and Networks*. Pearson Prentice Hall. ISBN: 0-13-191835-4 (cit. on pp. 21–27).

Theam (2014). *Theam Applications of mixer mounted concrete conveyor belts*. URL: http://www.theam.com/UK/theam-applications.php (visited on 05/22/2014) (cit. on p. 1).

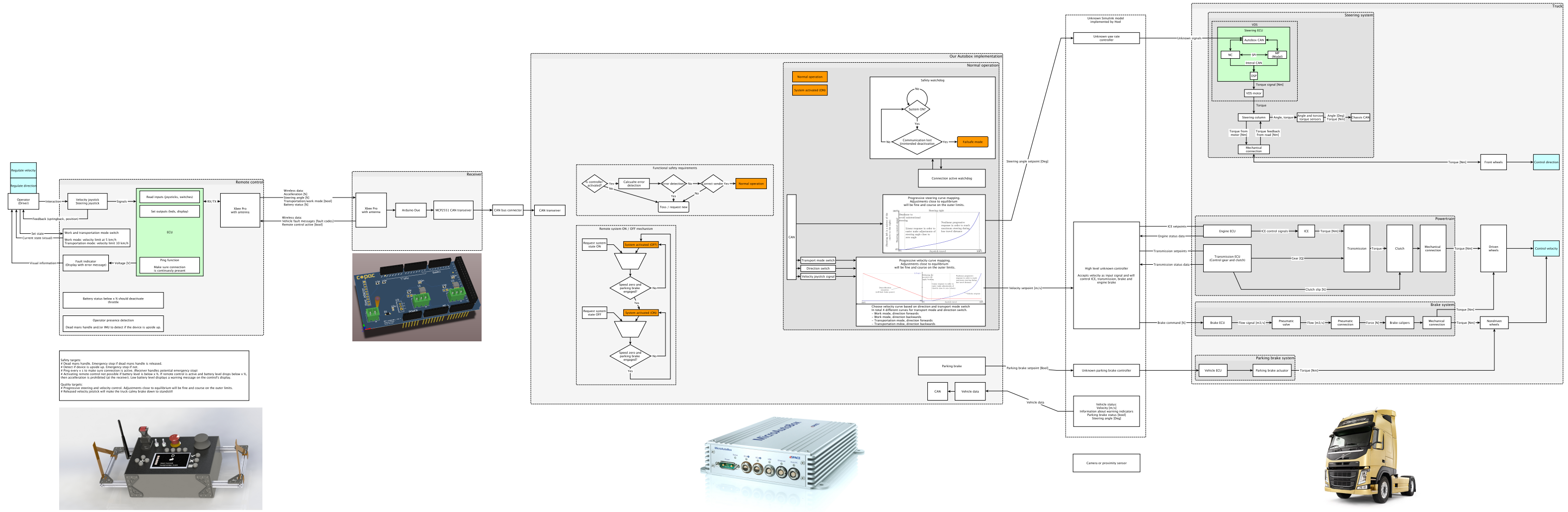
Torkel Glad, Lennart Ljung (2000). *Control Theory Multivariable and Nonlinear Methods*. London: Taylor&Francis. ISBN: 0-7484-0877-0 (cit. on p. 40).

arcelect (May 22, 2014). *DSSS and FHSS - Spread Spectrum modem*. URL: http://www.arcelect.com/dsss_fhss-spead_spectrum.htm (cit. on p. 26).

Årzén, Karl-Erik et al. (2012). *Real-Time Control Systems*. Technical report. Lund Institute of Technology and The Royal Institute of Technology (cit. on p. 37).

Appendix A

Solution model

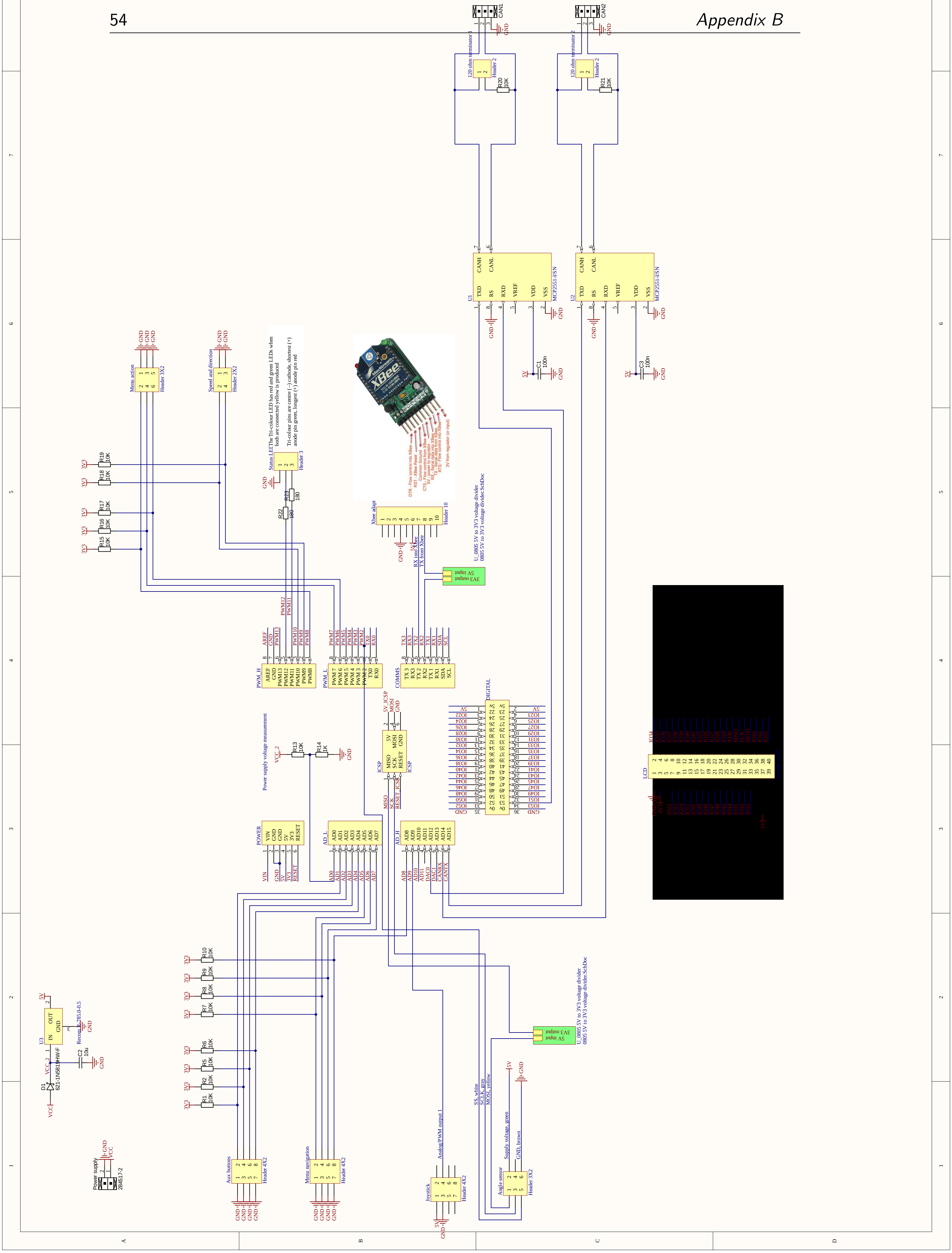

Regulate velocity
Regulate direction
Operator (Driver)
Interaction
Feedback (springback, position)
Set state
Current state (visual)
Visual information
Remote control
Velocity joystick Steering joystick
Signals
Read inputs (joysticks, switches)
Set outputs (leds, display)
ECU
Ping function
Make sure connection is continuesly present
Voltage [V]
Fault indicator (Display with error message)
Work and transportation mode switch
Work mode: velocity limit at 5 km/h
Transportation mode: velocity limit 10 km/h
Battery status below x % should deactivate throttle
Operator presence detection
Dead mans handle and/or IMU to detect if the device is upside up.
RX/TX
Xbee Pro with antenna
Wireless data:
Accelleration [%]
Steering angle [%]
Transportation/work mode [bool]
Battery status [%]
Wireless data:
Vehicle fault messages [fault codes]
Remote control active [bool]
Receiver
Xbee Pro with antenna
Arduino Due
MCP2551 CAN transeiver
CAN bus connector
CAN transeiver
Our Autobox implementation
Functional safety requirements
Is controller activated?
Yes
No
Calcualte error detection
Error detection?
Correct sender
Normal operation
Toss / request new
Remote system ON / OFF mechanism
Request system state ON
System activated (OFF)
Speed zero and parking brake engaged?
Request system state OFF
System activated (ON)
Normal operation
Normal operation
System activated (ON)
Safety watchdog
System ON?
Communication lost Unintended deactivation
Failsafe mode
Connection active watchdog
CAN
Progressive steering curve mapping. Adjustments close to equilibrium will be fine and course on the outer limits.
Steering right
Deadzone to avoid unintentional steering
Linear response in order to easier make adjustments of steering angle close to zero angle
Nonlinear progressive response in order to reach maximum steering during less travel distance
(Steering left is a mirror of the curve to the right)
Steering control signal
Joystick travel
0%
100%
Transport mode switch
Direction switch
Velocity joystick signal
Progressive velocity curve mapping. Adjustments close to equilibrium will be fine and course on the outer limits.
Releasing the joystick will apply braking
Linear response in order to easier make adjustments of throttle close to zero velocity
Nonlinear progressive response in order to reach maximum steering during less travel distance
Deacelleration saturation (will limit brake power)
Velocity setpoint
Joystick travel
-100%
0%
100%
Choose velocity curve based on direction and transport mode switch
In total 4 different curves for transport mode and direction switch.
– Work mode, direction forwards
– Work mode, direction backwards
– Transportation mode, direction forwards
– Transportation mdoe, direction backwards
Parking brake
CAN
Vehicle data
Steering angle setpoint [Deg]
Velocity setpoint [m/s]
Parking brake setpoint [Bool]
Vehicle data
Unknown Simulink model implemented by Hoel
Unknown yaw rate controller
High level unknown controller
Accepts velocity as input signal and will control ICE, transmission, brake and engine brake
Unknown parking brake controller
Vehicle status:
Velocity [m/s]
Information about warning indicators
Parking brake status [bool]
Steering angle [Deg]
Camera or proximity sensor
Unknown signals
ICE setpoints
Engine status data
Transmission setpoints
Transmission status data
Brake command [%]
Truck
Steering system
VDS
Steering ECU
Autobox CAN
NC
SPI
MP (Model)
Interal CAN
DSP
Torque signal [Nm]
VDS motor
Torque
Steering column
Angle, torque
Angle and torsion torque sensors
Angle [Deg] Torque [Nm]
Chassis CAN
Torque from motor [Nm]
Torque feedback from road [Nm]
Mechanical connection
Torque [Nm]
Front wheels
Control direction
Powertrain
Engine ECU
ICE control signals
ICE
Torque [Nm]
Transmission
Torque
Clutch
Mechanical connection
Transmission ECU (Control gear and clutch)
Gear [0]
Clutch slip [%]
Torque [Nm]
Driven wheels
Control velocity
Brake system
Brake ECU
Flow signal [m3/s]
Pneumatic valve
Flow [m3/s]
Pneumatic connection
Force [N]
Brake calipers
Mechanical connection
Torque [Nm]
Nondriven wheels
Parking brake system
Vehicle ECU
Parking brake actuator
Torque [Nm]

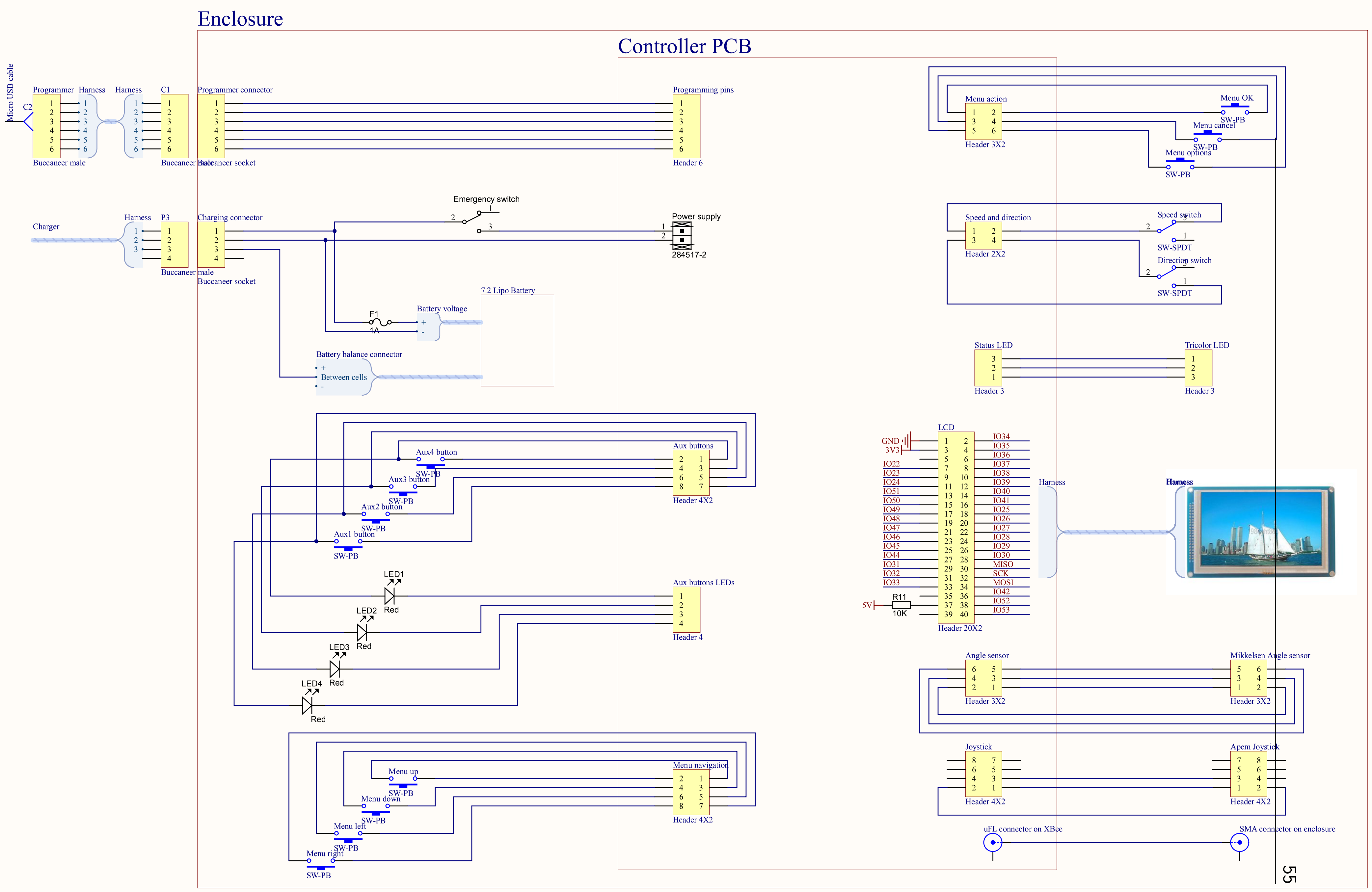
Safety targets:
Dead mans handle. Emergency stop if dead mans handle is released.
Detect if device is upside up. Emergency stop if not.
Ping every x s to make sure connection is active. (Receiver handles potential emergency stop)
Activating remote control not possible if battery level is below x %. If remote control is active and battery level drops below x %, then accelleration is prohibited (at the receiver). Low battery level displays a warning message on the control's display.

Quality targets:
Progressive steering and velocity control. Adjustments close to equilibrium will be fine and course on the outer limits.
Released velocity jotstick will make the truck calmy brake down to standstill

Appendix B

PCB schematics

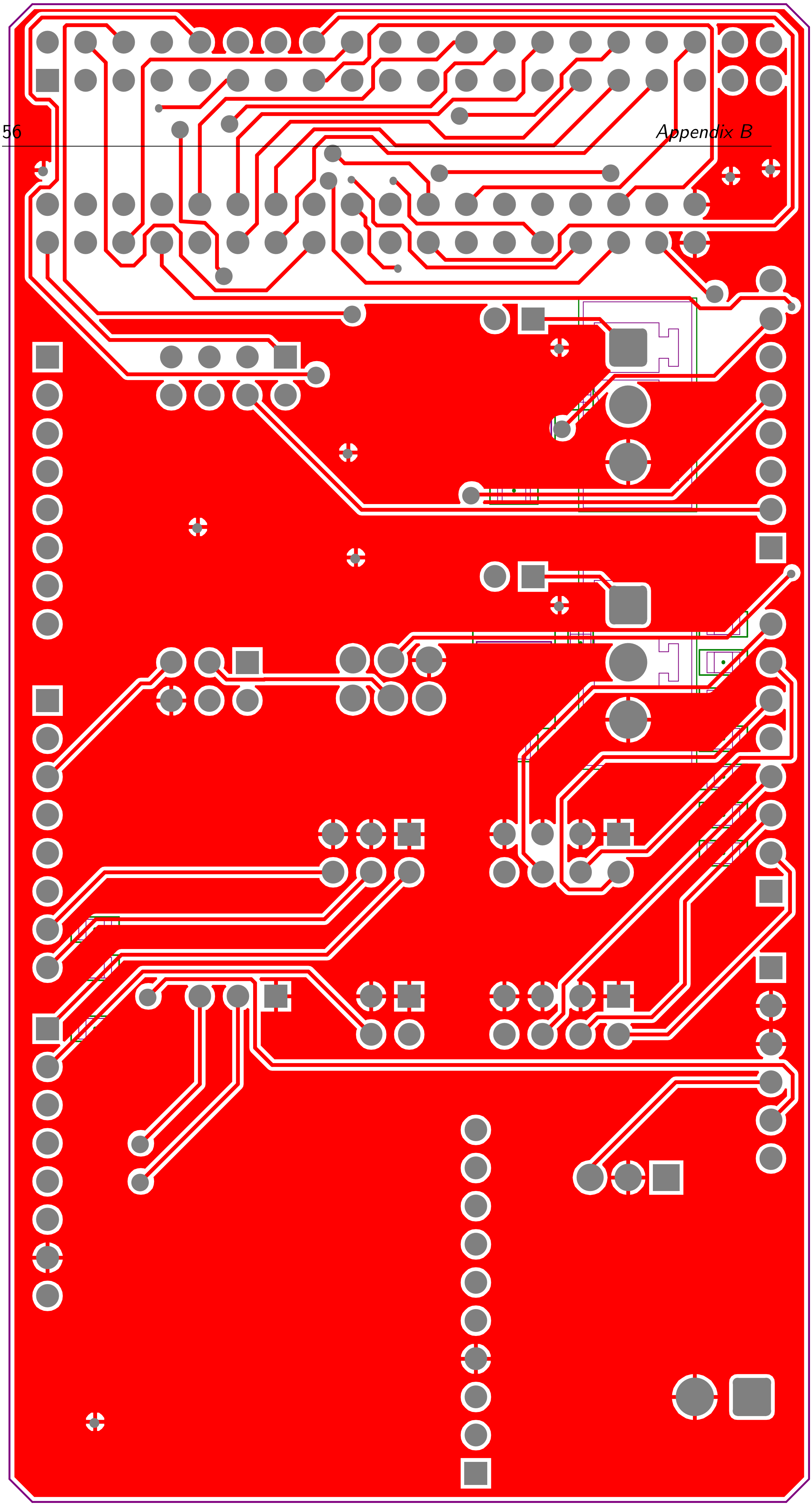

CAN1
CAN2
120 ohm terminator 1
120 ohm terminator 2
Header 2
R20 10K
R21 10K
U1
U2
MCP2551-I/SN
CANH
CANL
TXD
RS
RXD
VREF
VDD
VSS
C1 100n
C3 100n
5V
GND
3V3
Menu action
Header 3X2
Speed and direction
Header 2X2
Status LED
The Tri-colour LED has red and green LEDs when both are connected yellow is produced
Tri-colour pins are centre (−) cathode, shortest (+) anode pin green, longest (+) anode pin red
Header 3
R22 180
R23 180
R15 10K
R16 10K
R17 10K
R18 10K
R19 10K
Xbee adapt
Header 10
RX into Xbee
TX from Xbee
3V3 output
5V input
U_0805 5V to 3V3 voltage divider
0805 5V to 3V3 voltage divider.SchDoc
PWM_H
PWM_L
COMMS
AREF
PWM13
PWM12
PWM11
PWM10
PWM9
PWM8
PWM7
PWM6
PWM5
PWM4
PWM3
PWM2
TX0
RX0
TX3
RX3
TX2
RX2
TX1
RX1
SDA
SCL
DIGITAL
ICSP
5V_ICSP
MISO
MOSI
SCK
RESET
RESET_ICSP
Power supply voltage measurement
VCC_2
R13 10K
R14 1K
POWER
VIN
AD_L
AD_H
AD0
AD1
AD2
AD3
AD4
AD5
AD6
AD7
AD8
AD9
AD10
AD11
DAC0
DAC1
CANRX
CANTX
LCD
R1 10K
R2 10K
R5 10K
R6 10K
R7 10K
R8 10K
R9 10K
R10 10K
Aux buttons
Header 4X2
Menu navigation
Joystick
Analog/PWM output 1
Angle sensor
SS, white
SCLK, gray
MOSI, yellow
Supply voltage, green
GND, brown
U3
Recom R-785.0-0.5
IN
OUT
C2 10u
D1 621-1N5819HW-F
VCC
Power supply
284517-2

