UWA GENG5512 SEMESTER 2 2019
SCHOOL OF MECHANICAL ENGINEERING

Redesign the Safety System of an Autonomous Formula SAE-Electric Vehicle

Research Project Final Report

(Word Count: 6045)

Junwen Huang (22191737)

Supervisor: Professor Dr. Thomas Bräunl

Abstract

The safety system is a crucial part of an autonomous vehicle, which can protect the vehicle, driver, and people nearby. By implementing the safety system, the driver can instantly stop the vehicle by several methods or stop by vehicle itself when failures happen, especially when the autonomous driving mode is processing. This dissertation describes the redesigned development of the safety system, which has implemented on an autonomous Formula SAE vehicle. A printed circuit board (PCB) was designed as independent hardware for the safety system. The PCB design process through Eagle CAD, which is consists of two major stages, schematic and board layout, is described. The selection of electronic components based on the expected function will be discussed in the schematic stage, and the optimisation in the board layout design process will be demonstrated. A Launchpad (Hercules TMS570LC43x) from Texas Instruments, which specially designed for the vehicle field, will be introduced as the controller of the safety system. Software tools, a code generation tool (HALCoGen), and a Code Composer Studio (CCS) that based on C language are introduced to the controller to execute the safety functions. The new vehicle dashboard will be applied for the introduction and deletion of the device to fix the new safety system. Future development is considered during the process, and it presents in this dissertation.

Acknowledgement

I would like to thank the following people for their support and assistance in this project:

Prof. Thomas Bräunl for his guidance, suggestion and devotion to the REV Project.

Thomas H. Drage for his design advice, technical support and assistance.

My teammate Yi for his software assistance, PCB soldering and advice.

All of the team members for their invaluable advice and help.

My family and friends for their encouragement and support.

UWA mechanical workshop for their professional manufacturing parts and advance advice.

Nomenclature

UWA	The University of Western Australia
PCB	Printed Circuit Board
SAE	Society of Automotive Engineers
REV	Renewable Energy Vehicle Project
HALCoGen	Code Generation Tool
CCS	Code Composer Studio

Table of Contents

Table of Figures

1.Introduction and background

The autonomous vehicles have lots of benefits and are used in many fields, but there are concerns about their safety and risks are also being widely discussed [1]. A fatal crushing accident of Tesla's autopilot happened in 2016 which was pushed to the topic of safety to the cusp. The software uncertainty caused the accidence, and it shows the inability of the technology to avoid accidences in some specific scenarios [2]. However, a study shows 90% of car accidents caused by human mistake operations [3]. The autonomous vehicles can potentially decrease the accidences occurrence, and a study predicts that autonomous vehicles will take a quarter of the market share by 2040 [4]. Safety is a significant part of the autonomous vehicle which worth studying.

The Renewable Energy Vehicle (REV) project has modified a BMW X5 by implementing a driver assistant system, which enables help driver to avoid objects on the path [5]. The team developed a formula SAE-electric vehicle as to the testbed of the autonomous vehicle study. The formula SAE vehicle was created by UWA Motorsport, and it was converted entirely from piston racing vehicle to electric vehicle by the effort of several generations team members [6]. Although the SAE vehicle is much compact and straightforward than the commercial vehicle, it remains the fundamental functions including steering, brake, acceleration function. These functions implement most of the autonomous driving function. The absent of the dispensable components can reduce the risks they may bring. Therefore, the SAE vehicle is the ideal low-cost testbed of the autonomous driving study.

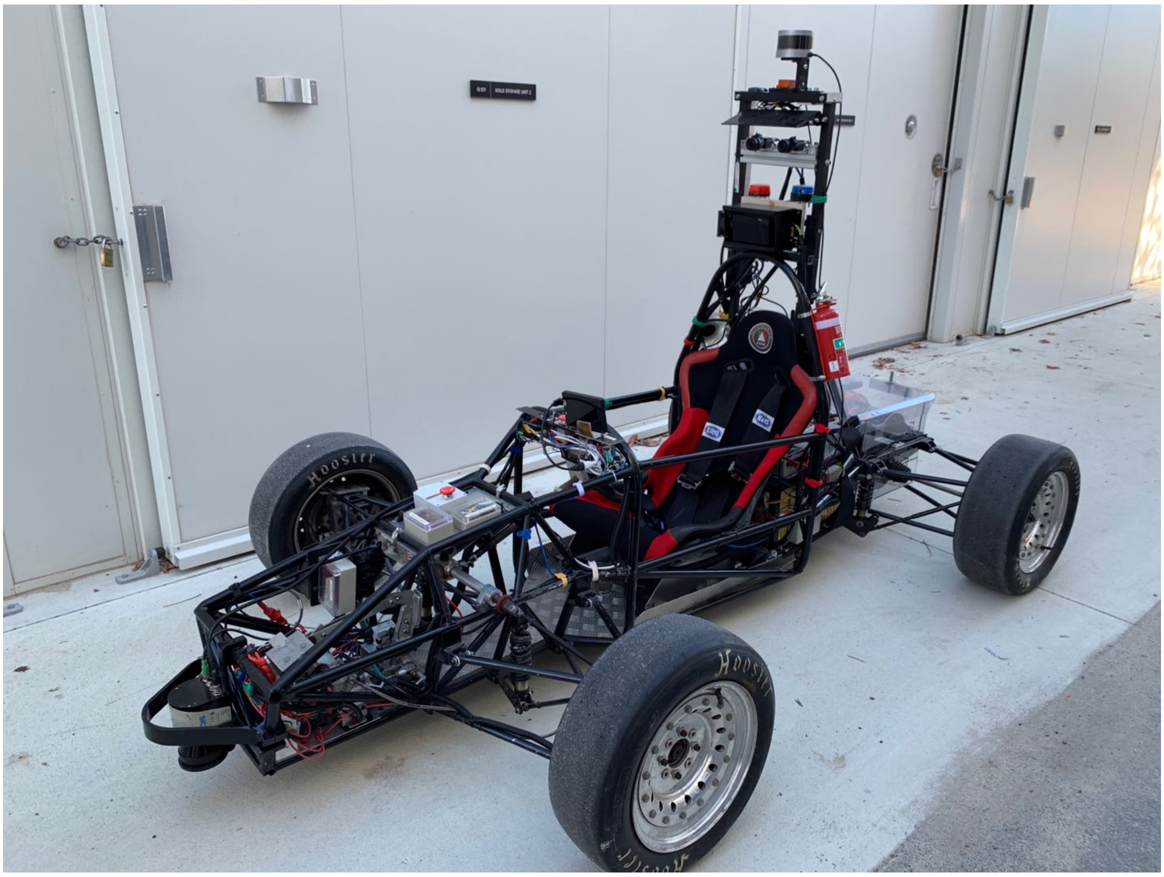


Figure 1 Formula SAE electric vehicle

The goals of the REV autonomous driving are developing the formula SAE vehicle to (1) Map the planned cones track and run smoothly, (2) Run automatically around internal UWA roads without prior planning and human operations. To achieve the goal the team has to ensure safety during the driving process such as protect the vehicle, driver and the bystander. Therefore, a safety system is added to the vehicle to achieve the functions. The previous safety system was designed and implemented to the vehicle in 2013 by previous student [7] [8]. As the development of the autonomous driving technology, the advanced devices and professional standards are introduced for further research.

This dissertation describes the redesign safety system process. A new printed circuit board (PCB), which is the hardware of the system, was designed by the Eagle CAD. The software part is developed by code generation tool (HALCoGen) and a Code Composer Studio (CCS). A new dashboard model was designed to support more devices and future development, and it is modelled in Siemens NX (UG). Besides, two other contributions to increase the safety of the vehicle are discussed in the dissertation. The new safety system is called the "safety instrumented system".

2. PCB design

2.1 Overview

The safety system is to protect the vehicle from risks especially when processing the autonomous driving mode. It has three main functions. Firstly, it can analyse and identify the risks. Secondly, it can detect failures and stop the vehicle when failures happen. Lastly, it can stop the vehicle quickly when we need it. The previous safety system can achieve these functions to some extent. However, due to limitations of the old-style devices and designs, they are not achieved perfectly.

The previous safety system was designed by Thomas Drage [7]and Jordan Kalinowski [8]in 2013 and modified by two notable changes since 2014 [9]. The safety system consists of low-level safety circuit and safety supervisor. The low-level system handles physical outputs of SAE vehicle control system, for example, brake servomotor operation and signal to the steering control system. The low-level safety circuit, which separates from the high-level circuit, is non-programable and straightforward to increase its reliability. The advantage of it is the safety system can still execute its functions in a scenario such as low-level autonomous parts is disabled, and when the code is running on the system or the microcontroller developing a fault. The low-level safety circuit uses combinational logic chips and comparators which can drive relays physically cut off the connections of the autonomous system. The driver inputs signal from the steering motor, brake hall sensor and brake servo hall sensor will be compared with the set voltage by comparators. If the input voltage is higher than the set voltage, the relay will be energised and cut off the power to motors and unlock the steering wheel. The safety supervisor is introduced to the system for providing a level of redundancy to the vehicle safety systems. Additional risk-reduction is achieved by using it to not only monitor the control systems and human interaction but also perform independent actions in trip status.