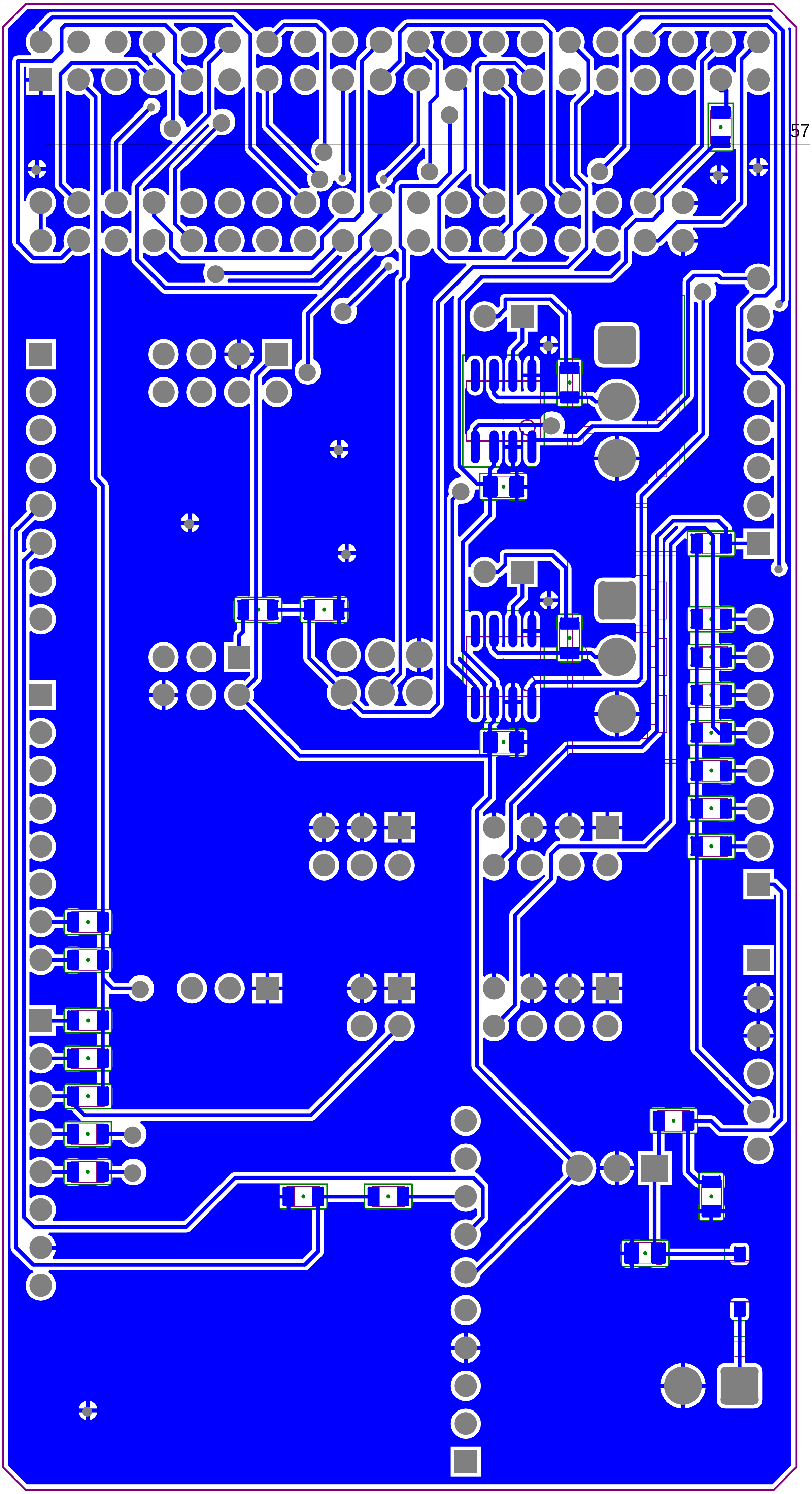


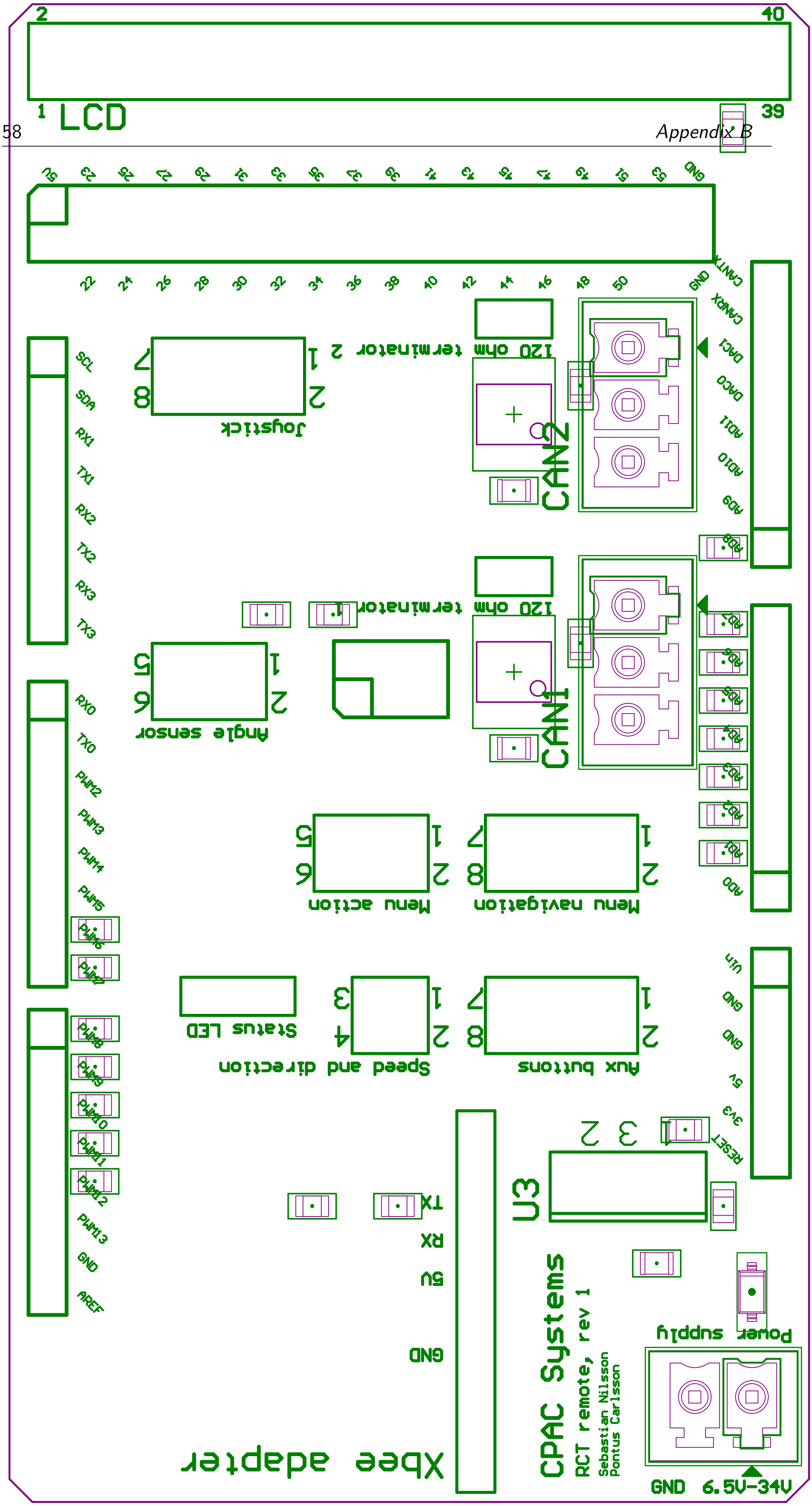
Title
RCT controller overall wiring

Size	Number	Revision
A3		1

Date: 2014-04-15
Sheet of
File: \\..\CPAC Controller.SchDoc
Drawn By: Sebastian Nilsson

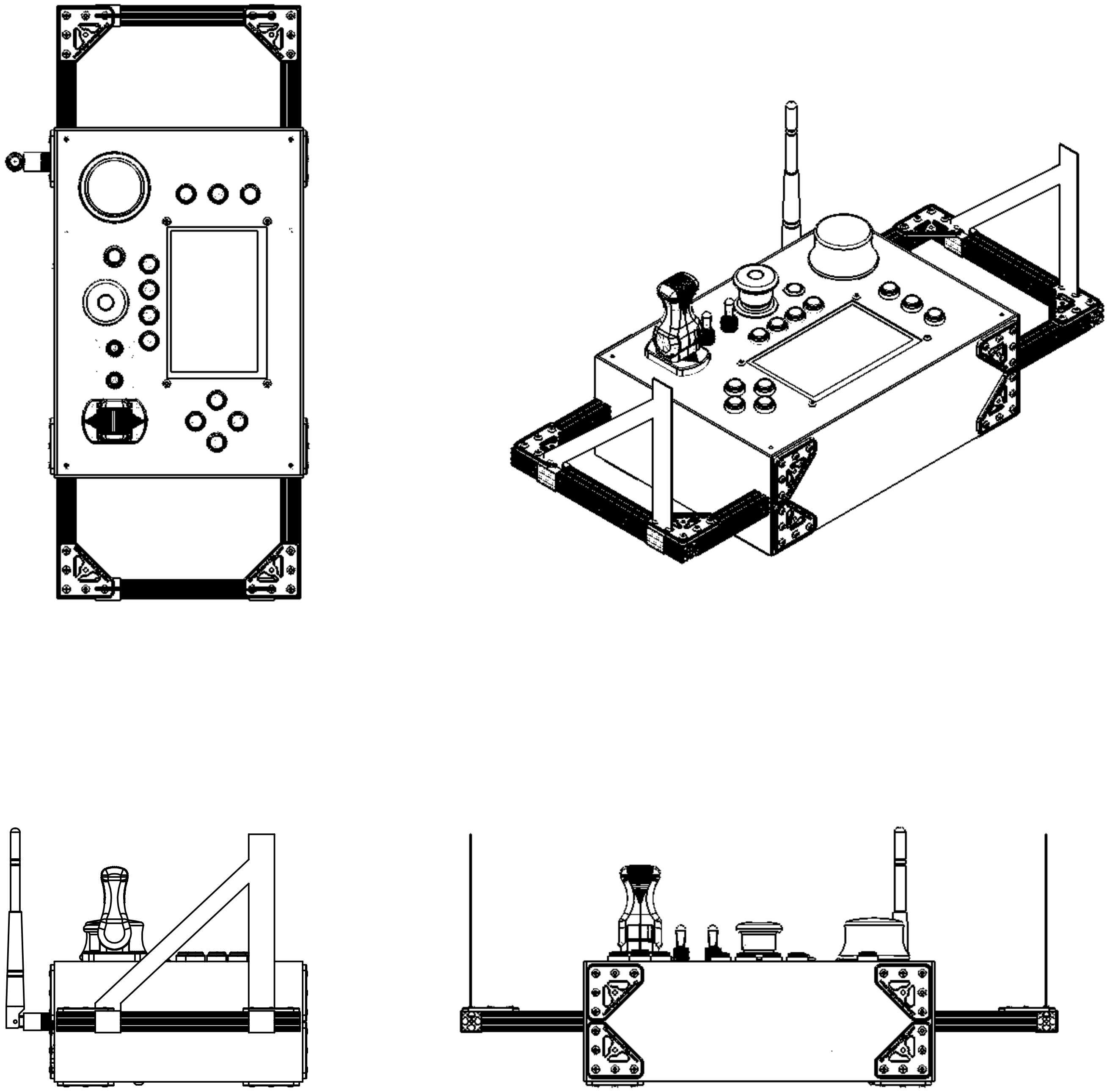



57


2
40
1
LCD
39
5V
23
25
27
29
31
33
35
37
39
41
43
45
47
49
51
53
GND
22
24
26
28
30
32
34
36
38
40
42
44
46
48
50
GND
CANTX
CANRX
DAC1
DAC0
AD11
AD10
AD9
AD8
AD7
AD6
AD5
AD4
AD3
AD2
AD1
AD0
SCL
SDA
RX1
TX1
RX2
TX2
RX3
TX3
RX0
TX0
PWM2
PWM3
PWM4
PWM5
PWM6
PWM7
PWM8
PWM9
PWM10
PWM11
PWM12
PWM13
GND
AREF
120 ohm terminator 2
Joystick
CAN2
120 ohm terminator 1
CAN1
Angle sensor
Menu action
Menu navigation
Status LED
Speed and direction
Aux buttons
U3
TX
RX
5V
GND
Xbee adapter
Vin
GND
GND
5V
3V3
RESET
CPAC Systems
RCT remote, rev 1
Sebastian Nilsson
Pontus Carlsson
Power supply
GND
6.5V-34V

Appendix C

CAD drawings



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN	Sebastian Nilsson		
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:

WEIGHT:

TITLE:

Assembly

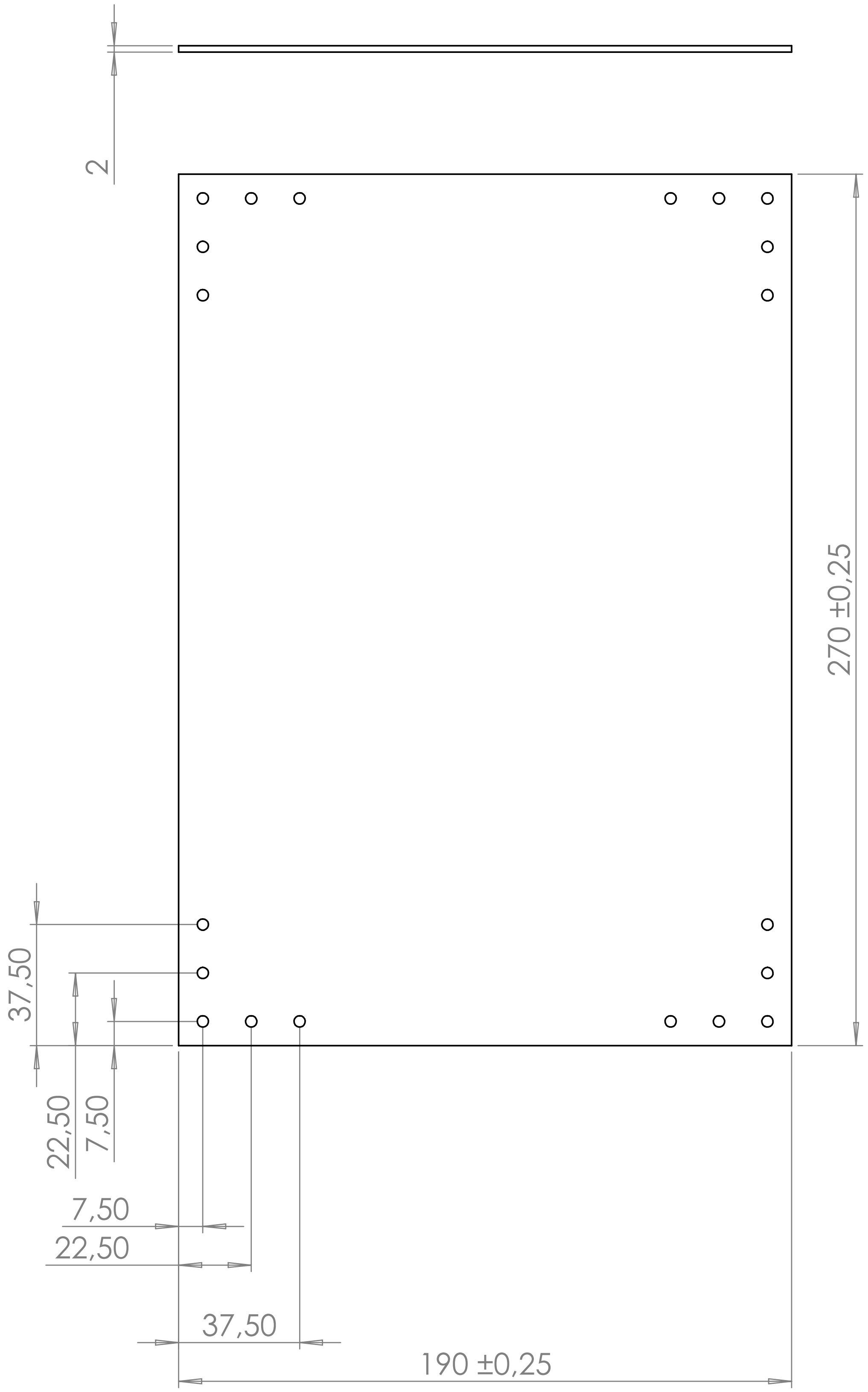
DWG NO.