However, the previous safety system has some limitations of reliability, flexibility and accuracy, further development potential. Firstly, the safety supervisor and low-level safety circuit are the bread-board-based design. The breadboard is unreliable because it can easily cause the short circuit. Secondly, the low-level safety circuit is non-programmable. The team set a specific position for the brake server, which needs to be adjusted manually. In actual tests drive, this position may be slightly offset due to vibrations caused during driving. This will cause the system to issue a brake command in error. Solving this problem needs manual adjustment and not accurate. The last one is that there is no space to install more components in the current closure boxes. The size of the box matches the size of the breadboard, which is covered with wires and it is difficult to add more components. Besides, vehicle dashboards are also not enough to provide more space for future development.

In order to solve the above limitations, our design team proposed several solutions. Firstly, designing a PCB to replace the current breadboard design. To save space, we will combine the low-level safety circuit with the safety supervisor. In addition, the team used a more advanced controller to replace the PIC controller that was originally in the safety supervisor.

2.2 PCB Design Process

2.2.1 Preliminary work

Before we start designing the PCB, the team needs some preliminary work to sort out the design process in a more comprehensive and targeted manner. These preliminary tasks include sorting out the functions of the new system and figuring out the current safety supervisor and low-level safety circuit inputs and outputs. These preliminary works can help us save design time and cost, because the team can refer to the original design and reasonable places. Besides, if we find that there are unreasonable places, we can never use such design then improve or redesign them.

The functions of the whole safety system have been sorted out with the assistant of Thomas Drage. The functions have implemented on the existing system which created and modified by previous year team members. The functions were collected from Thomas Drage [7], Jordan Kalinowski [8], William Lai reports [10], and they are listed by the logic tree [11], like the example shown below:

Table 1Example of the function list

Interlock ID	IF	WHEN	THEN	WHY	HOW
1	Steering motor over current	Safety supervisor is armed	Low-Level Safety circuit causes a trip of the safety supervisor, by wiring the relay contacts in series with the safety supervisors e-stop feedback	Stop autonomous driving if a human has taken over	Safety Supervisor
2	Steering motor over current	Autonomous system powered	- The steering motor is disconnected-The indicator of excess steering force light	Allow human to take over steering if interference detected. Protect mechanical system from over-torque.	Low-Level Safety Circuit

Below are the explanations of each column:

"If steering motor overcurrent when the safety supervisor is armed. Then the low-level safety circuit causes a trip of the safety supervisor by wiring the relay contacts in series with the safety supervisor's e-stop feedback."

"IF": some conditions occur

"WHEN": the status of the SAE vehicle

"THEN": the output of the safety system

"WHY": why safety system needs this function

"HOW": which part of the safety system is responsible for executing this function

There are 14 conditions that will trigger the safety system to execute the functions, and there are more than 20 outputs can be achieved. After listing all the functions, it is clear to know what functions should be integrated into the new circuit.

The second part of the preliminary work is to figure out the input and output of all components on the current safety supervisor and low-level safety circuit. This task can help the team understands how the current system works, such as which pin is used and where should it connect to which pin. Once the team figure out them, they can be used in the next stage. Since these two parts were designed by the previous final year project students, the labels on the schematic are not clear and do not meet the standards. The team are not sure where are the pins connected to. Eventually, we have successfully listed the input and output tables by reading the designer's graduation design report and further study of the circuit schematic.

2.2.2 Schematic

The part of the schematic is to connect the pins to be used on each component through Eagle CAD. Because the team have already known which pin to use through the preliminary work, this part is to find the model of the component from various resource libraries, and then connect them correctly. The original safety supervisor also has the schema of Eagle CAD, so the team create a new schematic based on the old one. The specific improvements and their advantages will be analysed in detail in section 2.3.

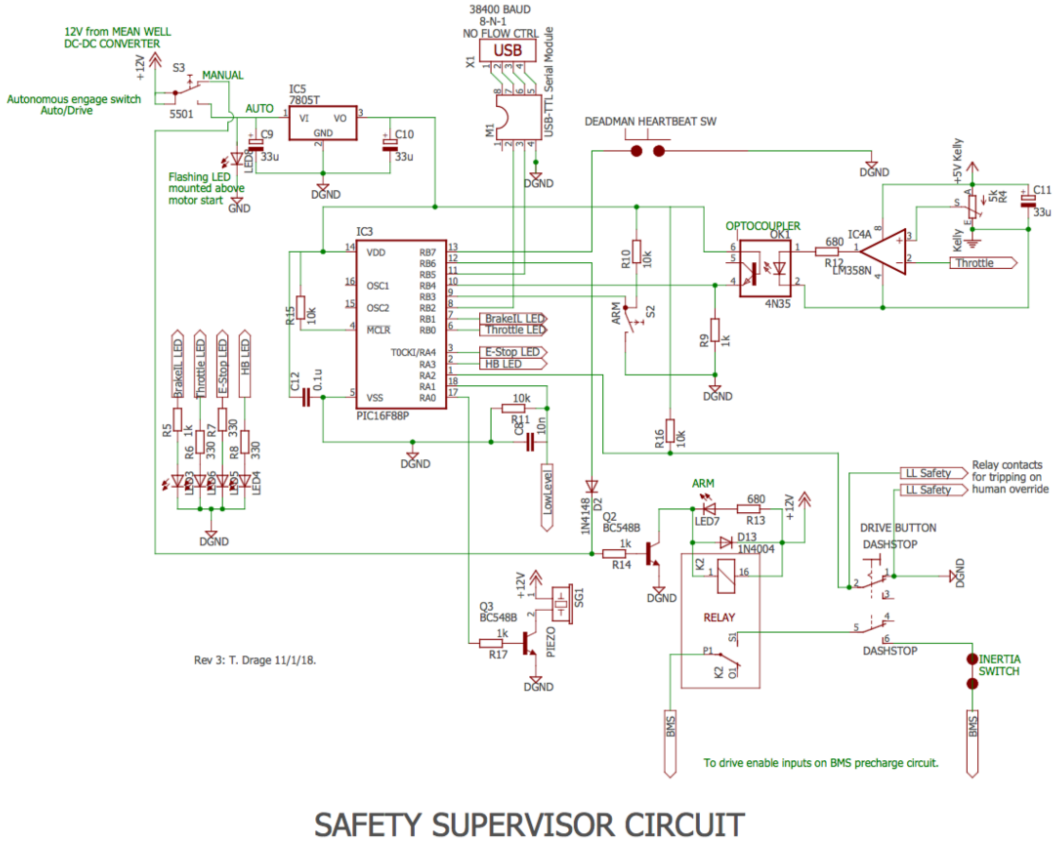


Figure 2 Previous safety supervisor schematic

2.2.3 Layout

This part was started after the schematic is completed. All of the components used in the previous step will have their 1:1 model in this stage. Then place them on a virtual board. The placement of the component will be the final appearance of the finished PCB. Therefore, the placement of the component should take into account whether the component needs to be pulled out or inserted frequently, for example, terminal block, USB and ethernet interfaces on the controller. They are arranged at the edge of the PCB. This will help the access of the signal source. In addition, this PCB will be designed to be as small as possible to reduce the space demand on the compact SAE vehicle. At the same time, because Eagle CAD can provide the width of the wires on the PCB, the width is also required to be as large as possible to improve reliability. However, the two requirements are mutually contradictory. The shrinking of the PCB means that the components will get closer and closer, which means that the wires connecting them will gradually approach. A certain gap is required between the wires, otherwise, they will interfere with each other. After considering the system will be installed in a closure box on the small platform in front of the dashboard. The design team finally decided to meet the requirement to minimize the size first. If the size is too large, it will affect the driver vision. Unexpectedly, under the requirement of meeting the minimum volume. The width of the wire can be set to a maximum of 20 mils (approximately 0.5 mm) with a slight modification.

2.2.4 Revise

This part is to check whether the choice of components such as resistors and capacitors on the PCB is reasonable; whether the component pins are used correctly; and whether the positive and negative of the components; details inspection and so on. The design team learnt on the experience of the previously designed low-level control PCB, and deliberately focused on the details. For example, the font position on the board should be around the component model and not set under the components. This is convenient for installation and future inspection. Lastly, the screw holes are added for the installation to the closure box.