Controller rev3

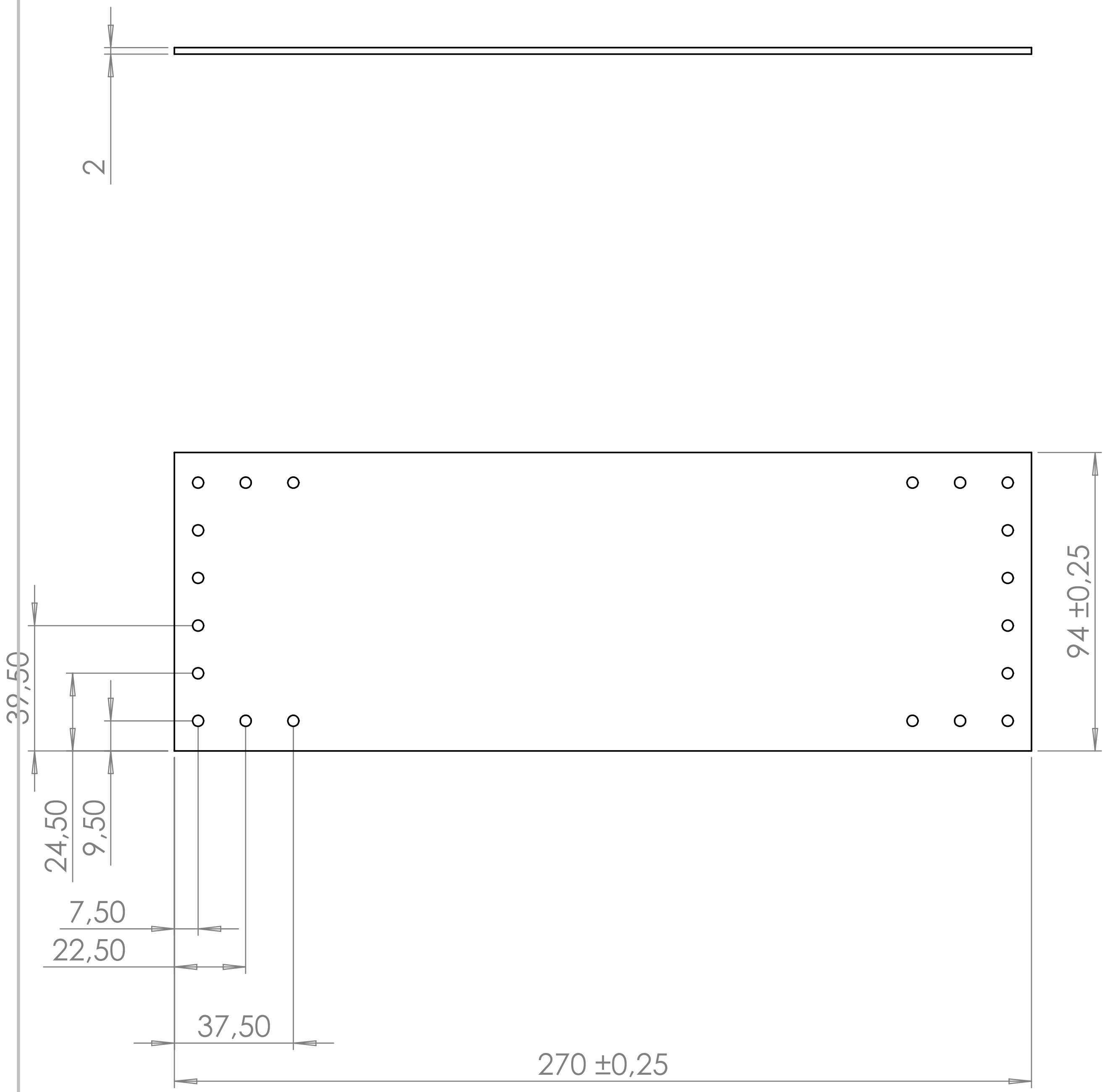
A4

SCALE:1:5

SHEET 1 OF 19



UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:	FINISH:				DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING
	NAME	SIGNATURE	DATE			REVISION
DRAWN						TITLE:
CHK'D						Bottom plate
APPV'D						
MFG						
Q.A				MATERIAL:		DWG NO. Controller rev3
						A4
				WEIGHT:		SCALE:1:2 SHEET 2 OF 19



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:

WEIGHT:

TITLE:

Long side plate back

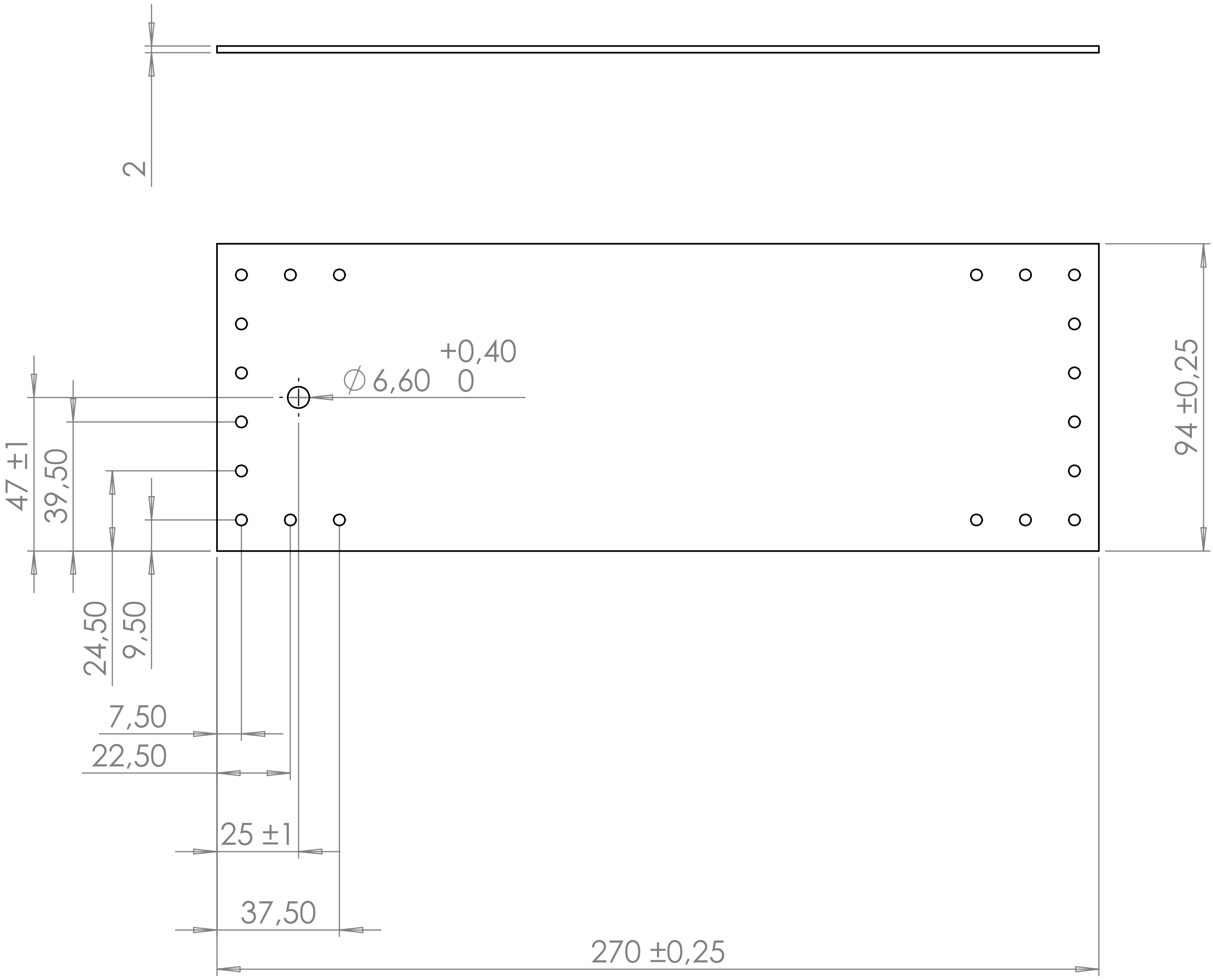
DWG NO.

Controller rev3

A4

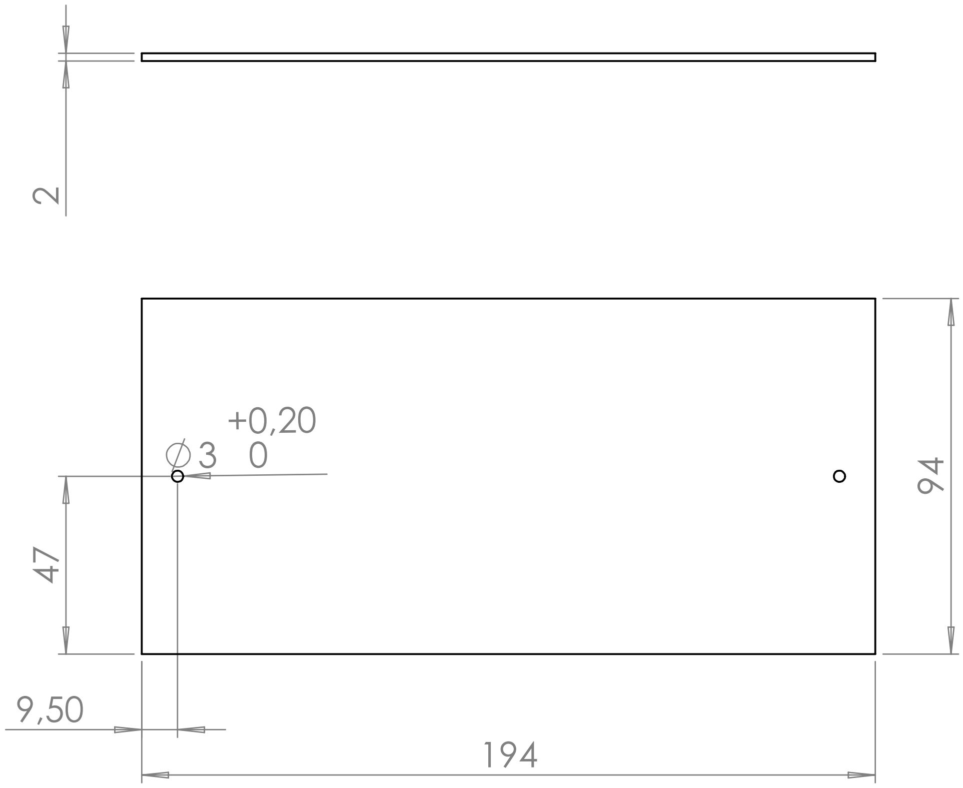
SCALE:1:2

SHEET 3 OF 19



UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:		FINISH:			DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING	REVISION
	NAME	SIGNATURE	DATE			TITLE:	
DRAWN						Long side plate front	
CHK'D							
APPV'D							
MFG							
Q.A				MATERIAL:		DWG NO. Controller rev3	A4
				WEIGHT:		SCALE:1:2	SHEET 4 OF 19

2x



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE		
DRAWN					
CHK'D					
APPV'D					
MFG					
Q.A					

TITLE:

Short side plate

MATERIAL:

DWG NO.

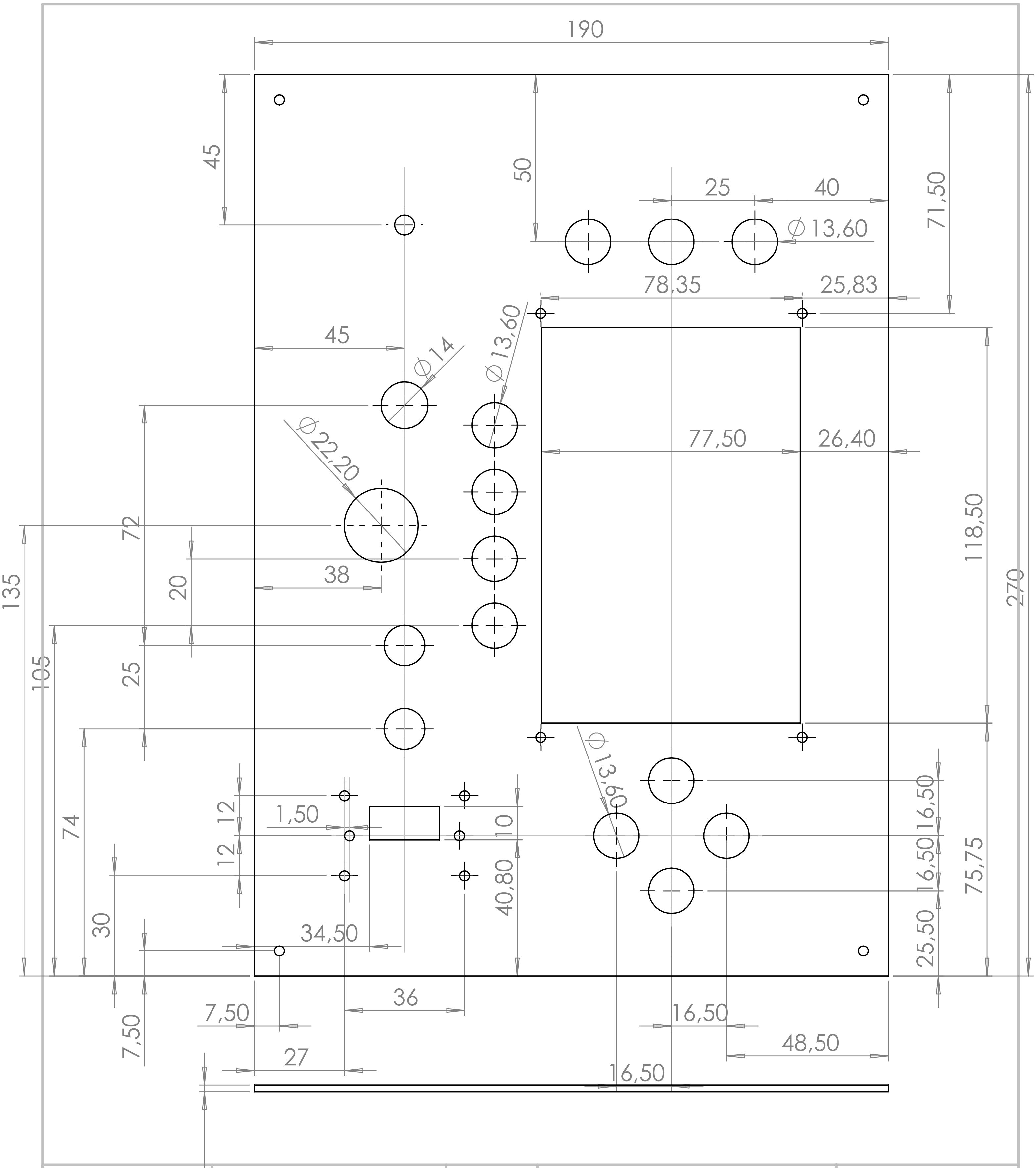
Controller rev3

A4

WEIGHT:

SCALE:1:2

SHEET 5 OF 19



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

(Multiple drawings)

	NAME	SIGNATURE	DATE		
DRAWN					
CHK'D					
APPV'D					
MFG					
Q.A					

TITLE:

Top plate

MATERIAL:

DWG NO.

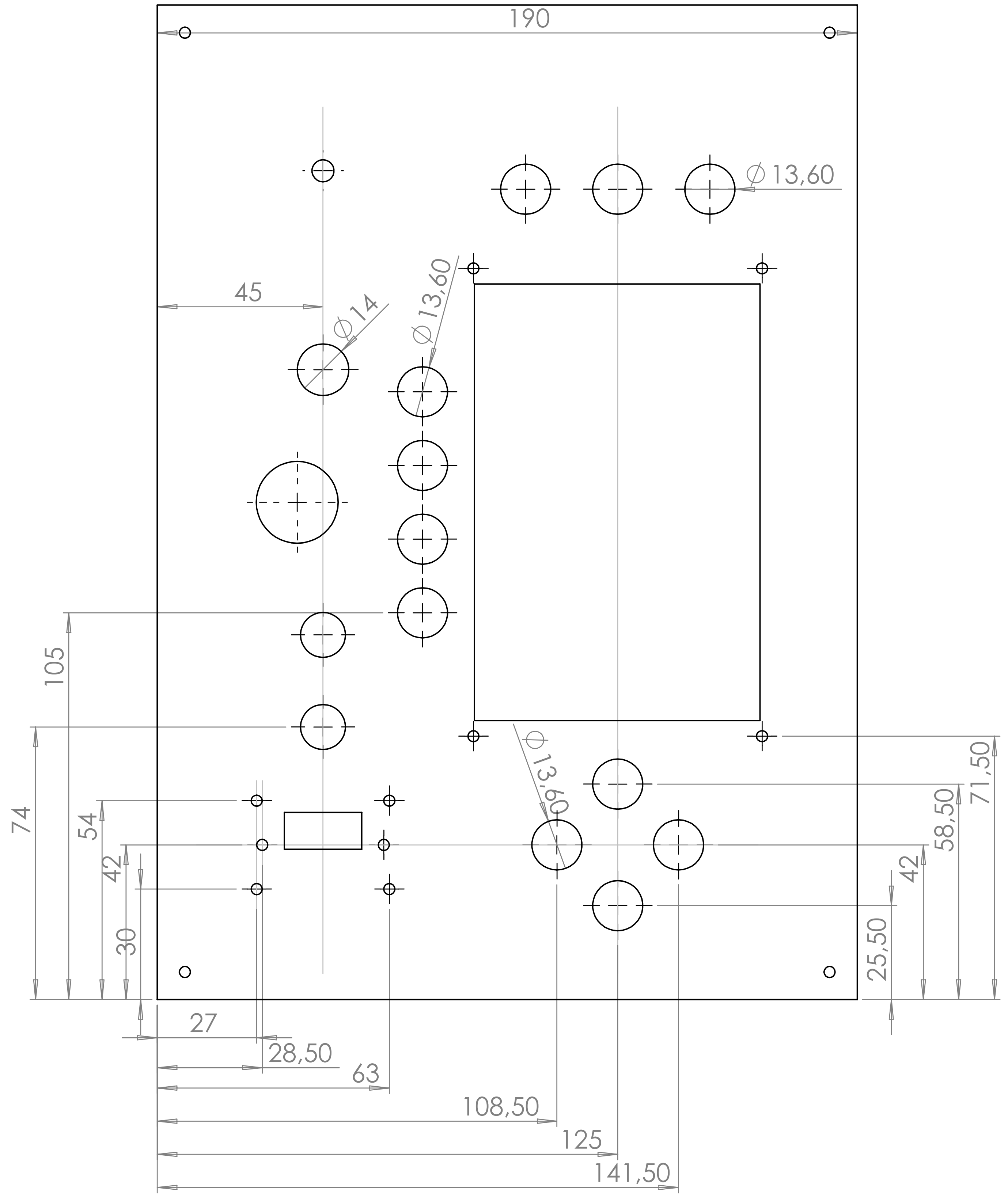
Controller rev3

A4

WEIGHT:

SCALE:2:3

SHEET 6 OF 19



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

(Multiple drawings)

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

TITLE:

Top plate

MATERIAL:

Alu

DWG NO.

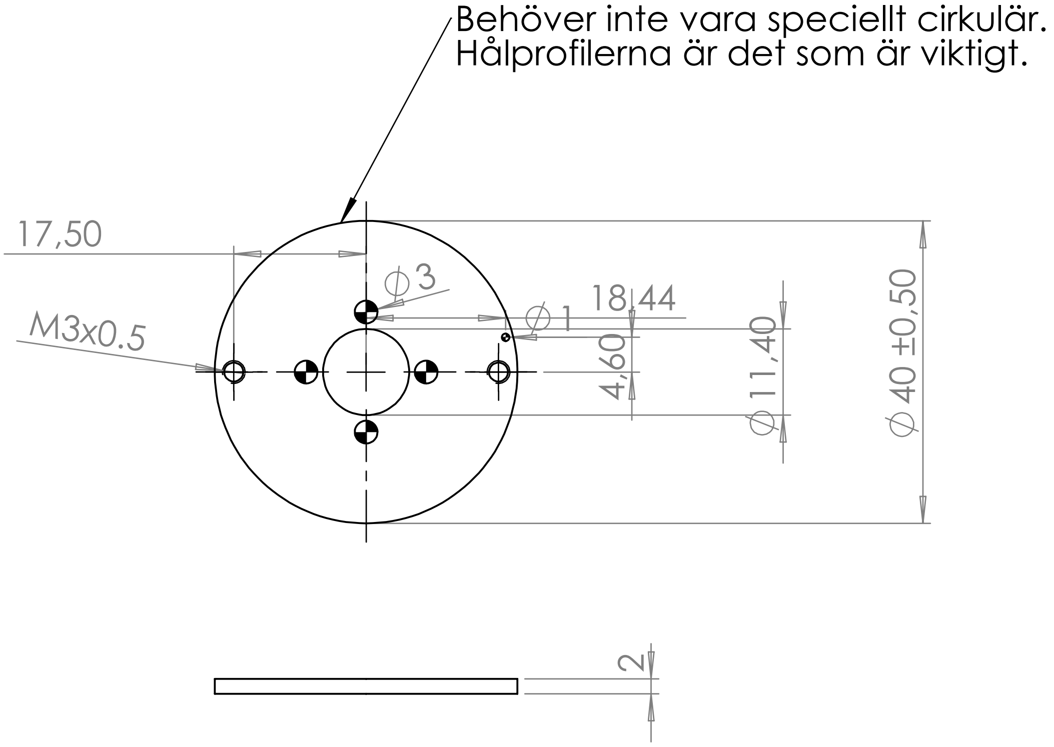
Controller rev3

A4

WEIGHT:

SCALE:2:3

SHEET 7 OF 19


Behöver inte vara speciellt cirkulär.
Hålprofilerna är det som är viktigt.
17,50
M3x0.5
⌀3
⌀1
18,44
4,60
⌀11,40
⌀40 ±0,50
2

UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

DEBUR AND BREAK SHARP EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:

WEIGHT:

TITLE:

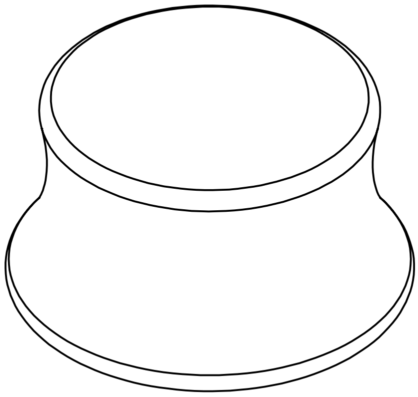
Hub for steering wheel

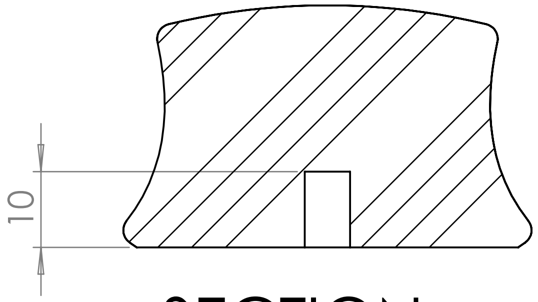
DWG NO. Controller rev3

A4

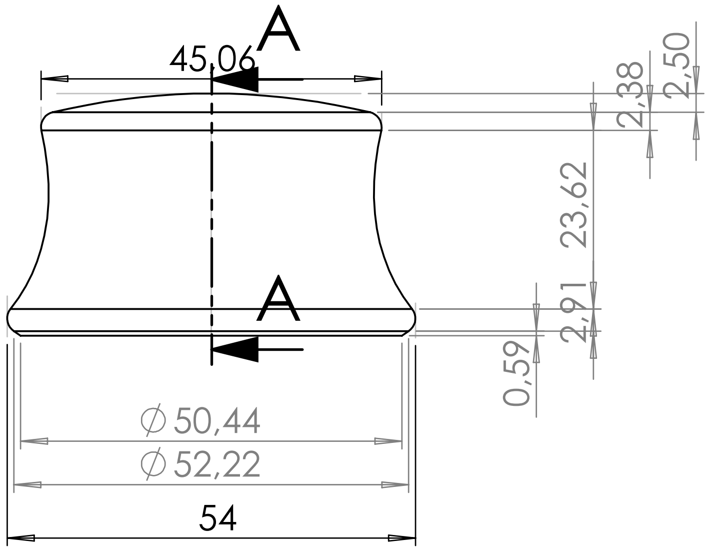
SCALE:1:1

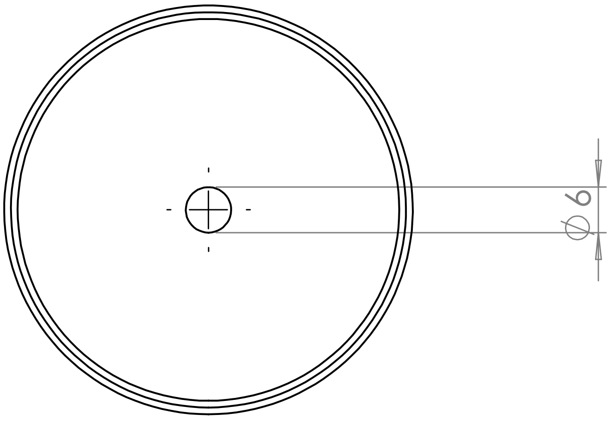
SHEET 8 OF 19



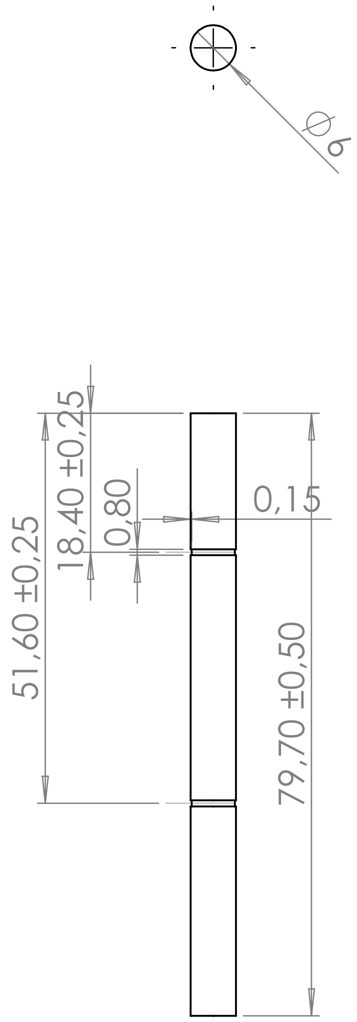


SECTION A-A





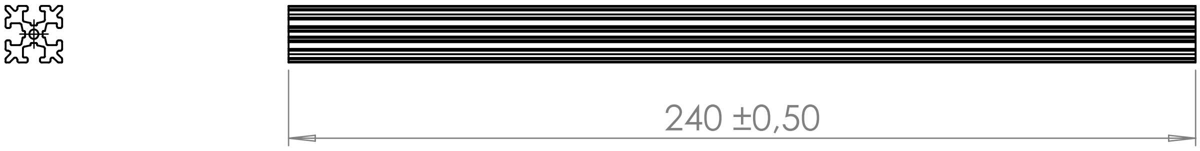
UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:		FINISH:				DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING	REVISION
	NAME	SIGNATURE	DATE				TITLE:	
DRAWN							Knob	
CHK'D								
APPV'D								
MFG								
Q.A				MATERIAL:			DWG NO. Controller rev3	A4
				WEIGHT:			SCALE:1:1	SHEET 9 OF 19



2 spår för spårringar
Wiberger SGA-6

UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:			FINISH:			DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING	REVISION
	NAME	SIGNATURE	DATE				TITLE:	
DRAWN							Knob axle	
CHK'D								
APPV'D								
MFG								
Q.A				MATERIAL:			DWG NO. Controller rev3	A4
				WEIGHT:			SCALE:1:1	SHEET 10 OF 19

4x



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

SEE NOTES

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:

SEE NOTES

WEIGHT:

TITLE:

Long side beam

DWG NO.

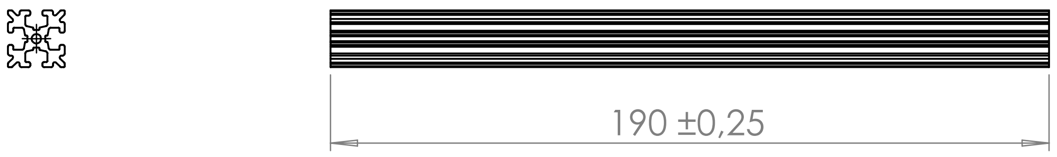
Controller rev3

A4

SCALE:1:2

SHEET 11 OF 19

4x



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:
SEE NOTES

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:
SEE NOTES

WEIGHT:

TITLE:
Short side beam

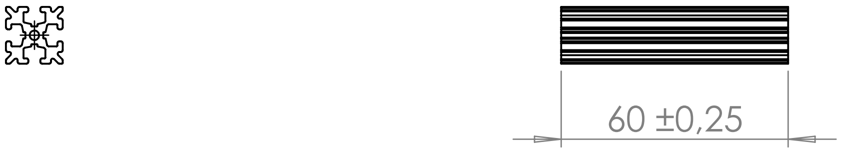
DWG NO.
Controller rev3

A4

SCALE:1:2

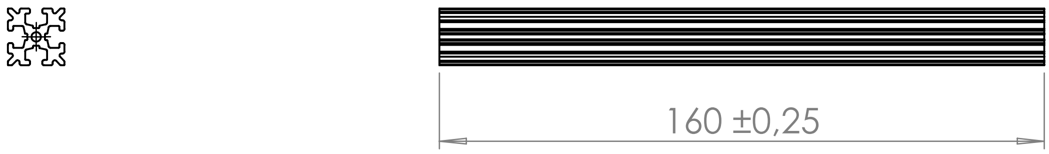
SHEET 12 OF 19

4x



UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:	FINISH: SEE NOTES	DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING	REVISION		
	NAME	SIGNATURE	DATE			TITLE: Vertical beam
DRAWN						
CHK'D						
APPV'D						
MFG						
Q.A				MATERIAL: SEE NOTES	DWG NO. Controller rev3	A4
				WEIGHT:	SCALE:1:2	SHEET 13 OF 19

2x



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:
SEE NOTES

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE		
DRAWN					
CHK'D					
APPV'D					
MFG					
Q.A					

MATERIAL:
SEE NOTES

WEIGHT:

TITLE:

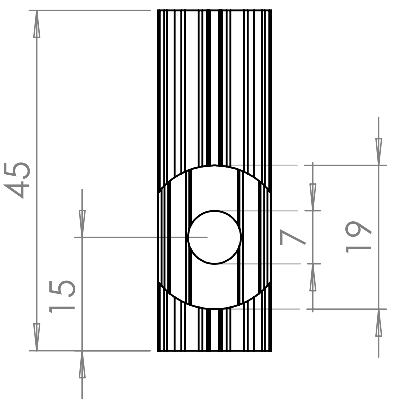
Inner short beam

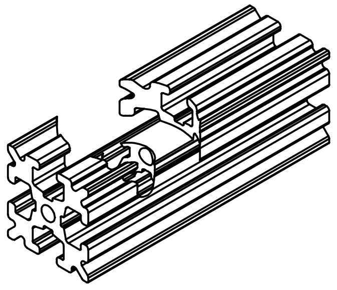
DWG NO.
Controller rev3

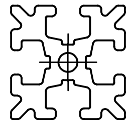
A4

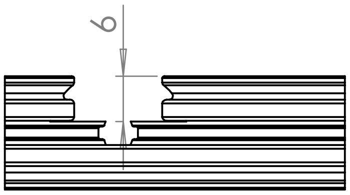
SCALE:1:2

SHEET 14 OF 19



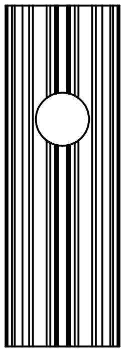






Infästning för kullager.
Kullagrets höjd är 6 mm.

Borra ett hål med diameter7 mm rakt igenom.
Borra/fräs 6 mm djupt med diameter 19 mm.



UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:	FINISH: SEE NOTES	DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING	REVISION

	NAME	SIGNATURE	DATE			
DRAWN						
CHK'D						
APPV'D						
MFG						
Q.A				MATERIAL: SEE NOTES		
				WEIGHT:		

TITLE:

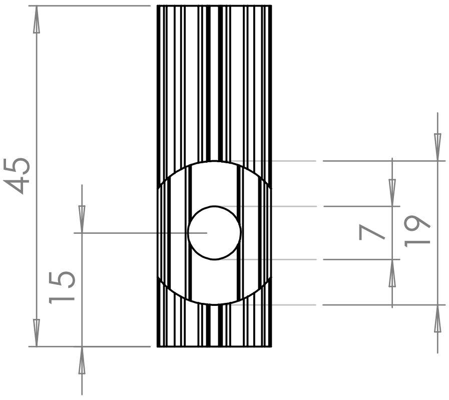
Steering lower support beam

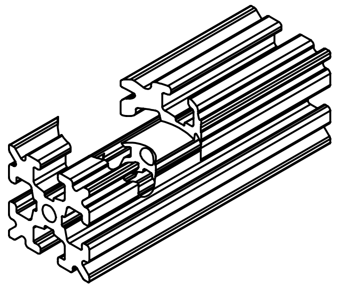
DWG NO. Controller rev3

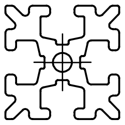
A4

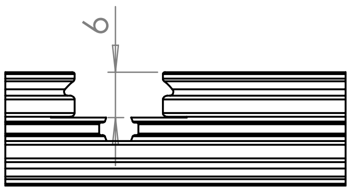
SCALE:1:1

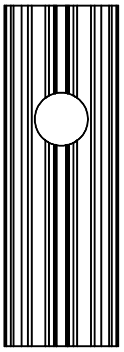
SHEET 15 OF 19











Infästning för kullager.
Kullagrets höjd är 6 mm.

Borra ett hål med diameter 7 mm rakt igenom.
Borra/fräs 6 mm djupt med diameter 19 mm.

UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:	FINISH: SEE NOTES	DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING	REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:
SEE NOTES

WEIGHT:

TITLE:
Steering upper support beam

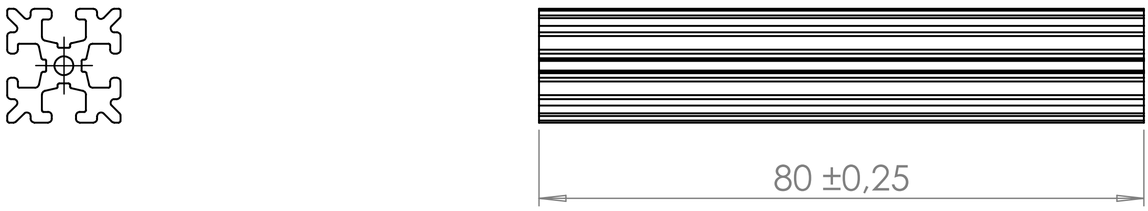
DWG NO.
Controller rev3

A4

SCALE:1:1

SHEET 16 OF 19

4x



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:
SEE NOTES

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:
SEE NOTES

WEIGHT:

TITLE:
Belt holder short side

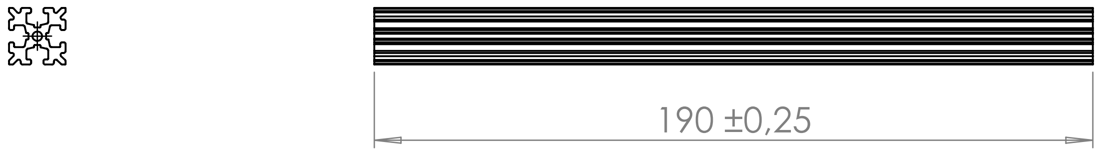
DWG NO.
Controller rev3

A4

SCALE:1:1

SHEET 17 OF 19

2x



UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
SURFACE FINISH:
TOLERANCES:
LINEAR:
ANGULAR:

FINISH:

SEE NOTES

DEBUR AND
BREAK SHARP
EDGES

DO NOT SCALE DRAWING

REVISION

	NAME	SIGNATURE	DATE
DRAWN			
CHK'D			
APPV'D			
MFG			
Q.A			

MATERIAL:

SEE NOTES

WEIGHT:

TITLE:

Belt holder long side

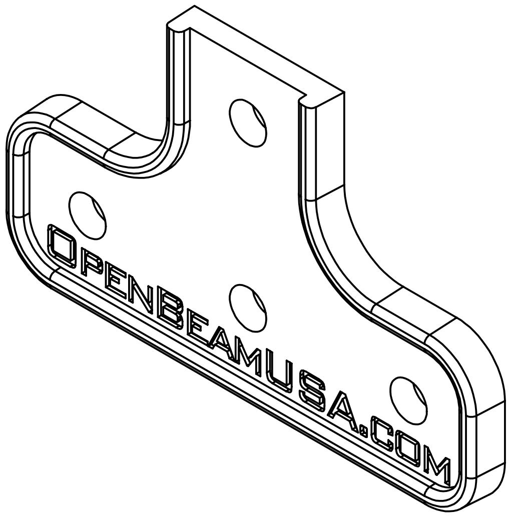
DWG NO.

Controller rev3

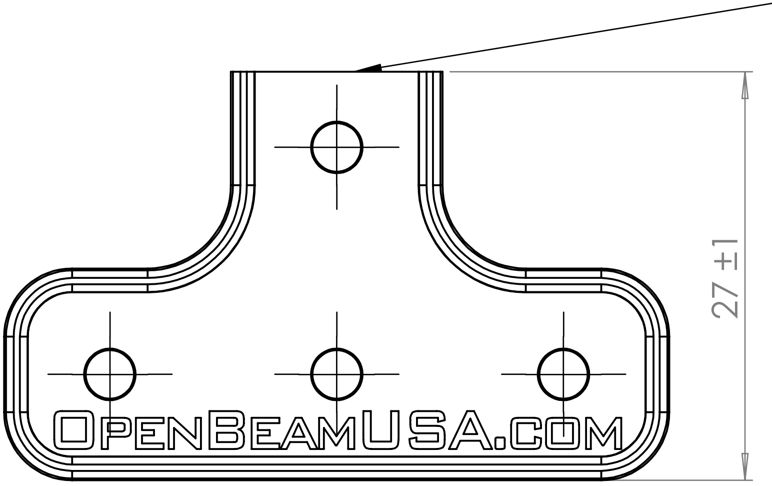
A4

SCALE:1:2

SHEET 18 OF 19



Såga av en redan befintlig komponent i plast



UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN MILLIMETERS SURFACE FINISH: TOLERANCES: LINEAR: ANGULAR:		FINISH: SEE NOTES				DEBUR AND BREAK SHARP EDGES	DO NOT SCALE DRAWING / REVISION
	NAME	SIGNATURE	DATE				TITLE:
DRAWN							T bracket cut
CHK'D							
APPV'D							
MFG							
Q.A				MATERIAL: SEE NOTES			DWG NO. Controller rev3 / A4
				WEIGHT:			SCALE:2:1 / SHEET 19 OF 19

Appendix D

Manufacturing and assembly

D.1 Manufacturing and assembly of PCBs

The manufacturing process for the PCBs was done both in house and outsourced. The design was in house, manufacturing of the PCB outsourced and soldering of all components in house. The main reason for outsourcing the PCB was that we would not be able to reach the same quality in-house for the board and the demands for reliability of the electrical system is set high. A failure in any of the PCBs might cause an unsafe behaviour during testing and demonstration. The design of the PCBs are covered in the design part of this report and this section will therefore only cover the soldering of the PCBs. The procedure for soldering components onto the PCB is as follows: Tools needed are soldering iron, flux, solder and a good holder for the PCB. Also a computer with the ECAD for the PCB is important to make sure the right component is in the right place. Figure x shows an empty PCB as they are delivered from the PCB manufacturing factory. Reliable solder joints are done by making that surfaces are clean and therefore flux solution is applied before mounting the component. Solvents to clean a surface might be helpful but are insufficient due to the rapid rate at which oxides will form on the surface of heated metals. The function of the flux is to remove oxides and keep them removed for the whole soldering operation. The flux will volatilize rapidly at a much lower temperature than melting of the solder. Leftover flux can be cleaned off with solvents when the soldering is done. Mount components one by one. When the PCB assembly is done (see figure **??**) it is tested for the basic functions (digital I/Os, analog inputs, CAN bus and SPI) in a test bench. The setup for the CAN bus test bench can be seen in Figure x.