2.3. Results and design discussion

After completing the schematic and layout, the PCB model was sent to the factory for manufacturing. The size of the PCB is 174*163mm (see figure.3). In this section, the constraints imposed on the design, development of the design concept, selection and specification of components will be discussed.

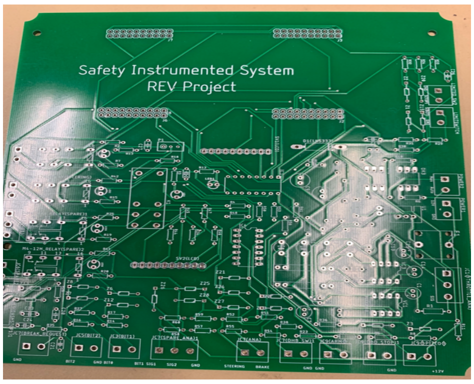


Figure 3 The actual PCB

2.3.1 New controller introduction

The new controller, Texas Instrument Hercules Launchpad (LAUNCHXL2-570LC43), is introduced into the new safety system. It is specifically designed for automotive and transportation applications, which can improve reliability and make safety system meet industry standard (ISO26262 & IEC61508) [12]. The launchpad has several connectivity options such as ethernet socket, USB and 40 ways pin, and there are additional 40 ways standard BoosterPack headers which have been used in our design. This launchpad is pre-programmed with a Hercules safety MCU demo and their debug tools, HALCoGen and CCS, which are available to download on TI website. The debug tools are used in writing the function's code and testing the PCB.

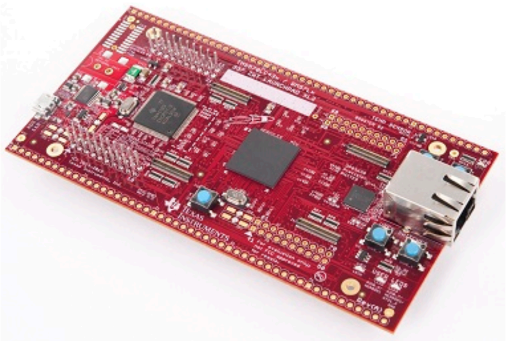


Figure 4 The new controller, Texas Instrument Hercules Launchpad (LAUNCHXL2-570LC43). Available [online]: http://www.ti.com/tool/LAUNCHXL2-570LC43

2.3.2 Analogue circuit introduction

Analogue circuits are introduced into the PCB circuit. Through the analogue circuit, the safety system can detect the analogue signal from the inputs, which is the complex and real-time information [13]. There are two different kinds of analogue circuit designs in the new PCB design. One is a higher cost and more complex design. It consists of two voltage converters, MAX680 [13] and a precision isolation amplifier, ISO124P [14]. This design refers to the low-level control PCB of the previous team design. The MAX680 raises the +5V voltage to ±10V then provide two sets of positive and negative voltages to the ISO124P. This circuit is used to amplify the signal from the throttle and send the amplified signal to the pins on the controller. Then the micro-chip unit on the controller analyses the signal.

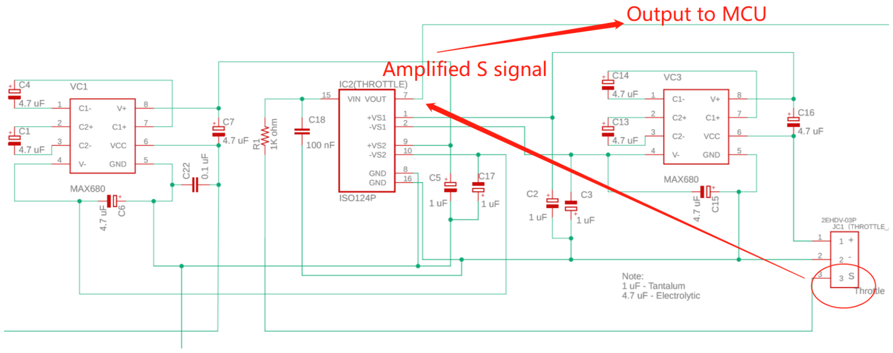


Figure 5 The ISO124P and MAX680 combination analogue circuit.

Another analogue circuit is made up of a combination of diodes and an amplifier. It is used in circuits that accept brake position and steering wheel signals. In addition to the two mentioned above, there are two spare analogue circuits also use this circuit. This kind of circuit is simpler and easier to understand than the previous analogue circuit, and four of the five analogue circuits in this design use this kind due to cost constraints. However, this relatively simple design does not provide stable and reliable performance as the former kind of circuit.

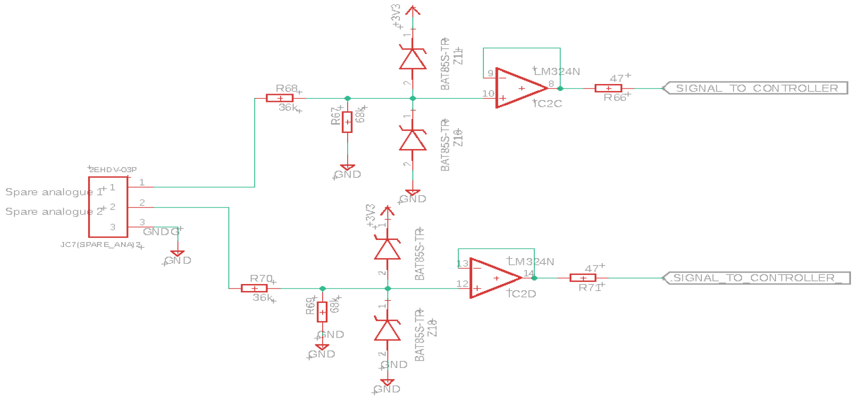


Figure 6 The diodes and amplifier combination analogue circuit

The previous throttle signal is a digital signal transmitted through the optocoupler, so the safety system can only judge whether it is a 5V signal or a 0V signal. The function of the safety system can only be used when there is a signal or no signal. However, after the analogue signal is used, the missing part between 0 to 5V can be detected. The safety system can efficiently capture the current throttle signal, and the team can set more safety functions. For example, when the throttle signal is greater than 2V, once the brake signal is input, the throttle signal is immediately turned off. The analogue circuit increases flexibility. Besides, the previous system occasionally shows errors if there is external interference, but with the analogue circuit, it becomes more reliable.

2.3.3 Digital circuit

Digital circuits have also been introduced into the PCB. The limit switch signal, low-level control signal, and autonomous system E-stop button signal are all input by the digital circuits (see figure 7). This digital circuit introduces a protection mechanism, which will be discussed in section 2.3.4. The purpose of the pull up circuit in a blue frame on the left side is to increase the drive current. Besides, there is another pull up circuit inside of the microcontroller. These pull up circuits can make the microcontroller load smaller (easy to detect the signal).

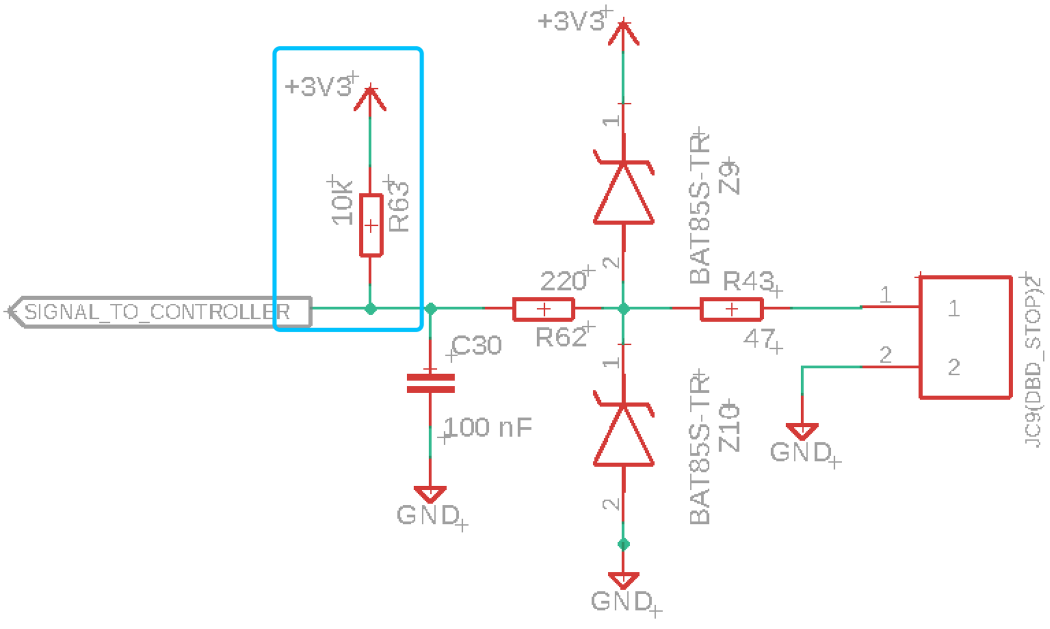


Figure 7 Digital circuit

2.3.4 LCD monitor

The real-time information of the safety system is displayed on an LCD monitor, 1602A [15]. The LCD monitor will be mounted on the dashboard (see section 3.3). The driver can monitor the safety system through the display. Besides, the test team can see which function is triggered or which program is running incorrectly when a fault occurs in the automatic driving mode. The previous low-level safety circuit is not programmable, so there is no message indicating where the error occurred, and in this case, the team needs to guess where the fault occurred and perform manual repairs or adjustments. It is a waste of time and annoying to spend time fixing mistakes in a limited test time each week. With this display, the team can troubleshoot fault faster and increase system flexibility. Besides, the code can be modified effectively after the test drive.