D.1.1 PCB bugs

Almost no PCB is manufactured without bugs and mistakes on the first try. Listed below are the mistakes:

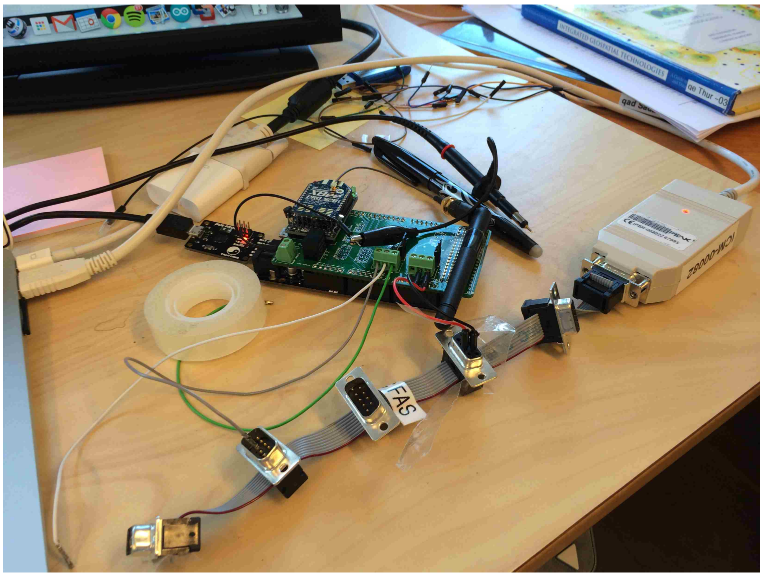


Figure D.1. Test bench for PCB. The white device to the right is a PCAN dongle to transmit and receive CAN messages.

- Voltage divider for the joystick is missing outputting a maximum of 4.5 V which saturates the uC maximum voltage 3.3 V. Fixed by adding air wires and extra resistors.

- Some 20K should be 18K to comply with E12 standard resistor values. Fixed by using 18K instead.

- For the angle sensor, the MISO and MOSI connections should be on the same bus. This could have been done with a jumper. Fixed by replacing the SPI angle sensor with an analog one, and adding ports for analog inputs with air wires and resistors.

- Missing outputs for the 4 button LEDS. Fixed by adding port on the unused CAN bus ports. 180 ohm resistors are also added.

- LCD port connector has columns switched. Fixed by switching positions on the cable connector.

- Jumpers for CAN should have 3 pins instead of 2 to give the jumper a resting position. Fix not necessary.

- CAN bus termination should be 120 ohm. Fixed by using the correct resistor value.

- Silkscreen for the CAN bus ports are missing. Difficult to know which port is which. Fix not necessary.

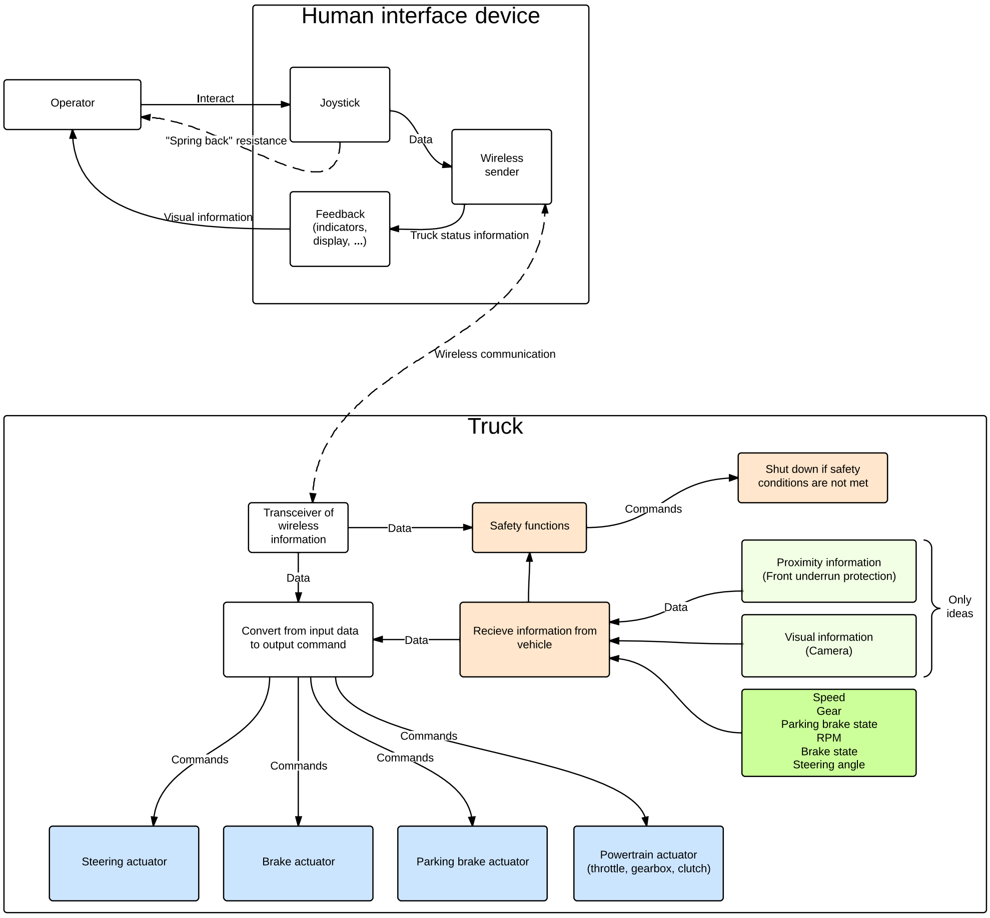


Figure D.2. Functional model

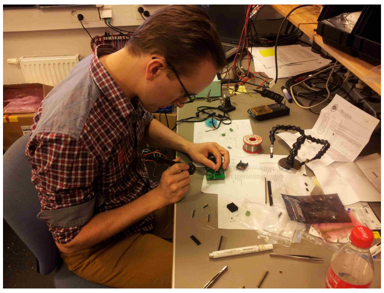


Figure D.3. Action photo of soldering

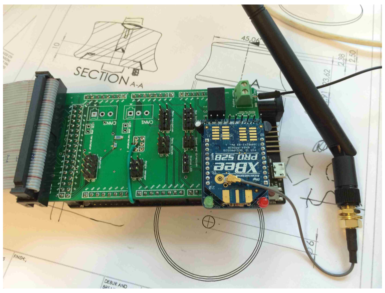


Figure D.4. Action photo of soldering

D.1.2 CNC milling

The CNC milling process:

1. Create CAM files from CAD, so called g-code

2. Upload to the milling computer and fasten the material

3. Mill it

4. Remove sharp edges with Dremel and file tool

Figure D.5. Fastening fixture

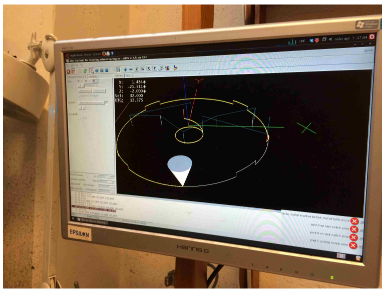


Figure D.6. CAM file for steering knob component

Figure D.7. Milling process

D.2 Cutting

The beams and plates are cut in Chalmers workshop.

D.2.1 3D printing

The steering knob was 3D printed since it either required an advanced milling machine or manufacturing in wood.

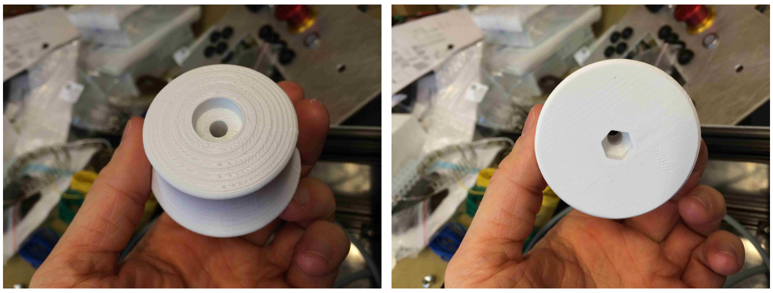


Figure D.8.

D.2.2 Assembly

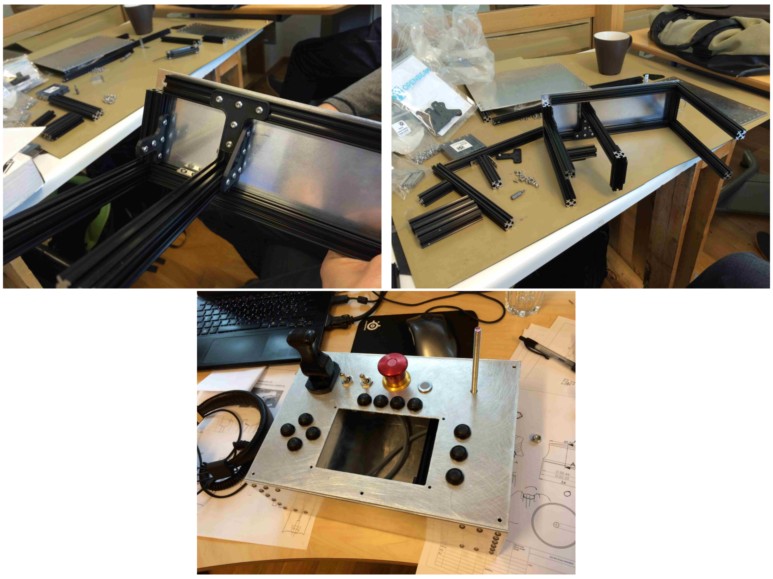


Figure D.9.

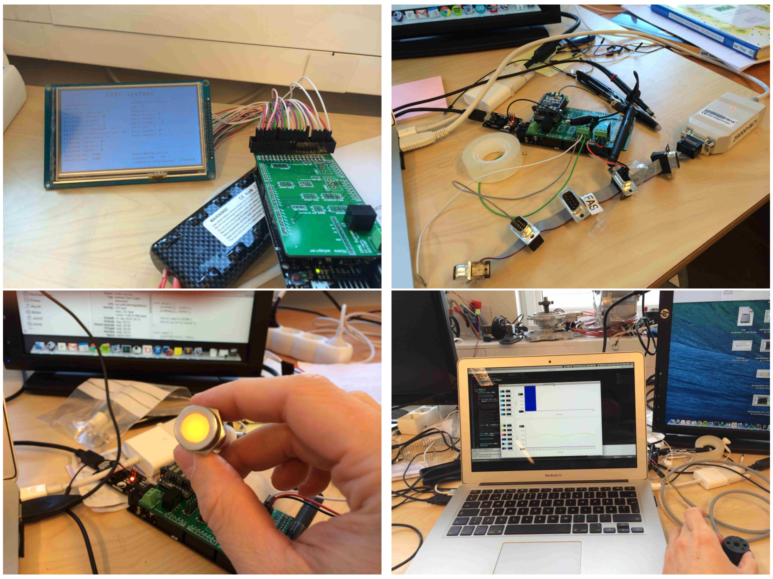


Figure D.10. Every electronic component was tested before being put into the box

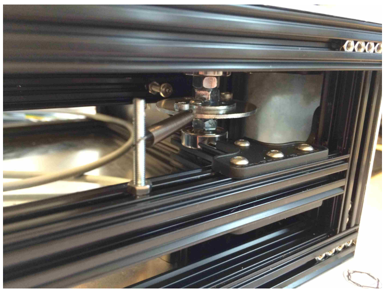


Figure D.11. Steering mechanics

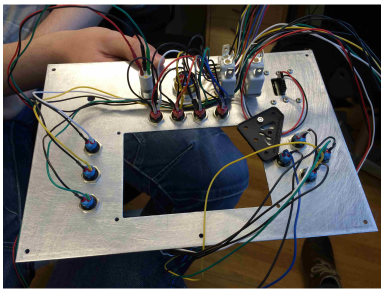


Figure D.12. Wiring

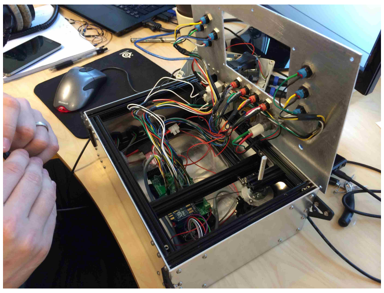


Figure D.13. Connecting connectors and components to the ECU

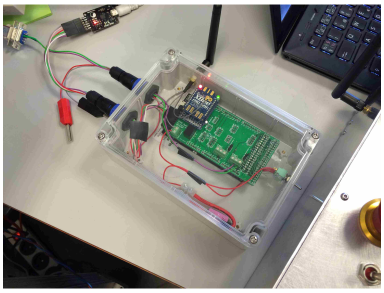


Figure D.14. Receiver box assembled

Appendix E

Work distribution

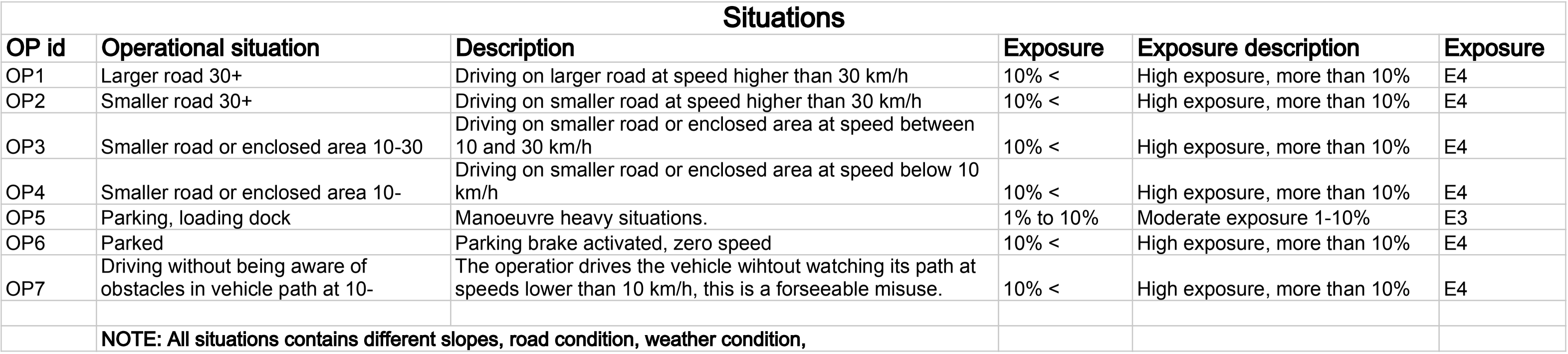
Item	Pontus	Sebastian	Comment
System architecture	x	x	
Safety concept according to ISO-26262	x		
Mechanical CAD design		x	The concept was done by both
Chosing components	x	x	
Human-machine interface	40%	60%	
Communication design		x	
Xbee configuration	x		
Electronics design		x	
Soldering and PCB assembly		x	
Assembly of enclosure	x		
C programming	75%	25%	Some modules programmed by Sebastian. Pontus put it together and did the overall concept.
Schedulability and RTOS	95%	5%	(RTOS selected by Sebastian from previous experience.) Implemented by Pontus.
Testing and verification	x	x	

Table E.1. Work distribution

Appendix F

ISO-26262 safety analysis

F.1 Operating situations



Situations					
OP id	**Operational situation**	**Description**	**Exposure**	**Exposure description**	**Exposure**
OP1	Larger road 30+	Driving on larger road at speed higher than 30 km/h	10% <	High exposure, more than 10%	E4
OP2	Smaller road 30+	Driving on smaller road at speed higher than 30 km/h	10% <	High exposure, more than 10%	E4
OP3	Smaller road or enclosed area 10-30	Driving on smaller road or enclosed area at speed between 10 and 30 km/h	10% <	High exposure, more than 10%	E4
OP4	Smaller road or enclosed area 10-	Driving on smaller road or enclosed area at speed below 10 km/h	10% <	High exposure, more than 10%	E4
OP5	Parking, loading dock	Manoeuvre heavy situations.	1% to 10%	Moderate exposure 1-10%	E3
OP6	Parked	Parking brake activated, zero speed	10% <	High exposure, more than 10%	E4
OP7	Driving without being aware of obstacles in vehicle path at 10-	The operatior drives the vehicle wihtout watching its path at speeds lower than 10 km/h, this is a forseeable misuse.	10% <	High exposure, more than 10%	E4
	NOTE: All situations contains different slopes, road condition, weather condition,				

F.2 Malfunctions

Function	Failure mode mapping to checklist	Failure mode, description	Hazard/Malfunction (MF) Id	Hazard/Malfunction (MF) Described as condition or behaviour at vehicle level
Steering	Commission	The truck receives a steering request that the operator did not issue	MF1	Unintended steering request
Steering	Omission	The operator requests steering but the truck does not receive the request	MF2	Loss of steering request
Steering	Late	The operator requests steering, the truck gets the request delayed X timeunits	MF3	Delayed steering request
Braking	Commission	The truck receives a braking request that the operator did not issue	MF4	Unintended braking request
Braking	Omission	The operator requests braking but the truck does not receive the request	MF5	Loss of brakes request
Braking	Late	The operator requests braking , the truck gets the request delayed X timeunits	MF6	Braking delayed request
Acceleration	Commission	The truck receives a acceleration request that the operator did not issue	MF7	Unintended acceleration request
Acceleration	Omission	The operator requests acceleration but the truck does not receive the request	MF8	Loss of acceleration request
Acceleration	Late	The operator requests acceleration, the truck gets the request delayed X timeunits	MF9	Delayed acceleration request
Remote system	Commission	Unintended activation of remote system, since steering then tries to center and braking is applied it will be a combination between unintended steering and unintended braking. Also the driver is in the drivingseat since the system was prior to failure deactivated. We then have double requests to controllers which makes this failure hard to control.	MF10	Unintended activation of remote system
Remote system	Omission	Unintended deactivation of remote system, all requests are lost	MF11	Unintended deactivation of remote system

F.3 Complete PHA table

RCT										ISO 26262								
			Hazard identification															
Hazard / Malfunction		Situation Analysis			Hazardous Events		Classification of hazardous events						Determination of Safety Integrity level and Safety goals					
Function / Actuator	Malfunction	Operational Situation	Items operational mode		Hazardous event ID	Consequence of Hazards Event	Severity rational (S)	Exposure rate rational (E)	Controllability factor(C)	S	E	C	Safety Integrity level	Safety Goal ID	Safety Goal	Safe State	Physical characteristics relevant for the Safety integrity level determination	comments
Steering	MF1: Unintended steering request	OP1: Larger road 30+	Activated	1	RCT_HE_1	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	At high speed driver is unlikely to react in time to counteract the steering	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A	VDS electric motor is capable of providing a maximum torque of ~25 Nm.	
	MF1: Unintended steering request	OP2: Smaller road 30+	Activated	2	RCT_HE_2	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	At high speed driver is unlikley to react in time to counteract the steering	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF1: Unintended steering request	OP3: Smaller road or enclosed area 10-30	Activated	3	RCT_HE_3	Frontal collision or running off-road at moderate speed, colide with VRU	Severe Injury with possible death	High exposure, more than 10%	Somewhat controllable by braking and coutersteering	S3	E4	C2	ASIL C	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF1: Unintended steering request	OP4: Smaller road or enclosed area 10-	Activated	4	RCT_HE_4	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Controllable by countersteering and braking, ~3m to stop including 1s reaction	S2	E4	C1	ASIL A	SG7	No unintended steering requests	Apply full brake		
	MF1: Unintended steering request	OP5: Parking, loading dock	Activated	5	RCT_HE_5	Collide with VRU at low speed	Severe injury survival likley	Moderate exposure 1-10%	Controllable by countersteering and braking, ~3m to stop including 1s reaction	S2	E3	C1	QM		--	Apply full brake		
	MF1: Unintended steering request	OP6: Parked	Activated	6	RCT_HE_6	No hazard possible, vehicle not moving	Vehicle is not moving	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		
	MF1: Unintended steering request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	7	RCT_HE_7	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S2	E4	C3	ASIL C	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		
Steering	MF2: Loss of steering request	OP1: Larger road 30+	Activated	8	RCT_HE_8	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	Low controlability since remote does not have physical connection	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF2: Loss of steering request	OP2: Smaller road 30+	Activated	9	RCT_HE_9	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	Low controllabillity since remote does not have physical connection	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF2: Loss of steering request	OP3: Smaller road or enclosed area 10-30	Activated	10	RCT_HE_10	Frontal collision or running off-road at moderate speed, colide with VRU	Severe Injury with possible death	High exposure, more than 10%	Somewhat controlable by braking cause of the lower speed	S3	E4	C2	ASIL C	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF2: Loss of steering request	OP4: Smaller road or enclosed area 10-	Activated	11	RCT_HE_11	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Controllable by braking, ~3m to stop including 1s reaction	S2	E4	C1	ASIL A	SG9	No loss of steering request	Apply full brake		
	MF2: Loss of steering request	OP5: Parking, loading dock	Activated	12	RCT_HE_12	Collide with VRU at low speed	Severe injury survival likley	Moderate exposure 1-10%	Controllable by braking, ~3m to stop including 1s reaction	S2	E3	C1	QM		--	Apply full brake		
	MF2: Loss of steering request	OP6: Parked	Activated	13	RCT_HE_13	No hazard possible, vehicle not moving	Vehicle is not moving	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		

	MF2: Loss of steering request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	14	RCT_HE_14	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S2	E4	C3	ASIL C	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		
Steering	MF3: Delayed steering request	OP1: Larger road 30+	Activated	15	RCT_HE_15	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	Steering delayed but too delayed for driver to be able to control the vehicle	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF3: Delayed steering request	OP2: Smaller road 30+	Activated	16	RCT_HE_16	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	Steering delayed but too delayed for driver to be able to control the vehicle	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF3: Delayed steering request	OP3: Smaller road or enclosed area 10-30	Activated	17	RCT_HE_17	Frontal collision or running off-road at moderate speed, colide with VRU	Severe Injury with possible death	High exposure, more than 10%	Somewhat controllable by braking cause of the lower speed	S3	E4	C2	ASIL C	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF3: Delayed steering request	OP4: Smaller road or enclosed area 10-	Activated	18	RCT_HE_18	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Controllable by braking, ~3m to stop including 1s reaction	S2	E4	C1	ASIL A	SG8	No requests delayed more than X	Apply full brake		
	MF3: Delayed steering request	OP5: Parking, loading dock	Activated	19	RCT_HE_19	Collide with VRU at low speed	Severe injury survival likley	Moderate exposure 1-10%	Controllable by braking, ~3m to stop including 1s reaction	S2	E3	C1	QM		--	Apply full brake		
	MF3: Delayed steering request	OP6: Parked	Activated	20	RCT_HE_20	No hazard possible, vehicle not moving	Vehicle is not moving	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		
	MF3: Delayed steering request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	21	RCT_HE_21	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S2	E4	C3	ASIL C	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		
Braking	MF4: Unintended braking request	OP1: Larger road 30+	Activated	22	RCT_HE_22	Vehicle hit in the back by vehicle from behind	Survival probable, severe injuries might occur	High exposure, more than 10%	Steering still working, driver could try avoid collision but still hard to control	S2	E4	C3	ASIL C	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF4: Unintended braking request	OP2: Smaller road 30+	Activated	23	RCT_HE_23	Vehicle hit in the back by vehicle from behind	Survival probable, severe injuries might occur	High exposure, more than 10%	Steering still working, driver could try to stop the vehicle	S2	E4	C2	ASIL B	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF4: Unintended braking request	OP3: Smaller road or enclosed area 10-30	Activated	24	RCT_HE_24	Vehicle hit in the back by vehicle from behind	Moderate injuries	High exposure, more than 10%	Lower speed, vehicle from behind is probably going to avoid accident	S1	E4	C1	QM	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF4: Unintended braking request	OP4: Smaller road or enclosed area 10-	Activated	25	RCT_HE_25	Operator standing on truck and fall over	Light injuries	High exposure, more than 10%	Low speed, controllable in general	S1	E4	C1	QM		--	Apply full brake		
	MF4: Unintended braking request	OP5: Parking, loading dock	Activated	26	RCT_HE_26	Operator standing on truck and fall over	Light injuries	Moderate exposure 1-10%	Low speed, controllable in general	S1	E3	C1	QM		--	Apply full brake		
	MF4: Unintended braking request	OP6: Parked	Activated	27	RCT_HE_27	No hazard possible, vehicle not moving	Vehicle is not moving	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		
	MF4: Unintended braking request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	28	RCT_HE_28	Operator standing on truck and fall over	Light injuries	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S1	E4	C3	ASIL B	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		

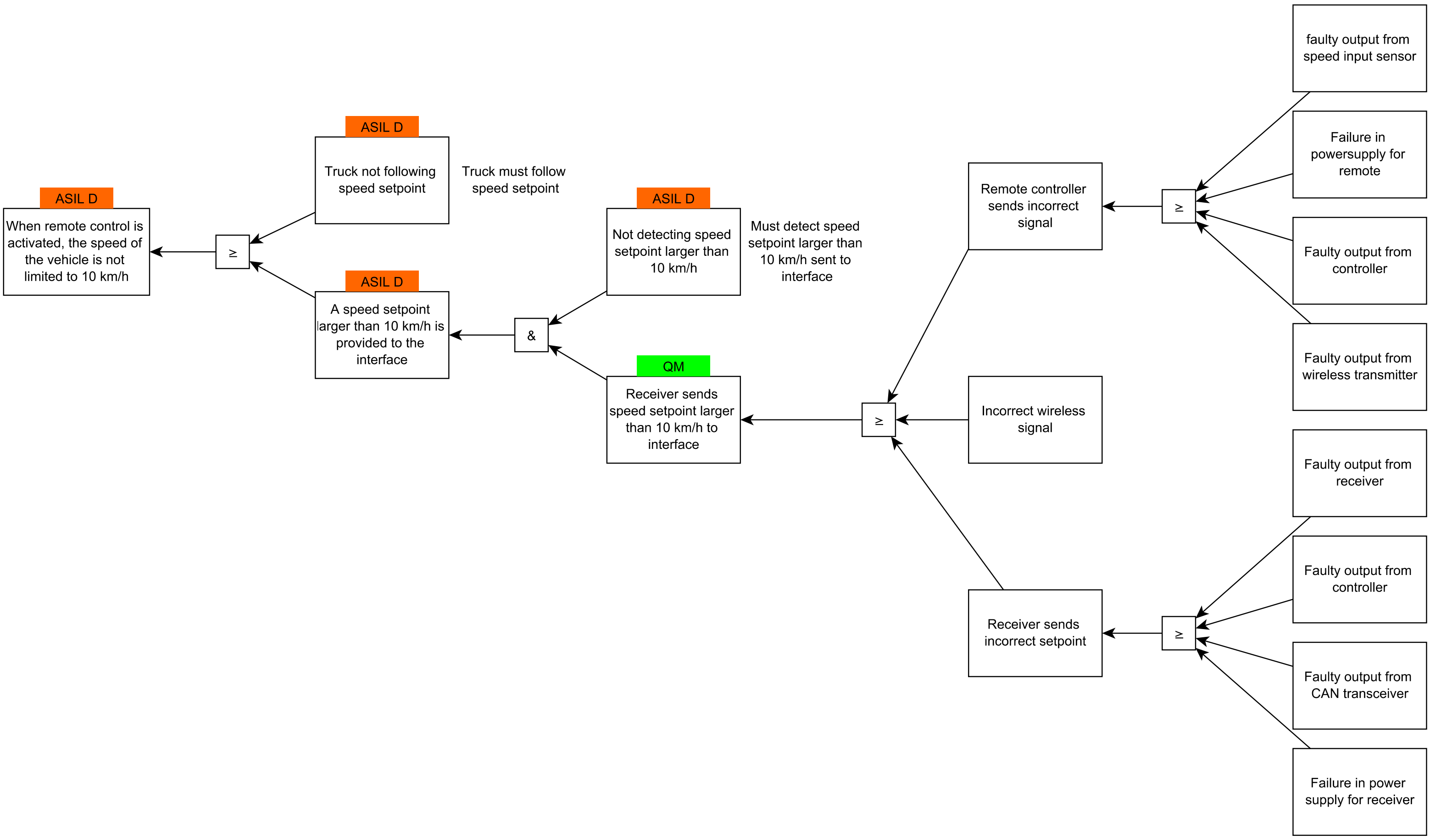
Braking	MF5: Loss of brakes request	OP1: Larger road 30+	Activated	29	RCT_HE_29	Collision at high speed	Severe Injury with possible death	High exposure, more than 10%	Steering still working, driver could try avoid collision but still hard to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF5: Loss of brakes request	OP2: Smaller road 30+	Activated	30	RCT_HE_30	Collision at high speed	Severe Injury with possible death	High exposure, more than 10%	Steering still working, driver could try avoid collision but still hard to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF5: Loss of brakes request	OP3: Smaller road or enclosed area 10-30	Activated	31	RCT_HE_31	Collision with VRU at moderate speed	Severe Injury with possible death	High exposure, more than 10%	Steering still working, driver could try avoid collision but still hard to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF5: Loss of brakes request	OP4: Smaller road or enclosed area 10-	Activated	32	RCT_HE_32	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Avoid collision by steering at low speed is normally controllable. VRU might avoid accident	S2	E4	C2	ASIL B	SG3	No loss of brake request when remote system activated	Apply full brake		
	MF5: Loss of brakes request	OP5: Parking, loading dock	Activated	33	RCT_HE_33	Collide with VRU at low speed	Severe injury survival likley	Moderate exposure 1-10%	Avoid collision by steering at low speed is normally controllable. VRU might avoid accident	S2	E3	C2	ASIL A	SG3	No loss of brake request when remote system activated	Apply full brake		
	MF5: Loss of brakes request	OP6: Parked	Activated	34	RCT_HE_34	Vehicle starts rolling and collide with VRU at low speed	Severe injury survival likley	High exposure, more than 10%	Avoid collision by steering at low speed is normally controllable. VRU might avoid accident	S2	E4	C2	ASIL B	SG3	No loss of brake request when remote system activated	Apply full brake		
	MF5: Loss of brakes request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	35	RCT_HE_35	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S2	E4	C3	ASIL C	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		
Braking	MF6: Braking delayed request	OP1: Larger road 30+	Activated	36	RCT_HE_36	Collision at high speed	Severe Injury with possible death	High exposure, more than 10%	Difficult to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF6: Braking delayed request	OP2: Smaller road 30+	Activated	37	RCT_HE_37	Collision at high speed with vehicle ahead	Severe Injury with possible death	High exposure, more than 10%	Difficult to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF6: Braking delayed request	OP3: Smaller road or enclosed area 10-30	Activated	38	RCT_HE_38	Collision with VRU at moderate speed	Severe Injury with possible death	High exposure, more than 10%	Difficult to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF6: Braking delayed request	OP4: Smaller road or enclosed area 10-	Activated	39	RCT_HE_39	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Avoid collision by steering at low speed is normally controllable. VRU might avoid accident	S2	E4	C2	ASIL B	SG5	No braking requests delayed more than X	Apply full brake		
	MF6: Braking delayed request	OP5: Parking, loading dock	Activated	40	RCT_HE_40	Collide with VRU at low speed	Severe injury survival likley	Moderate exposure 1-10%	Avoid collision by steering at low speed is normally controllable. VRU might avoid accident	S2	E3	C2	ASIL A	SG8	No requests delayed more than X	Apply full brake		
	MF6: Braking delayed request	OP6: Parked	Activated	41	RCT_HE_41	No hazard possible, vehicle not moving	Vehicle is not moving	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		
	MF6: Braking delayed request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	42	RCT_HE_42	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S2	E4	C3	ASIL C	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		

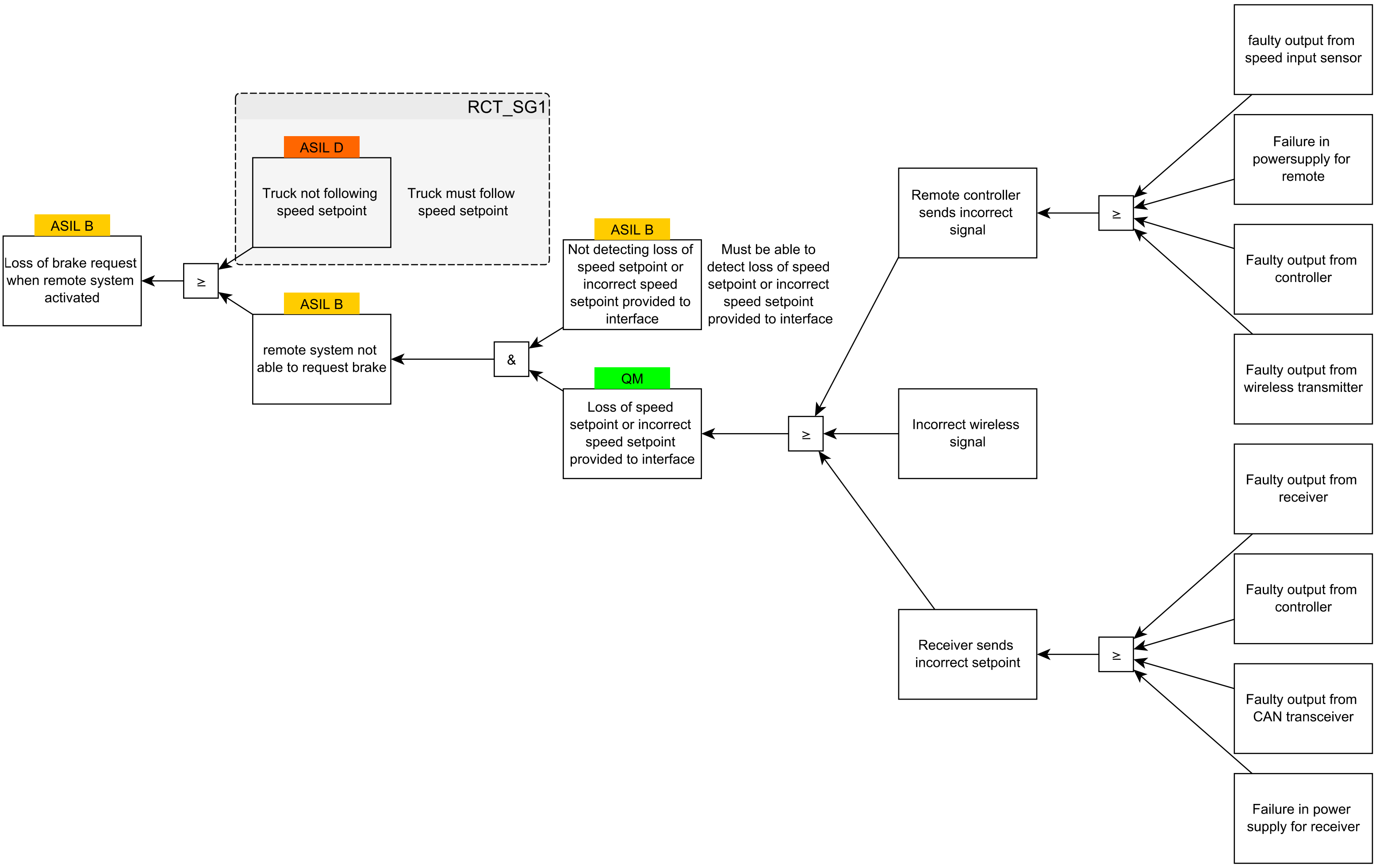
Driveline	MF7: Unintended acceleration request	OP1: Larger road 30+	Activated	43	RCT_HE_43	Collision at high speed with vehicle ahead	Severe Injury with possible death	High exposure, more than 10%	Highly controllable with steering and braking	S3	E4	C1	ASIL B	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF7: Unintended acceleration request	OP2: Smaller road 30+	Activated	44	RCT_HE_44	Collision at high speed with vehicle ahead	Severe Injury with possible death	High exposure, more than 10%	Highly controllable with steering and braking	S3	E4	C1	ASIL B	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF7: Unintended acceleration request	OP3: Smaller road or enclosed area 10-30	Activated	45	RCT_HE_45	Collision with VRU at moderate speed	Severe Injury with possible death	High exposure, more than 10%	Braking and steering to avoid accident	S3	E4	C1	ASIL B	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF7: Unintended acceleration request	OP4: Smaller road or enclosed area 10-	Activated	46	RCT_HE_46	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Controllable by braking, ~3m to stop including 1s reaction	S2	E4	C1	ASIL A	SG6	No unintended acceleration requests	Apply full brake		
	MF7: Unintended acceleration request	OP5: Parking, loading dock	Activated	47	RCT_HE_47	Colide with VRU or frontal collision	Severe injury survival likley	Moderate exposure 1-10%	Very controllable, brake and steering still intact	S2	E3	C1	QM		--	Apply full brake		
	MF7: Unintended acceleration request	OP6: Parked	Activated	48	RCT_HE_48	Truck rushes forward and ram a VRU, operator might be unaware of the rampaging truck	Severe injury survival likley	High exposure, more than 10%	Very controllable, brake and steering still intact	S2	E4	C1	ASIL A	SG6	No unintended acceleration requests	Apply full brake		
	MF7: Unintended acceleration request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	49	RCT_HE_49	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S2	E4	C3	ASIL C	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		
Driveline	MF8: Loss of acceleration request	OP1: Larger road 30+	Activated	50	RCT_HE_50	Vehicle hit in the back by vehicle from behind	Survival probable, severe injuries might occur	High exposure, more than 10%	Highly controllable, also vehicles from behind will easily avoid the slowing down vehicle	S2	E4	C0	QM	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF8: Loss of acceleration request	OP2: Smaller road 30+	Activated	51	RCT_HE_51	Vehicle hit in the back by vehicle from behind	Survival probable, severe injuries might occur	High exposure, more than 10%	Highly controllable, also vehicles from behind will easily avoid the slowing down vehicle	S2	E4	C0	QM	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF8: Loss of acceleration request	OP3: Smaller road or enclosed area 10-30	Activated	52	RCT_HE_52	Vehicle hit in the back by vehicle from behind	Moderate injuries	High exposure, more than 10%	Highly controllable, also vehicles from behind will easily avoid the slowing down vehicle	S1	E4	C0	QM	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF8: Loss of acceleration request	OP4: Smaller road or enclosed area 10-	Activated	53	RCT_HE_53	No hazard possible, brake and steering working	No injuries	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		
	MF8: Loss of acceleration request	OP5: Parking, loading dock	Activated	54	RCT_HE_54	No hazard possible, brake and steering working	No injuries	Moderate exposure 1-10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		
	MF8: Loss of acceleration request	OP6: Parked	Activated	55	RCT_HE_55	No hazard possible, vehicle not moving	No injuries, vehicle is not moving	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Apply full brake		
	MF8: Loss of acceleration request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	56	RCT_HE_56	No hazard possible, brake and steering working	No injuries	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S0	E4	C3	QM		--	Apply full brake		
Driveline	MF9: Delayed acceleration request	OP1: Larger road 30+	Activated	57	RCT_HE_57	Collision at high speed with vehicle ahead	Severe Injury with possible death	High exposure, more than 10%	Highly controllable with steering and braking	S3	E4	C1	ASIL B	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		