Figure 8 LCD monitor, 1602A, Available [online]: https://au.element14.com/powertip/pc1602aru-hwb-g-q/lcd-module-16x2-x-tmp/dp/1671498?gclid=CjwKCAjwxt_tBRAXEiwAENY8hRSirkcPf5IFN2SZT-9bWo3hgfnr5UTw8U9DuUsC8BDawd1VzUs7gxoC8vgQAvD_BwE&mckv=siVs4My4X_dc|pcrid|380892800521|pkw||pmt||slid||product|1671498|pgrid|76493923343|ptaid|aud-466289539647:pla-336893085108|&CMP=KNC-GOO-SHOPPING-1671498

2.3.5 Components Selection

Since the new PCB is based on the original schematic, we have retained some of the original designs. However, this is a design that has been designed for few years, so the group replaced them with newer models during the design process, for example, changing the voltage converter of the entire low-level system circuit. The original system used the IC57805T and is now replaced with OKI-78SR-5_1.5-W36-C [17]. They both can reduce the 12V from the MEAN WELL voltage to 5V, but the new converter has a wider Operating Temperature, a higher Efficiency and a smaller volume (20*10) and weight (2.1g) [17].

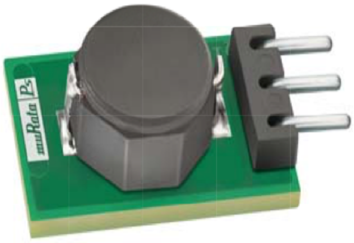


Figure 9 The new converter, OKI-78SR-5_1.5-W36-C

There are five relays on the new PCB. Four of them used the M4-12 [18] relays and the cooperated diodes, which are referred to the relays on the previous low-level control PCB design. Two of the four relays are used to cut off the throttle signal and the steering motor signal, respectively, and the remaining two are spared for future development components. The other relay is K1 50.12.9.012.1000 [19]. It is used to cut off the BMS (battery monitoring system) signal. The rated current of M-12 is 1A, while the rated current of K1 50.12.9.012.1000 can reach 8A. Because the signal comes from the vehicle battery, and its current is larger than the current inside the PCB, so a more powerful relay is needed to control this signal.

Figure 10 BMS relay, K1 50.12.9.012.1000

The diode mentioned in the last paragraph will be used on each relay to filter the excessive current to protect the circuit. However, since the new system PCB has five relays, the repeated components increase the number of components to make the PCB larger. Therefore, the team to simplify the design by replacing them with a transistor, ULN2003, which has 7 sets of NPN type triode inside [20]. After the introduction of this transistor, the original design has also been slightly modified. When a signal from the controller input to the transistor IN1 pin (see figure 11), the triode will turn on. Then the current that drives the relay to work can pass from the turned-on triode to the ground, which means the relay is energized and the switches inside will move to the other side.

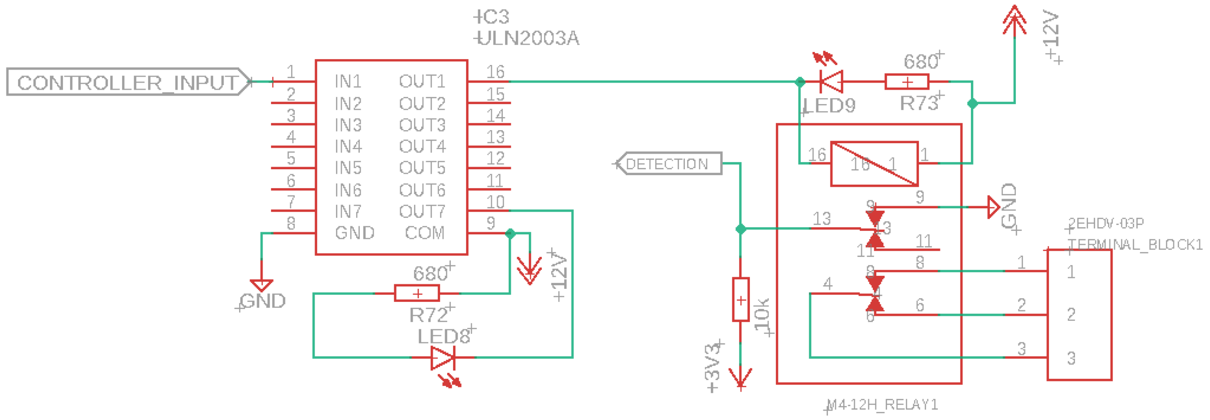


Figure 11 Transistor and relay schematic

Figure 12 ULN2003A transistor. Available [online]: https://au.element14.com/stmicroelectronics/uln2003a/darlington-array-7npn-2003-dip16/dp/1094421?gclid=CjwKCAjwxt_tBRAXEiwAENY8hXJRkpJ_3vn5_6-RDxQ9twNpGxY3bG01R5R4nGO2_Ubo1uAB9mFsCxoC3zQQAvD_BwE&mckv=sATcOprVg_dc|pcrid|97091120688|pkw|uln2003a|pmt|e|slid||product||pgrid|20889687168|ptaid|aud-112905144048:kwd-952225307|&CMP=KNC-GAU-GEN-SKU-G12-STM

The signal cable and PCB are connected using the pluggable terminal blocks, 2EHDV-03P and 2EHDV-02P [21]. One is a 3-head and the other is a 2-head, which were used in different signal sources from the input. The pluggable terminal blocks increase the flexibility of the safety system and also provides protection for vulnerable interfaces.

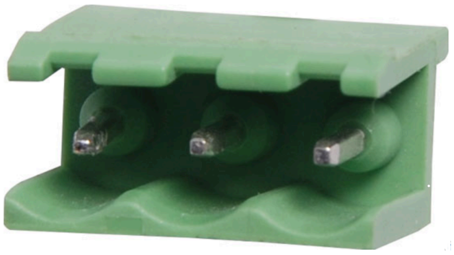


Figure 13 Terminal block. Available [online]: https://www.altronics.com.au/p/p2533-dinkle-3-way-5.08mm-vert-pcb-mount-pluggable-skt/

2.3.6 PCB Protection

Relay detection is added to the system. Since the M4-12 relay has two built-in switches, in addition to the switch that can cut off the signal, the other can also be used to check if the relay is working properly. The principle is that the relay should be working when there is a signal, and both switches will be connected to the upper circuit. At this time, the 3.3v current used as the relay signal will directly connect to the ground, making the connection to the controller short-circuited. If the relay does not work properly, the 3.3v current will not short circuit but connect to the controller. The controller can achieve the detection function.

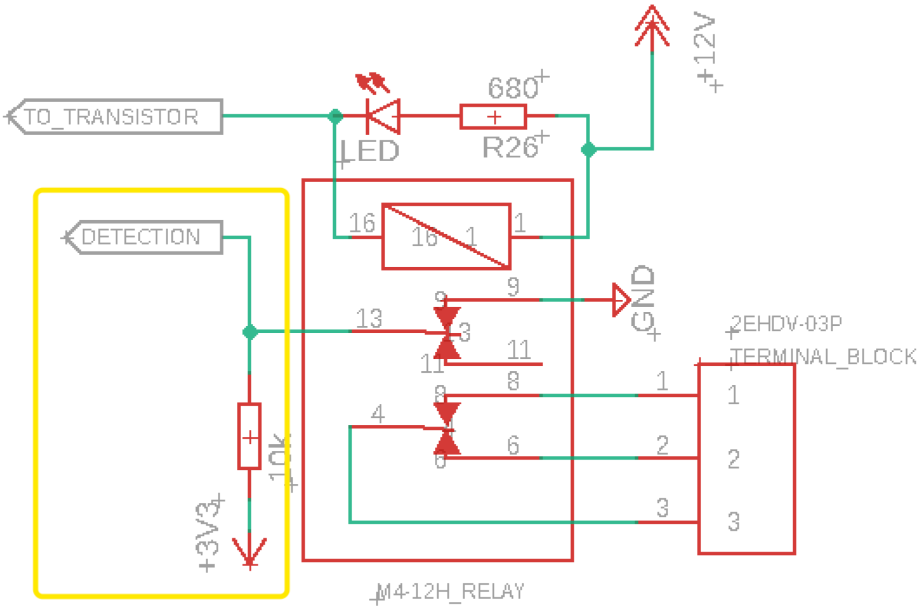


Figure 14 Relay detection schematic

In the digital circuit shown below, the team added two protection designs in the figure below to improve signal stability and protection circuitry. The R62 resistor and C30 capacitor in the yellow box form a low-pass filter. Two diodes in the blue box can filter too high or too low current. This design protects the signal from external environment interference and makes the signal more stable and accurate. The protection design of the two diodes is also used in the protection design of analogue wires.

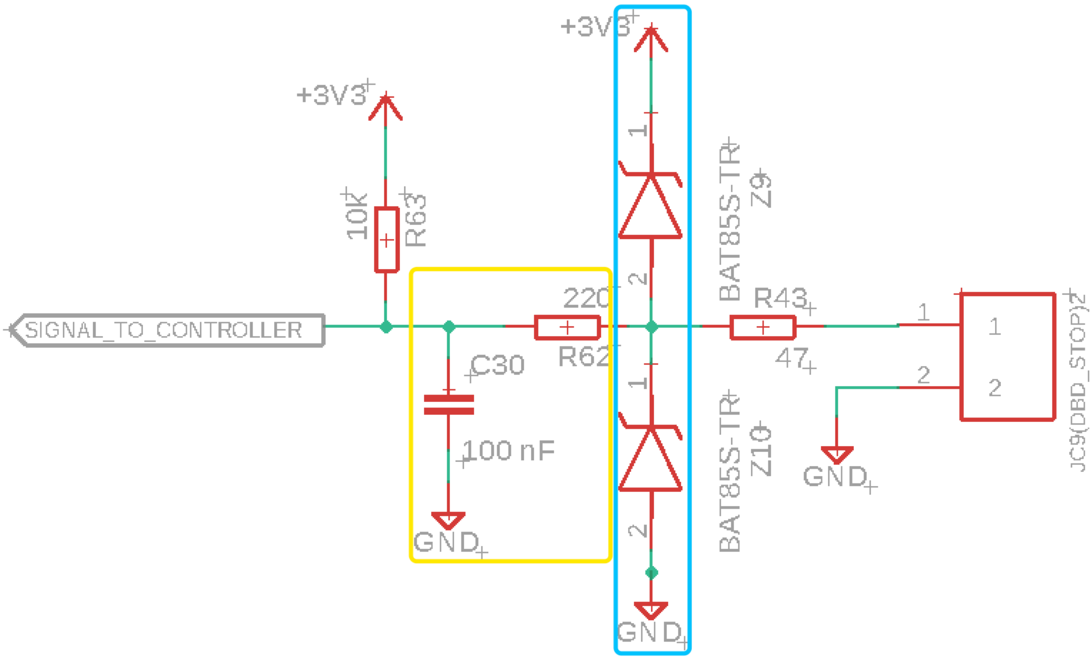


Figure 15 Protection design on digital circuit

The LEDs, Z0004, are mounted next to each important component, such as relays, transistors, converters. They are connected to the power supply of the component to show if the component is working properly. This design makes it easier to troubleshoot and reduce inspection time.

2.4 Components soldering

Components are soldered to the PCB in accordance with industry standards. Since the name of the component is marked on the board, the soldering process is easy to conduct.

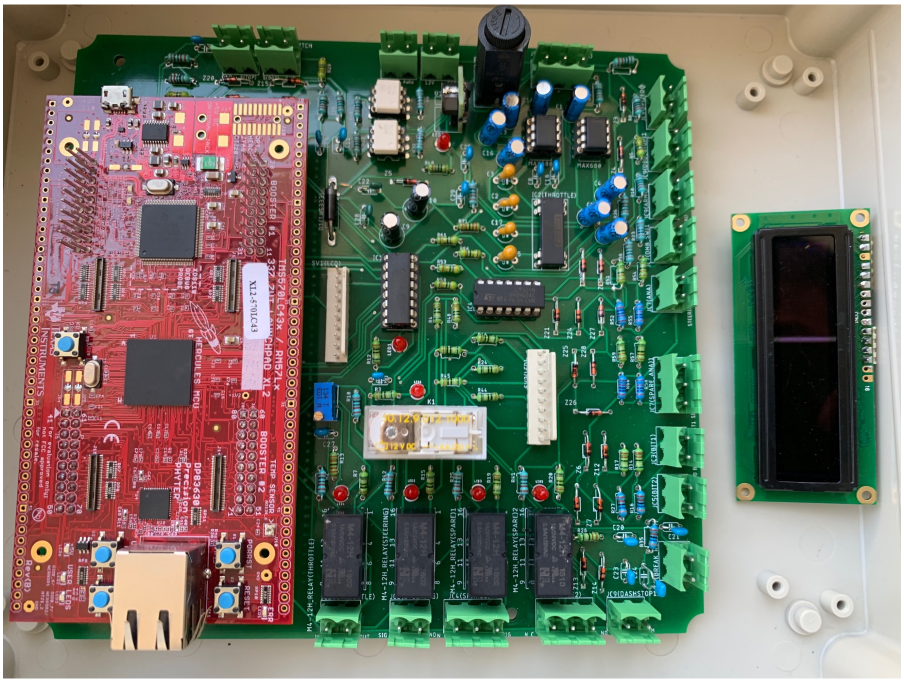


Figure 16 PCB after soldering

However, the team didn't know how to connect the LCD to the PCB at the beginning. With the help and advice of the Electrical workshop, the team used a 10-core cable and used a crimp pin to connect the 10 ways housing to both ends of the cable.

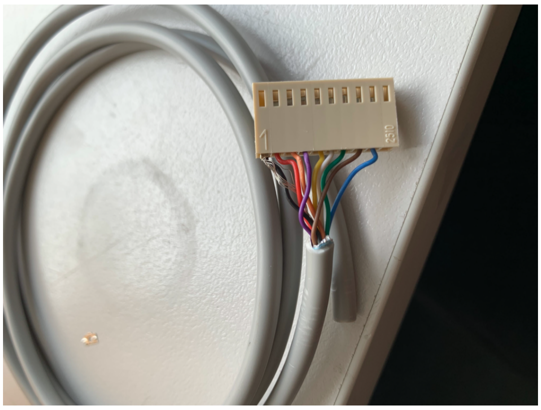


Figure 17 LCD 10-core cable

2.5 components testing

After the soldering was completed, the team used a multimeter to check the circuit diagram. The process was to use one end of the multimeter to contact one pin of the component and the other end to connect the pin of the other component connected to it. After all the pin checks are completed, the team can confirm that all physical connections on the PCB are ready for further development.

3. Dashboard Design

3.1 Overview

The existing dashboard has two parts, and since they are placed vertically and horizontally, they are referred to as "vertical dashboards" and "horizontal dashboards" in the following discussion. These two sections have serval monitors that show the status of the vehicle, and there are various buttons that trigger the safety system. The driver or tester need to run the corresponding start-up program on the touch screen on the left-hand side of the dashboard before triggering the auto-driving mode. Then pull up the two emergency switches and press the ARM button to start the automatic driving mode. The components (touch screen monitor, E-stop button. etc) used in this process already occupy a considerable part of the space on the dashboard. It is difficult to clear space on the original dashboard for new components, such as the LCD display mentioned in the previous section. These two parts of dashboards have some issues and are difficult to improve on the original basis, so the group decided to redesign the entire dashboard with Siemens NX design software. In short, the team needs a bigger, more reliable dashboard, and reducing the buttons on the dashboard to make it look simpler and easier to operate.

3.2 Vertical dashboard design

On the existing dashboard, the speedometer, the current working voltage meter of the low-level system, the motor emergency switch (motor E-stop button), and the battery monitor system (BMS) are arranged from left to right. The steering wheel and alarm buzzer are also installed below the middle of the dashboard. The steering wheel captures most of the space above the vertical dashboard and blocks the components of the under it. The previous design arranged the position of the three displays to be unobstructed so that the driver could read the values on the three displays during driving. The speedometer is mounted on the far left which facilitate the driver to control speed when driving in the UWA’s internal road in manual mode. In addition, this can also help the driver to check if the vehicle is driving at the set speed when driving automatically. The voltage meter of the low-level system is relatively small and mounted in the middle. The BMS is installed at the far right to allow the team to monitor the voltage of battery while charging. However, such an arrangement means that the motor E-stop button must be installed in the shaded area were below the steering wheel. When the driver encounters an emergency, he can quickly stop the vehicle by pressing the motor E-stop to turn off the power of the motor. However, the button is under the steering wheel and it is hard to touch it. This can be a major hazard, so the position of this button needs to be moved to something else that is easy to reach.