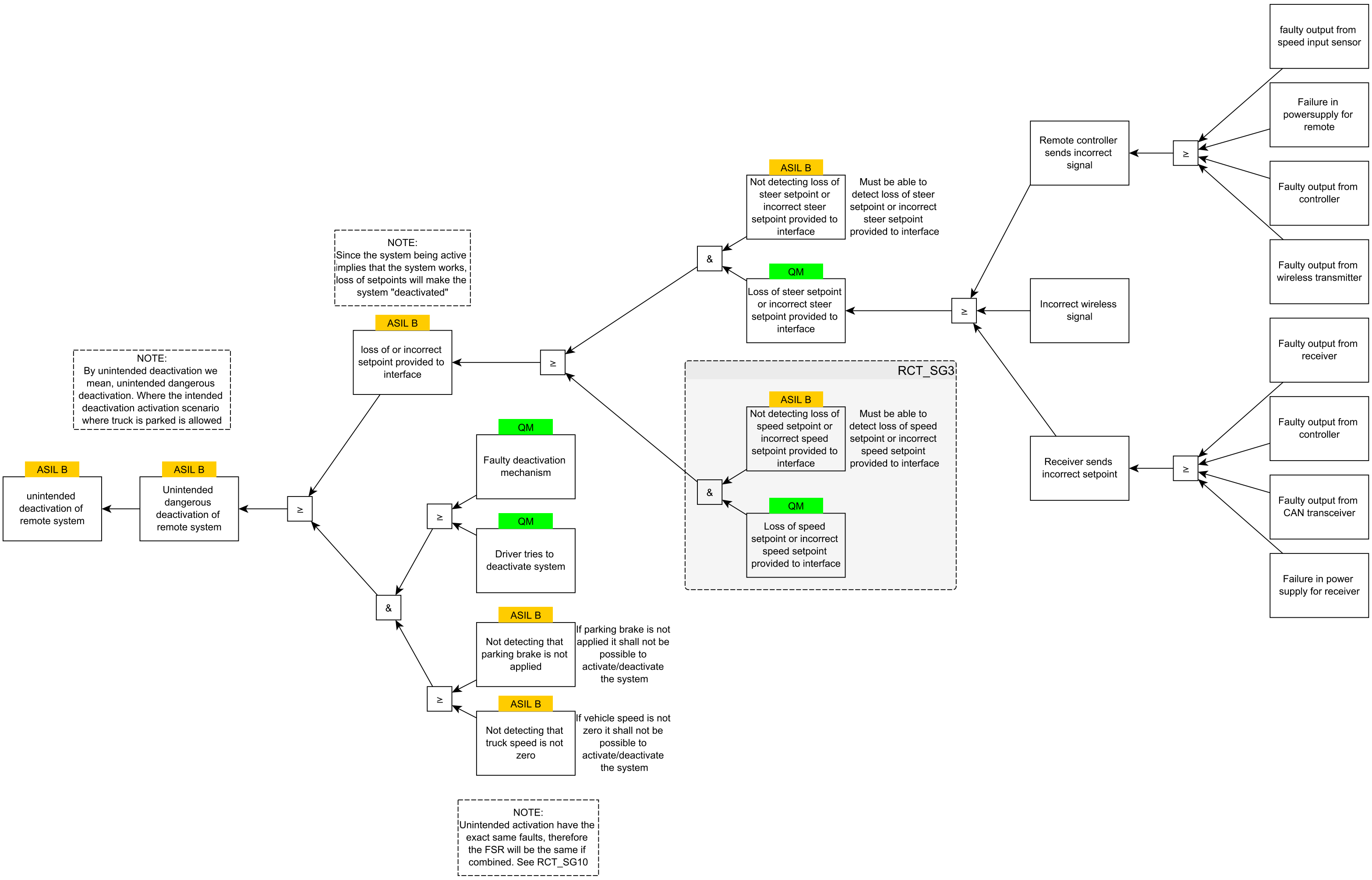
	MF9: Delayed acceleration request	OP2: Smaller road 30+	Activated	58	RCT_HE_58	Collision at high speed with vehicle ahead	Severe Injury with possible death	High exposure, more than 10%	Highly controllable with steering and braking	S3	E4	C1	ASIL B	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF9: Delayed acceleration request	OP3: Smaller road or enclosed area 10-30	Activated	59	RCT_HE_59	Collision with VRU at moderate speed	Severe Injury with possible death	High exposure, more than 10%	Braking and steering to avoid accident	S3	E4	C1	ASIL B	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF9: Delayed acceleration request	OP4: Smaller road or enclosed area 10-	Activated	60	RCT_HE_60	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Controllable by braking, ~3m to stop including 1s reaction	S2	E4	C1	ASIL A	SG8	No requests delayed more than X	Apply full brake		
	MF9: Delayed acceleration request	OP5: Parking, loading dock	Activated	61	RCT_HE_61	Colide with VRU or frontal collision	Severe injury survival likley	Moderate exposure 1-10%	Very controllable, brake and steering still intact	S2	E3	C1	QM		--	Apply full brake		
	MF9: Delayed acceleration request	OP6: Parked	Activated	62	RCT_HE_62	Truck rushes forward and ram a VRU, operator might be unaware of the rampaging truck	Severe injury survival likley	High exposure, more than 10%	Very controllable, brake and steering still intact	S2	E4	C1	ASIL A	SG8	No requests delayed more than X	Apply full brake		
	MF9: Delayed acceleration request	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	63	RCT_HE_63	Colide with VRU or frontal collision	Severe injury survival likley	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S2	E4	C3	ASIL C	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		
Communication	MF10: Unintended activation of remote system	OP1: Larger road 30+	Activated	64	RCT_HE_64	Frontal collision or hit in the back by vehicle from behind	Severe Injury with possible death	High exposure, more than 10%	Difficult to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Remote system decativated		
	MF10: Unintended activation of remote system	OP2: Smaller road 30+	Activated	65	RCT_HE_65	Frontal collision or hit in the back by vehicle from behind	Severe Injury with possible death	High exposure, more than 10%	Difficult to control	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Remote system decativated		
	MF10: Unintended activation of remote system	OP3: Smaller road or enclosed area 10-30	Activated	66	RCT_HE_66	Frontal collision or hit in the back by vehicle from behind	Severe Injury with possible death	High exposure, more than 10%	Difficult to control	S2	E4	C3	ASIL C	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Remote system decativated		
	MF10: Unintended activation of remote system	OP4: Smaller road or enclosed area 10-	Activated	67	RCT_HE_67	Collision with VRU at low speed	Light injuries	High exposure, more than 10%	VRU might avoid the accident, else difficult to control	S2	E4	C2	ASIL B	SG10	No unintended activation of remote system	Remote system decativated		
	MF10: Unintended activation of remote system	OP5: Parking, loading dock	Activated	68	RCT_HE_68	Collision with VRU at low speed	Light injuries	Moderate exposure 1-10%	VRU might avoid the accident, else difficult to control	S2	E3	C2	ASIL A	SG10	No unintended activation of remote system	Remote system decativated		
	MF10: Unintended activation of remote system	OP6: Parked	Activated	69	RCT_HE_69	No hazard possible, vehicle not moving	Vehicle is not moving	High exposure, more than 10%	Controllable in general	S0	E4	C0	QM		--	Remote system decativated		
	MF10: Unintended activation of remote system	OP7: Driving without being aware of obstacles in vehicle path at 10-	Activated	70	RCT_HE_70	Collision with VRU at low speed	Light injuries	High exposure, more than 10%	Driver can not see the collision, uncontrollable	S1	E4	C3	ASIL B	SG2	Driver must be aware of obstacles in vehicle path	Remote system decativated		
Communication	MF11: Unintended deactivation of remote system	OP1: Larger road 30+	Deactivated	71	RCT_HE_71	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	Uncontrollable	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		
	MF11: Unintended deactivation of remote system	OP2: Smaller road 30+	Deactivated	72	RCT_HE_72	Frontal collision or running off-road at high speed	Severe Injury with possible death	High exposure, more than 10%	Uncontrollable	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	N/A		

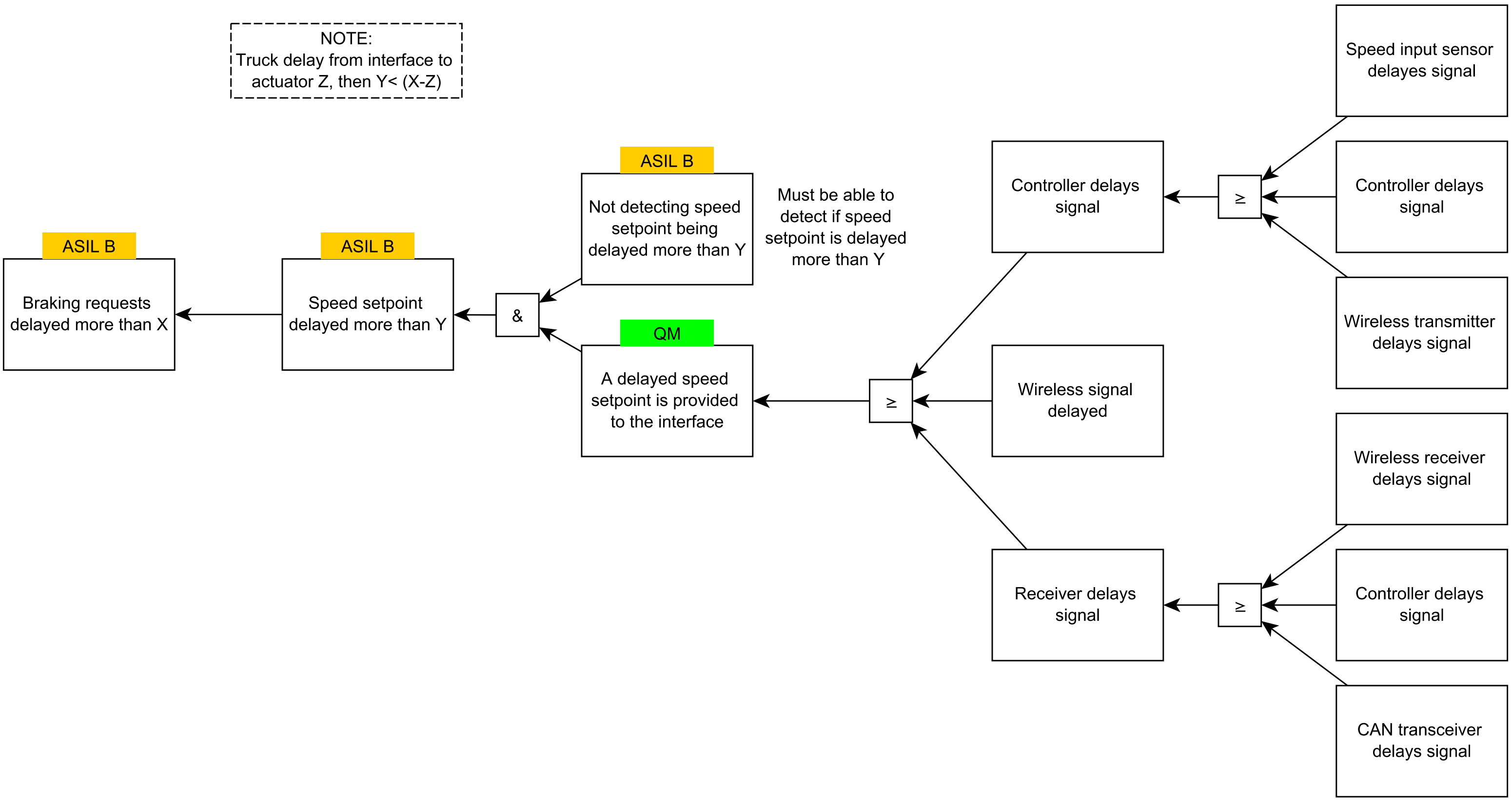
	MF11: Unintended deactivation of remote system	OP3: Smaller road or enclosed area 10-30	Deactivated	73	RCT_HE_73	Collision with VRU at moderate speed	Severe Injury with possible death	High exposure, more than 10%	Uncontrollable	S3	E4	C3	ASIL D	SG1	When remote control is activated, the speed of the vehicle shall be limited to 10 km/h	Apply full brake		
	MF11: Unintended deactivation of remote system	OP4: Smaller road or enclosed area 10-	Deactivated	74	RCT_HE_74	Collision with VRU at low speed	Low speed but still severe injury probable	High exposure, more than 10%	VRU might avoid the accident, else uncontrollable	S2	E4	C2	ASIL B	SG4	No unintended deactivation of remote system	Apply full brake		
	MF11: Unintended deactivation of remote system	OP5: Parking, loading dock	Deactivated	75	RCT_HE_75	Collision with VRU at low speed	Severe injury survival likley	Moderate exposure 1-10%	VRU might avoid the accident, else uncontrollable	S2	E3	C2	ASIL A	SG4	No unintended deactivation of remote system	Apply full brake		
	MF11: Unintended deactivation of remote system	OP6: Parked	Deactivated	76	RCT_HE_76	No hazard possible, vehicle not moving	Vehicle is not moving	High exposure, more than 10%	Uncontrollable	S0	E4	C3	QM	SG4	No unintended deactivation of remote system	Apply full brake		
	MF11: Unintended deactivation of remote system	OP7: Driving without being aware of obstacles in vehicle path at 10-	Deactivated	77	RCT_HE_77	Collision with VRU at low speed	Low speed but still severe injury probable	High exposure, more than 10%	VRU might avoid the accident, else uncontrollable	S2	E4	C2	ASIL B	SG2	Driver must be aware of obstacles in vehicle path	Apply full brake		

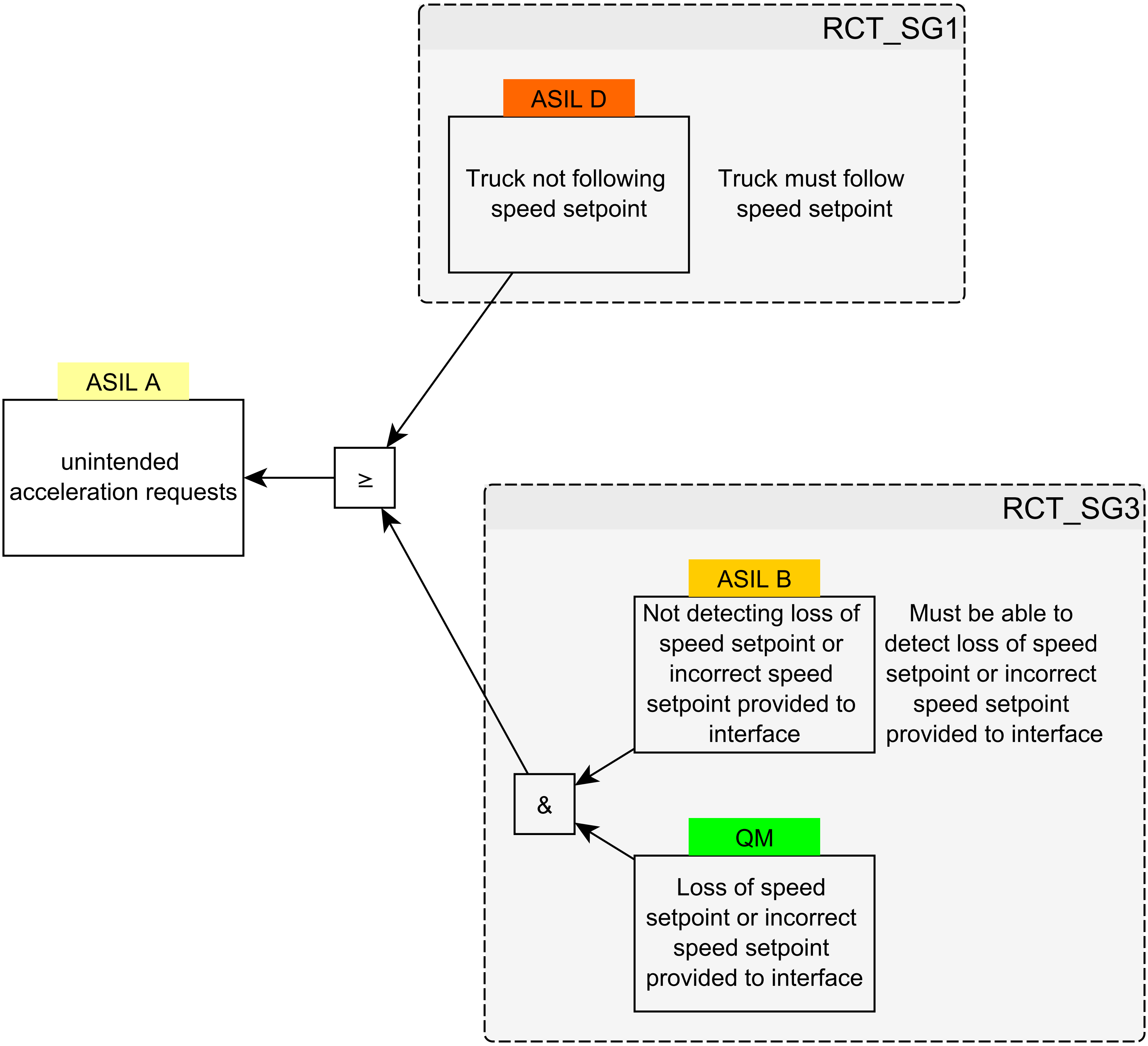
F.4 Fault tree analysis figures

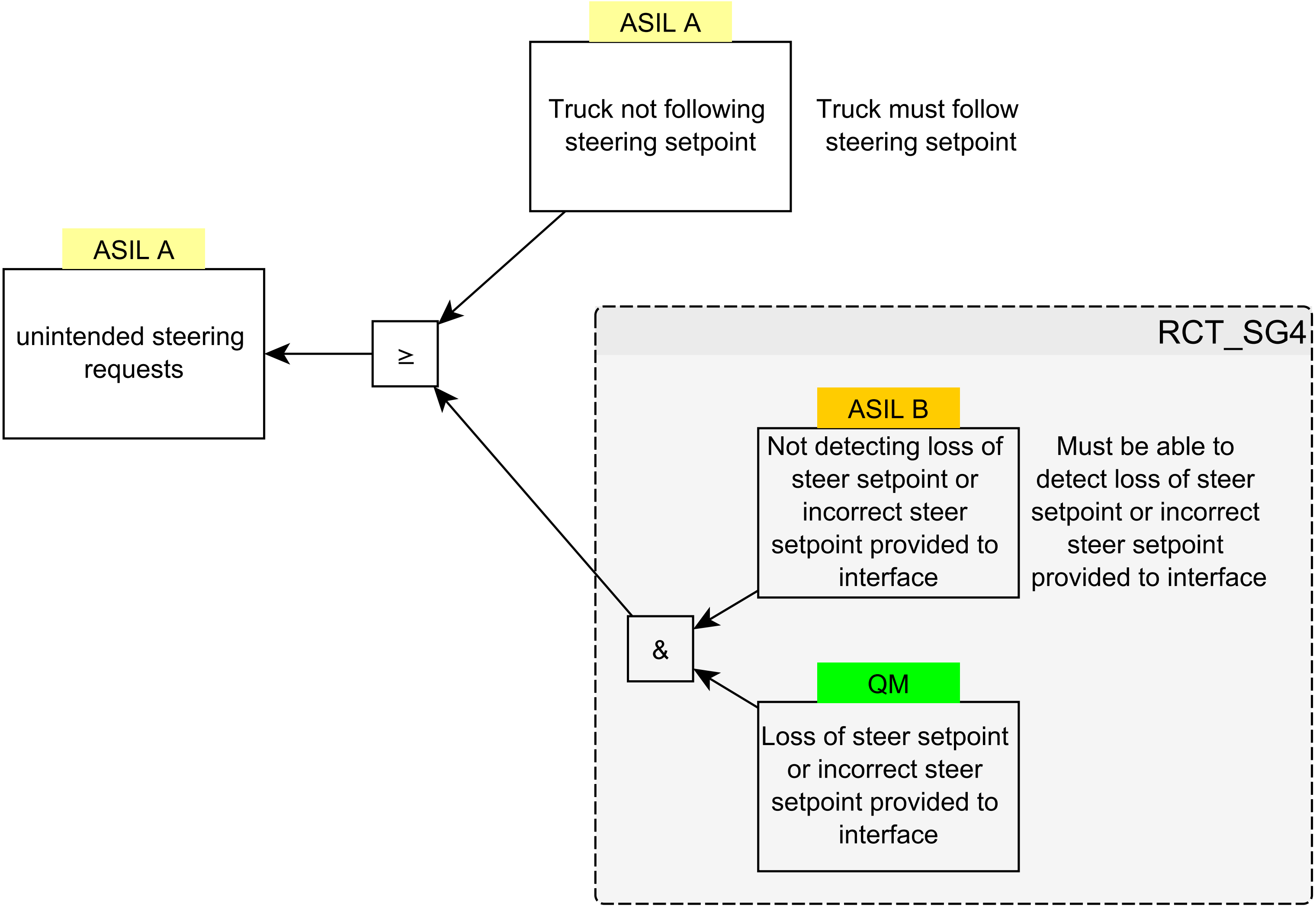

ASIL D
When remote control is activated, the speed of the vehicle is not limited to 10 km/h
≥
ASIL D
Truck not following speed setpoint
Truck must follow speed setpoint
ASIL D
A speed setpoint larger than 10 km/h is provided to the interface
&
ASIL D
Not detecting speed setpoint larger than 10 km/h
Must detect speed setpoint larger than 10 km/h sent to interface
QM
Receiver sends speed setpoint larger than 10 km/h to interface
≥
Remote controller sends incorrect signal
Incorrect wireless signal
Receiver sends incorrect setpoint
≥
faulty output from speed input sensor
Failure in powersupply for remote
Faulty output from controller
Faulty output from wireless transmitter
≥
Faulty output from receiver
Faulty output from controller
Faulty output from CAN transceiver
Failure in power supply for receiver