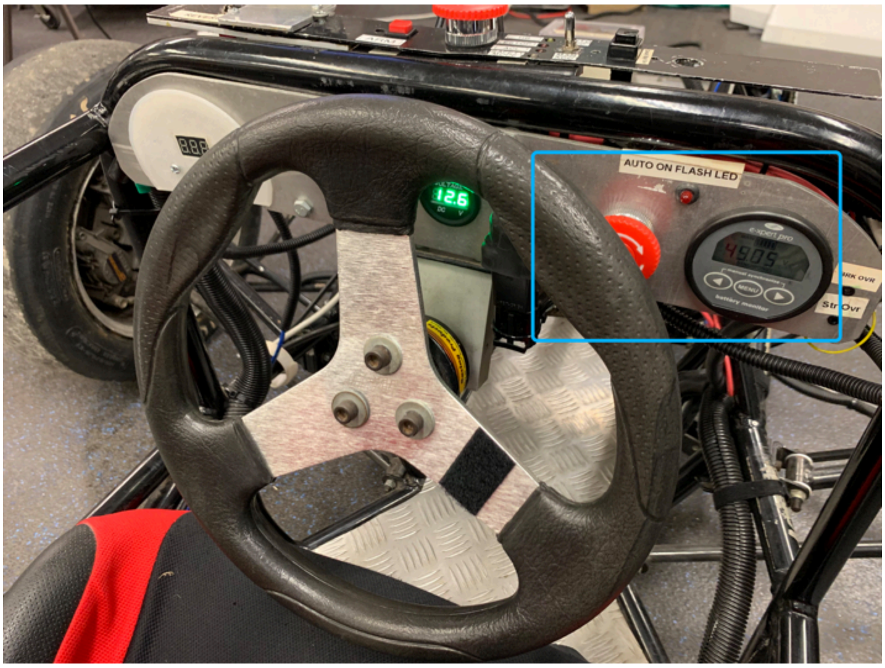


Figure 18 Dashboard overview

Considering the position of the current displays is not clearly defective, the team decided to move the position of the BMS because there are no other two important things in the driving process. Another consideration is that most people are used to use their right hand, so the best solution is to swap the position of the BMS with the position of the motor E-stop button. This emergency button will be on the far right and the easiest to touch.

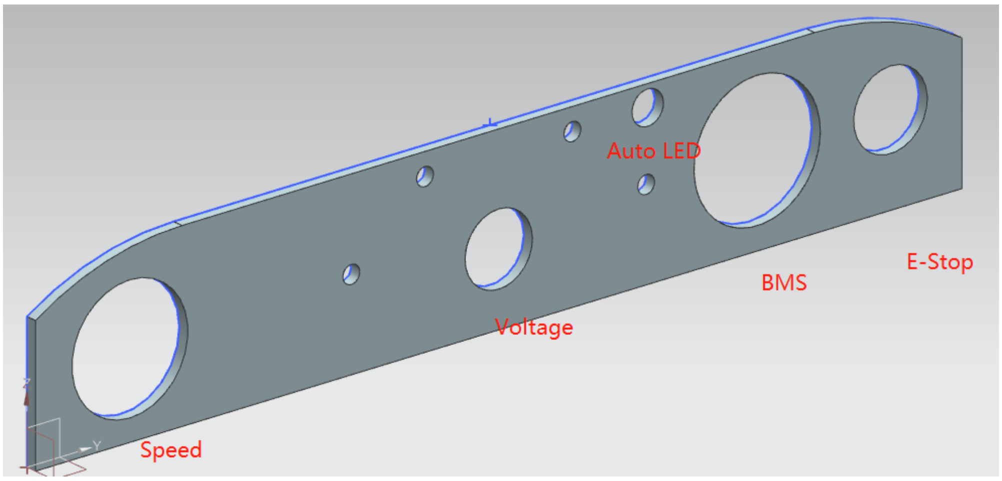


Figure 19 New vertical dashboard model

3.3 Horizontal dashboard design

The horizontal dashboard has various buttons and a touch screen that can be used to control the onboard computer. Due to the excessive number of buttons on the existing dashboard, the new security system removes some of the original designs, for example, the HB LED which shows the heart-beat signal. The current dashboard has two serious pitfalls. One is because the touch screen is fixed vertically on the bracket, and it blocks the driver's vision. The other is that the dashboard does not fully protect the wires that are connected to the dashboard components. The current dashboard is a simple metal sheet with no other underneath protective mechanisms. The wires are covered by the metal sheet at the top, but the other places are exposed. Moreover, the wires are not well fixed and directly supported by the interface with the components.

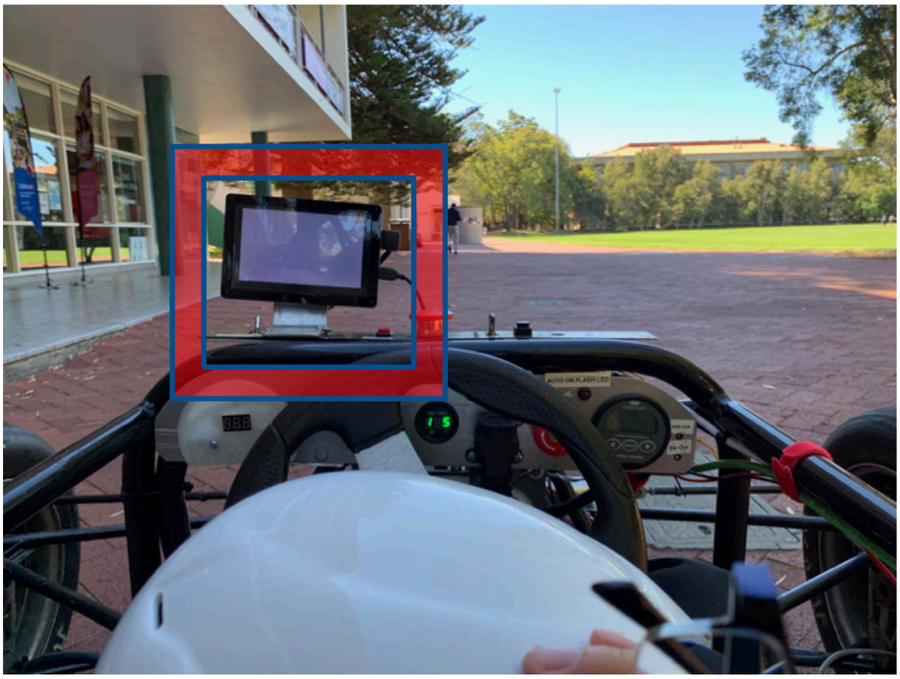


Figure 20 Current driver view

The team initially considered placing the display horizontally so that the driver's vision will be greatly expanded. However, this also means that the driver cannot see the display while sitting in the car. He needs to stand up and check, which is hard to monitor the real-time situation of the vehicle. Besides, the Formula SAE vehicle was designed for the match so that its accessibility is not a focus element. It is generally not easy to get in and out of the car. This simple solution to place the display horizontally needs to be improved. In addition, a better protection structure is needed to protect the wires for reliability. Eventually, the team considered the folded dashboard concept.

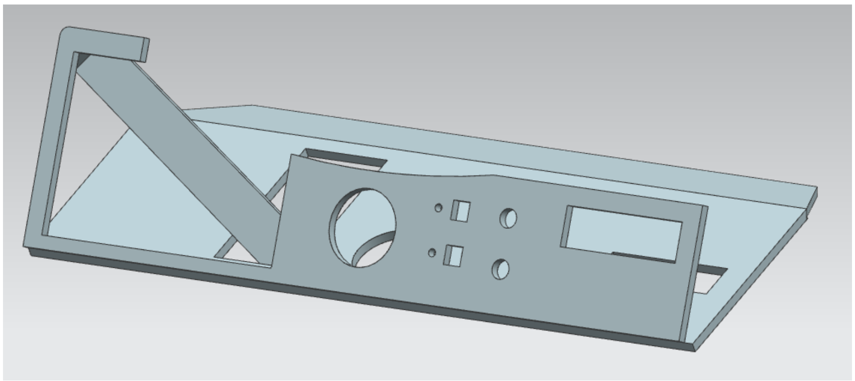


Figure 21 New horizontal dashboard model

This new dashboard is divided into two sections and they are connected by a hinge. The upper part is a component-mounted metal plate with an embedded display mounting area on the left-hand side. This lack-of-corner design is to reduce the size of the board to reduce the impact of blocking the driver vision. On the other hand, it can guarantee the huge socket of the display can be easily mounted to the embedded structure. The emergency stop button of the automatic driving system is installed in the middle of the plate. The area around the E-stop button (round hole) will be emptied as much as possible to avoid interference with the surrounding components in an emergency. There is also a small arc on the top edge of the middle part. It acts to minimize the size of the plate to provide a wider view. The original ARM and DEADMAN button (square holes) were also retained and their signals were sent directly to the new system. On the left hand of the switches are their corresponding indicators, which show if a signal is sent to the safety system when the button is pressed. The reverse button and manual automatic mode switch are also retained. At the far right of the sheet is a new LCD monitor that shows the real-time status of the security system.

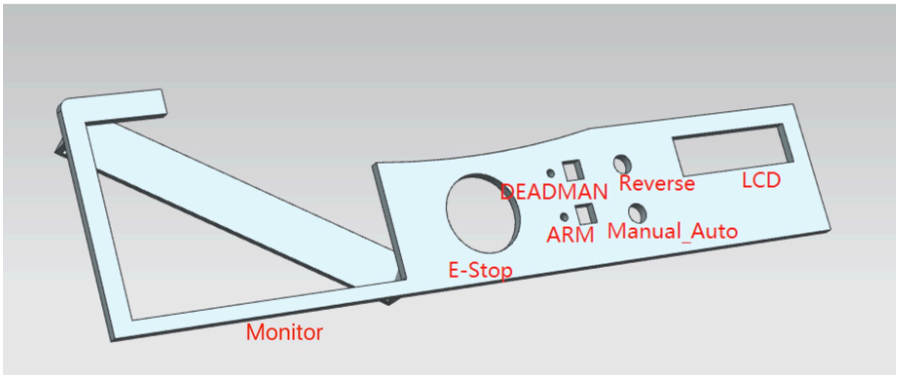


Figure 22 Upper part of the horizontal dashboard

The bottom part of the horizontal dashboard is fixed. The end of the wire which connected to the safety system will be fixed here. Most of the wire will be fixed, and there is only a small portion of the wire required to move freely to connect to the component (the maximum circumference of the upper part when folded, approximately 14 cm). In addition, the team introduced a downwardly sloping edge in the direction of the front of the board. This can be designed to protect the wires from the things flying from the front, such as stones splashed by wheels, rain. This design also reduces the air resistance to a certain extent and is more in line with the automotive design requirements. The team did not specifically perform hydrodynamic simulations for this bottom dashboard because the current vehicle speed was limited to 15 km/h, and improving performance was not the focus of this study. The design mimics the downsizing of modern cars, which will help develop high-performance self-driving cars in the future. The holes on the bottom dashboard correspond with the holes on the top part. The only difference is the rectangular hole on the left. This is a hole reserved specifically for the interface on the right side of the display to facilitate the pass-through of the wires.

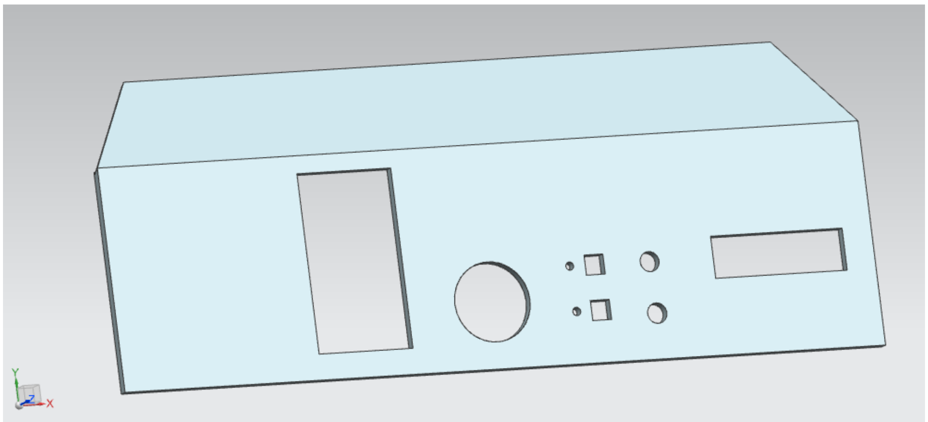


Figure 23 Bottom part of the horizontal dashboard

3.4 Conclusion

The new dashboard has the following improvements and advantages over the previous dashboard: first, the position of the component is more reasonable; the emergency button is placed in an easy-to-touch position with no obstacles around it. Then the removal of the LEDs makes the dashboard look simpler and more straightforward. The new LCD display shows the status of the safety system in real time, allowing the driver to monitor the vehicle more efficiently. The foldable design allows the driver to have a wider view in manual drive and then improve driving safety. Larger dashboard with front lower edge provides better protection to the wires underneath.

Such a dashboard is more compatible with new safety systems and provides better support for increased vehicle safety. These models have been submitted to the UWA mechanical workshop for manufacturing. The vertical dashboard is mounted under the frame so that it needs an accurate dimension. However, due to equipment limitations, the design team was not able to provide very accurate dimensions, and since the previous dashboard was designed long ago, the team was not sure how the dashboard was fixed to the frame. Professional staff and professional tools are, therefore required to determine the final dimensions. The vertical dashboards currently measured by the team are 440mm long and 80mm wide. The horizontal dashboard is a little shorter than 440mm; the widest dashboard is 130mm. The final size will be close to this size. The material of the new dashboard is 2mm thick aluminium alloy, but the final product will be determined according to what materials owned by the workshop, which may vary in thickness, but will be greater than 2mm to ensure sufficient strength.

4. Other Contributions

4.1 Limit switch installation

In order to improve the safety of the vehicle, the design team also installed two limit switches (s2722). These two limit switches are mounted behind the brake pedal, and when the driver steps on the brake pedal, the pedal contacts and presses the switch. Once the switch is pressed, its internal switches will connect and transport a signal to the safety system. When the safety system receives the signal, it will judge that the driver has stepped on the brake pedal and then suspend the automatic driving mode. Since the limit switches need to be attached to the brake mechanism, this means they need to be installed in the front of the vehicle where the brake mechanism is located. There are various wires and sensors and motors at the front of the vehicle. The space available in this area is very limited. Since the distance between the various components could not be accurately measured, the team originally designed an adjustable bracket. After the bracket and limit switches are mounted on the vehicle, the bracket can adjust to the most suitable angle and height. Then a fixed bracket is made according to the shape. The original design was using 3D printing to print three rectangular blocks with adjustable holes in the middle. There were two support feet, and the remaining one is the top part to support the limit switches. The figure below shows the original design.

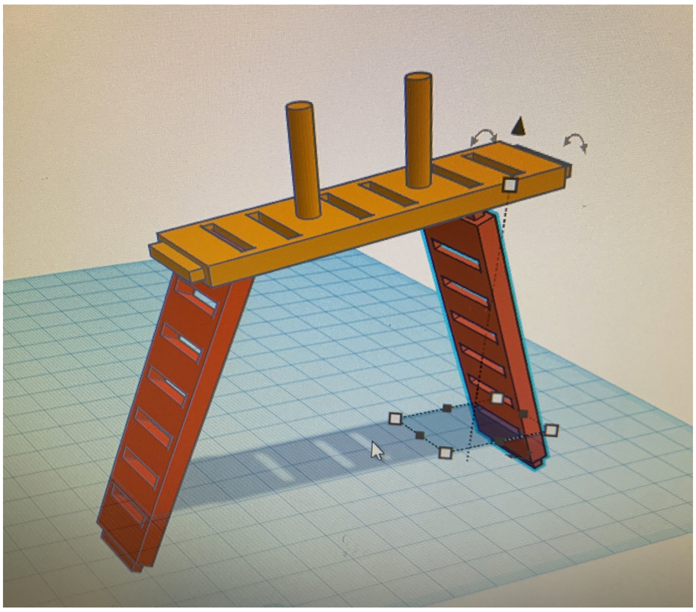


Figure 24 Original limit switch bracket

However, during the model testing, this structure is not stable enough because the support feet are too thin. Moreover, due to the bending moment of the structure after the limit switches are pressed, the bracket does not have a corresponding anti-torque structure, and the long-term use will cause the bracket to bend. The team modified the structure with the help of professionals at the mechanical workshop. They suggested that the structure be designed to be as simple as possible and easy to manufacture. Based on the existing materials of the workshop, the final design uses hollow square steel and cuts it from the middle to form a "C" shape. This structure can stably support the limit switch and effectively withstand the bending moment. Two bolts are used to fix the limit switches to the bracket, and a round shape extension part is added to the brake pedal.