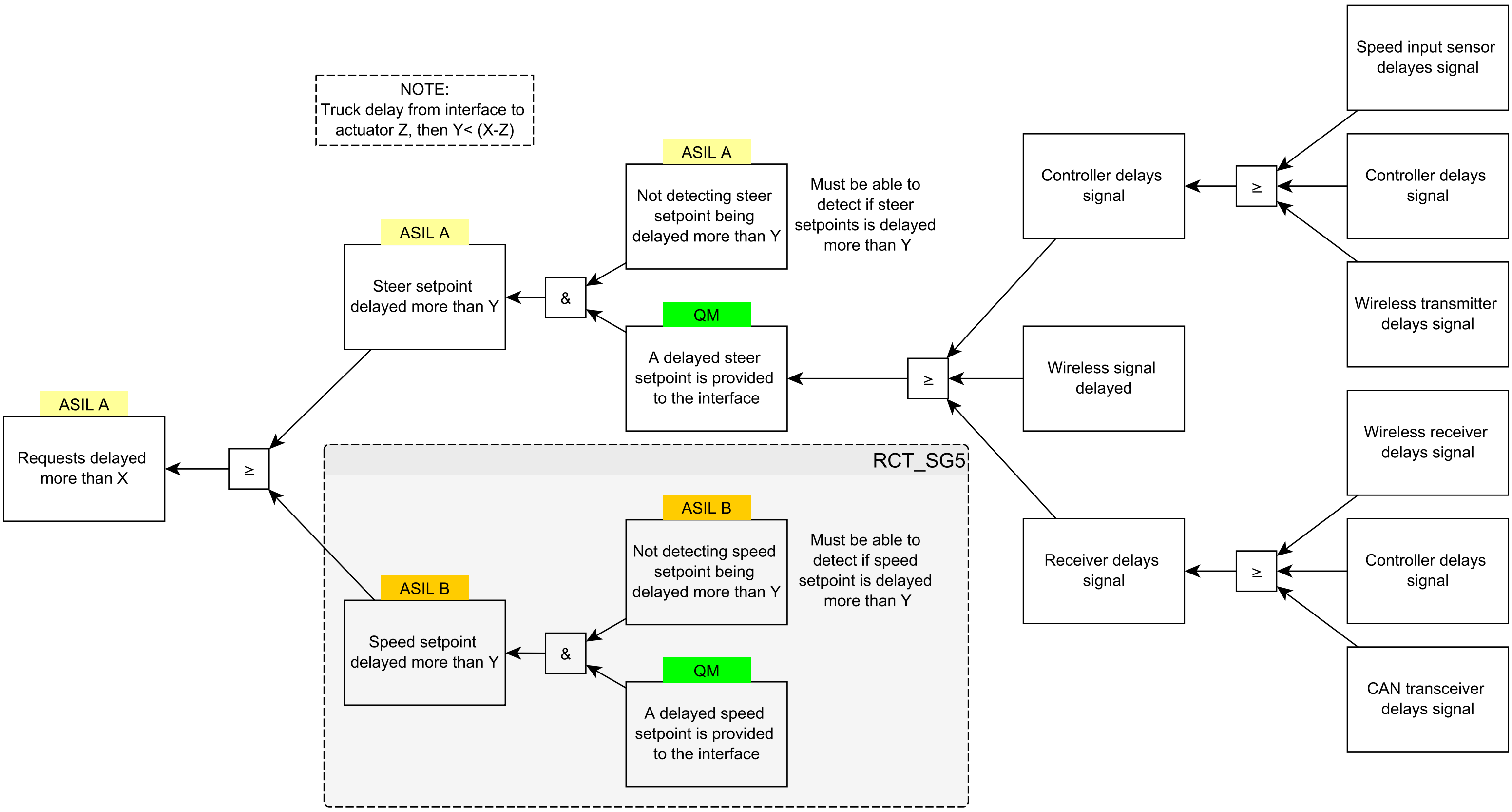

RCT_SG1
ASIL D
Truck not following speed setpoint
Truck must follow speed setpoint
ASIL B
Loss of brake request when remote system activated
≥
ASIL B
remote system not able to request brake
&
ASIL B
Not detecting loss of speed setpoint or incorrect speed setpoint provided to interface
Must be able to detect loss of speed setpoint or incorrect speed setpoint provided to interface
QM
Loss of speed setpoint or incorrect speed setpoint provided to interface
≥
Remote controller sends incorrect signal
Incorrect wireless signal
Receiver sends incorrect setpoint
≥
faulty output from speed input sensor
Failure in powersupply for remote
Faulty output from controller
Faulty output from wireless transmitter
≥
Faulty output from receiver
Faulty output from controller
Faulty output from CAN transceiver
Failure in power supply for receiver

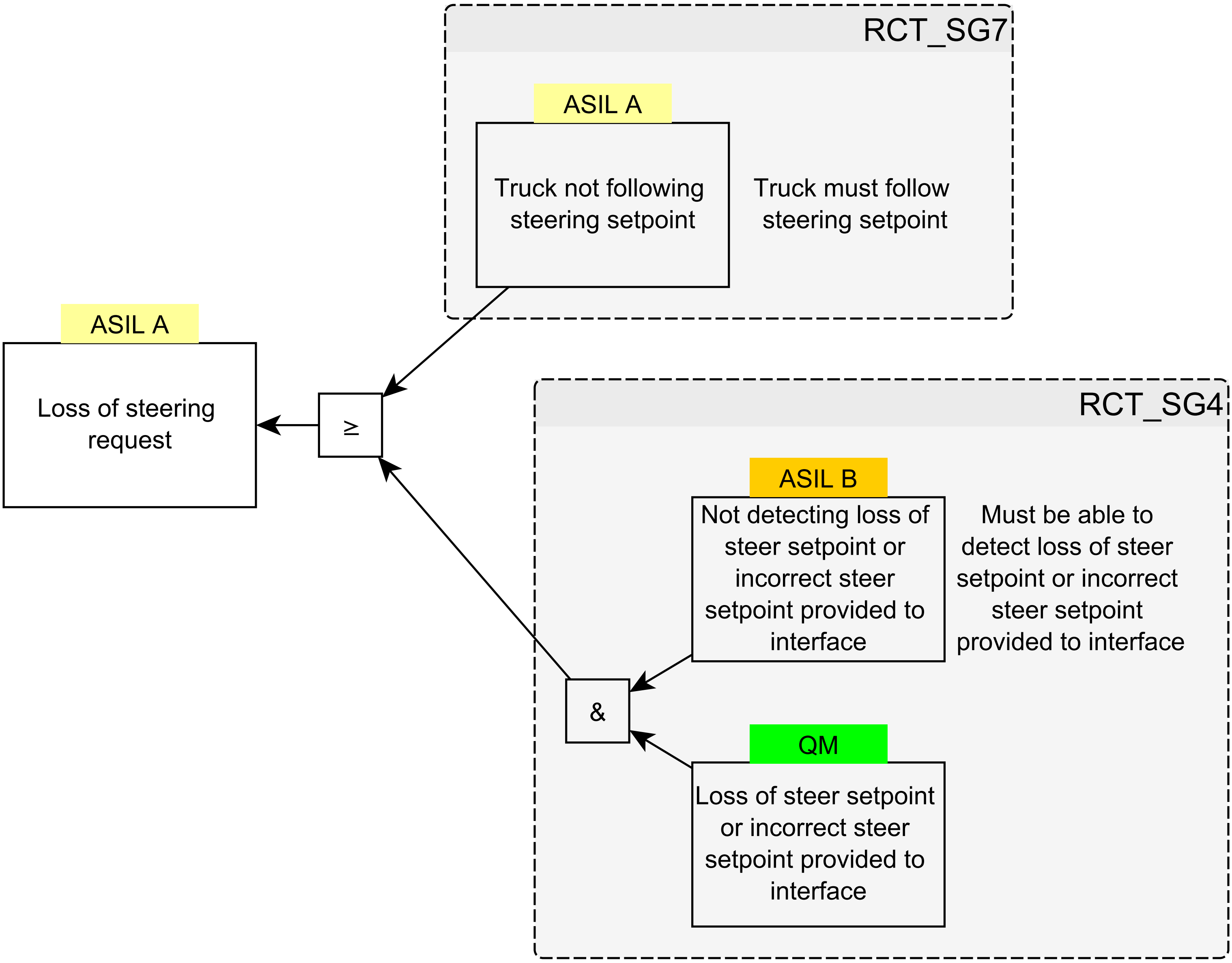

faulty output from speed input sensor
Failure in powersupply for remote
Faulty output from controller
Faulty output from wireless transmitter
Faulty output from receiver
Faulty output from controller
Faulty output from CAN transceiver
Failure in power supply for receiver
Remote controller sends incorrect signal
Incorrect wireless signal
Receiver sends incorrect setpoint
≥
≥
≥
ASIL B
Not detecting loss of steer setpoint or incorrect steer setpoint provided to interface
Must be able to detect loss of steer setpoint or incorrect steer setpoint provided to interface
QM
Loss of steer setpoint or incorrect steer setpoint provided to interface
&
RCT_SG3
ASIL B
Not detecting loss of speed setpoint or incorrect speed setpoint provided to interface
Must be able to detect loss of speed setpoint or incorrect speed setpoint provided to interface
QM
Loss of speed setpoint or incorrect speed setpoint provided to interface
&
≥
NOTE:
Since the system being active implies that the system works, loss of setpoints will make the system "deactivated"
ASIL B
loss of or incorrect setpoint provided to interface
NOTE:
By unintended deactivation we mean, unintended dangerous deactivation. Where the intended deactivation activation scenario where truck is parked is allowed
ASIL B
unintended deactivation of remote system
ASIL B
Unintended dangerous deactivation of remote system
≥
QM
Faulty deactivation mechanism
QM
Driver tries to deactivate system
≥
&
ASIL B
Not detecting that parking brake is not applied
If parking brake is not applied it shall not be possible to activate/deactivate the system
ASIL B
Not detecting that truck speed is not zero
If vehicle speed is not zero it shall not be possible to activate/deactivate the system
≥
NOTE:
Unintended activation have the exact same faults, therefore the FSR will be the same if combined. See RCT_SG10

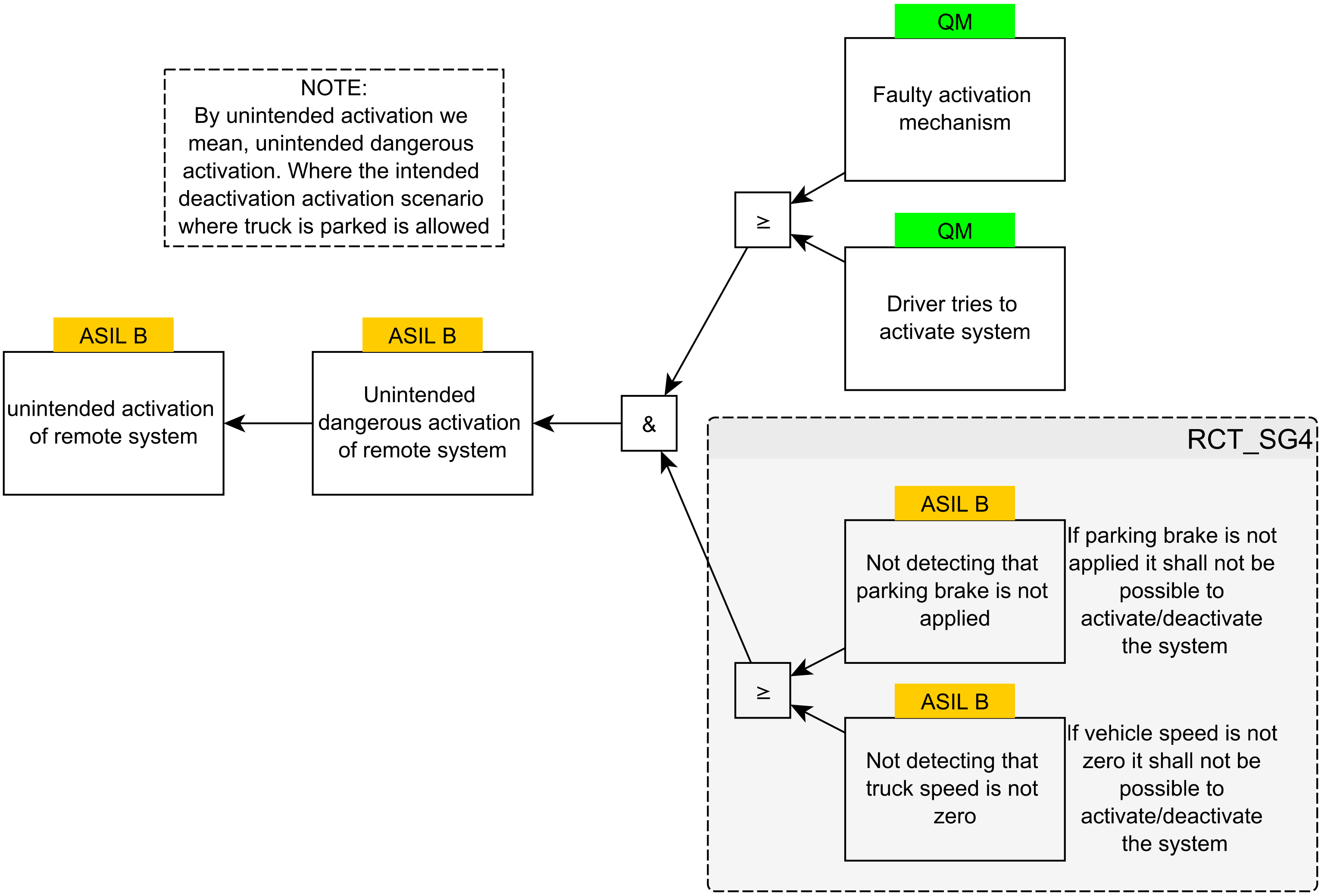

NOTE:
Truck delay from interface to actuator Z, then Y< (X-Z)
ASIL B
Braking requests delayed more than X
ASIL B
Speed setpoint delayed more than Y
&
ASIL B
Not detecting speed setpoint being delayed more than Y
Must be able to detect if speed setpoint is delayed more than Y
QM
A delayed speed setpoint is provided to the interface
≥
Controller delays signal
Wireless signal delayed
Receiver delays signal
≥
Speed input sensor delayes signal
Controller delays signal
Wireless transmitter delays signal
≥
Wireless receiver delays signal
Controller delays signal
CAN transceiver delays signal


RCT_SG1
ASIL D
Truck not following speed setpoint
Truck must follow speed setpoint
ASIL A
unintended acceleration requests
≥
RCT_SG3
ASIL B
Not detecting loss of speed setpoint or incorrect speed setpoint provided to interface
Must be able to detect loss of speed setpoint or incorrect speed setpoint provided to interface
&
QM
Loss of speed setpoint or incorrect speed setpoint provided to interface


ASIL A
Truck not following steering setpoint
Truck must follow steering setpoint
ASIL A
unintended steering requests
≥
RCT_SG4
ASIL B
Not detecting loss of steer setpoint or incorrect steer setpoint provided to interface
Must be able to detect loss of steer setpoint or incorrect steer setpoint provided to interface
&
QM
Loss of steer setpoint or incorrect steer setpoint provided to interface


NOTE:
Truck delay from interface to actuator Z, then Y< (X-Z)
ASIL A
Requests delayed more than X
≥
ASIL A
Steer setpoint delayed more than Y
&
ASIL A
Not detecting steer setpoint being delayed more than Y
Must be able to detect if steer setpoints is delayed more than Y
QM
A delayed steer setpoint is provided to the interface
≥
Controller delays signal
Wireless signal delayed
Receiver delays signal
≥
Speed input sensor delayes signal
Controller delays signal
Wireless transmitter delays signal
≥
Wireless receiver delays signal
Controller delays signal
CAN transceiver delays signal
RCT_SG5
ASIL B
Speed setpoint delayed more than Y
&
ASIL B
Not detecting speed setpoint being delayed more than Y
Must be able to detect if speed setpoint is delayed more than Y
QM
A delayed speed setpoint is provided to the interface


RCT_SG7
ASIL A
Truck not following steering setpoint
Truck must follow steering setpoint
ASIL A
Loss of steering request
≥
RCT_SG4
ASIL B
Not detecting loss of steer setpoint or incorrect steer setpoint provided to interface
Must be able to detect loss of steer setpoint or incorrect steer setpoint provided to interface
&
QM
Loss of steer setpoint or incorrect steer setpoint provided to interface


NOTE:
By unintended activation we mean, unintended dangerous activation. Where the intended deactivation activation scenario where truck is parked is allowed
QM
Faulty activation mechanism
≥
QM
Driver tries to activate system
ASIL B
unintended activation of remote system
ASIL B
Unintended dangerous activation of remote system
&
RCT_SG4
ASIL B
Not detecting that parking brake is not applied
If parking brake is not applied it shall not be possible to activate/deactivate the system
≥
ASIL B
Not detecting that truck speed is not zero
If vehicle speed is not zero it shall not be possible to activate/deactivate the system