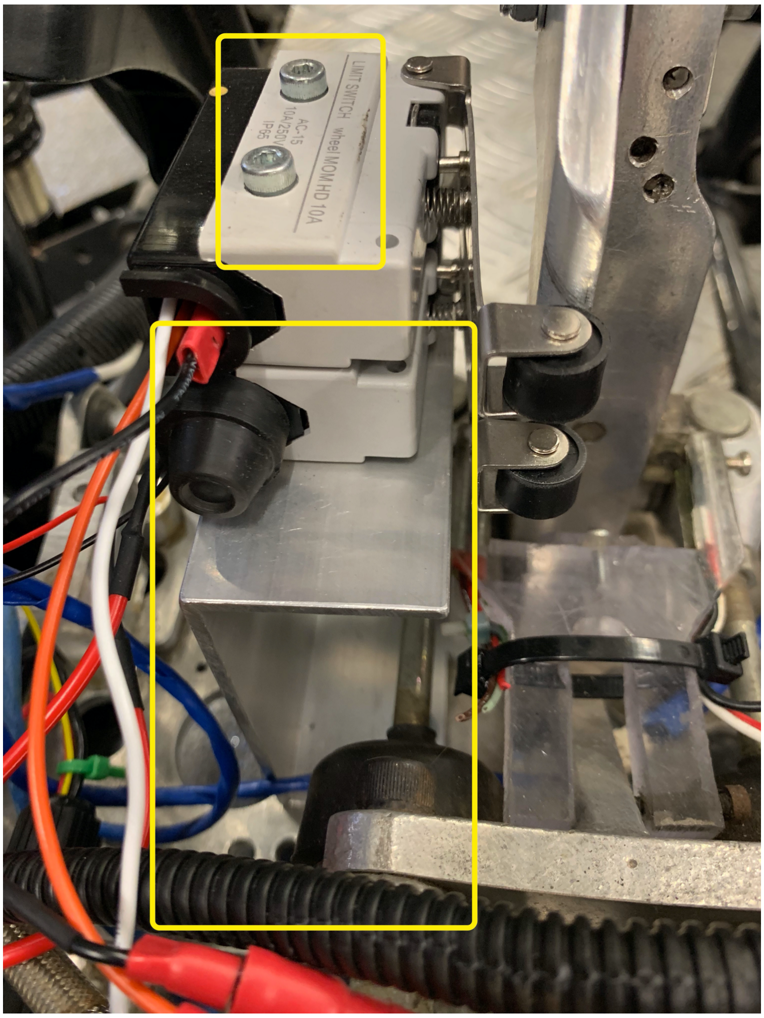


Figure 25 Final limit switch design

4.2 Conduits installation

At the beginning of this research project, most of the wires on the vehicle were bare. These wires are mainly located in the low-level control part of the front of the vehicle, the 48V to 12V converter under the seat, and the on-board computer wiring port. These exposed wires not only affect the appearance of the vehicle, but also add to the safety hazards of the car. In a vehicle demo, the professional advised the team to organize these messy exposed wires to ensure safety. In particular, the bare hydraulic brake pipe is installed under the steering frame. This place is easily scratched by sharp objects. Once the pipe broke, the liquid in the pipe will flow out of the hydraulic system, causing the malfunction of the brake. So, the team added a conduit to these bare lines, and the final result is shown below.

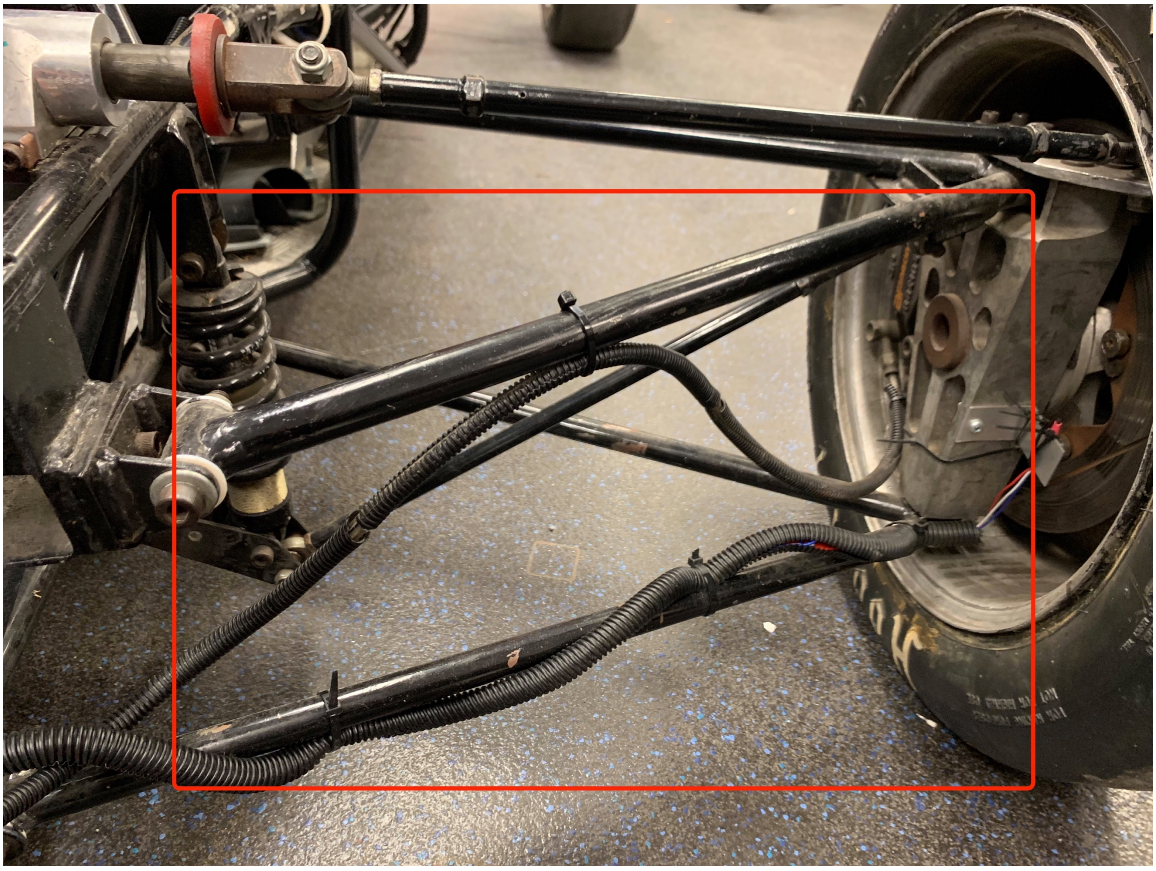


Figure 26 The hydraulic brake pipe with conduit

5. Conclusion and future development

This project shows a significant promise to achieve the REV team final goal by increasing safety. The hardware portion of the PCB of the new security system has been completed and checked. They provide more reliable components for the system to achieve more functions to ensure safe driving. The new dashboard models have been submitted to the UWA mechanical workshop and will be completed in the near future. The SAE vehicle with new dashboards provide a wider view and emergency buttons that are easier to touch. These advantages can improve vehicle safety and provide reliable hardware assistance to achieve the final goal.

Due to time constraints, the security function code of the security system has not been completed. These codes are based on the C language and require the use of the HalCoGen to set up the controller's pinout and CCS for logic control to perform new functions on the controller. The old safety supervisor code is also written in C, and some of them can be used for new code. After programming is complete, the team needs members who are not involved in the design of the safety system to thoroughly check whether the safety system can perform all of the intended functions on the vehicle. With the help of the new system, it is foreseeable in the near future that the car can achieve its final goal more safely and reliably.

6. Reference

[1] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transport Reviews,* vol. 39, no. 1, pp. 103-128, 2019.

[2] V. A. Banks, K. L. Plant and N. A. Stanton, "Driver error or designer error: Using the Perceptual Cycle Model to explore the circumstances surrounding the fatal Tesla crash on 7th May 2016," *Safety Science,* vol. 108, pp. 278-285, 2018.

[3] S. Singh, "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey," NHTSA's National Center for Statistics and Analysis , Washington DC, 2015.

[4] D. M. West, "Moving forward: Self-driving vehicles in China, Europe, Japan, Korea, and the United States," Center for Technology Innovation at BROOKINGS, September 2016.

[5] T. R. Project, "Autonomous BMW," The university of western Australia, 2019. [Online]. Available: http://therevproject.com/vehicles/bmw.php. [Accessed 30 October 2019].

[6] T. R. Project, "Electric Hub Motor SAE Race car," The university of western Australia, [Online]. Available: http://therevproject.com/vehicles/sae-electric.php. [Accessed 30 10 2019].

[7] T. H. Drage , "Development of a Navigation Control System for an Autonomous Formula SAE-Electric Race Car," Perth, 2013.

[8] J. Kalinowski, "Conversion of a Formula SAE Vehicle to Full Drive-by-Wire Capability," Perth, 2013.

[9] T. R. team, "SAEAuto Engineering Manual," The REV team, [Online]. Available: https://github.com/braunl/SAEAuto/wiki . [Accessed 30 October 2019].

[10] W. L. W. Lai, "Autonomous Driving with Dynamic Path Planning," The REV team, [Online]. Available: http://robotics.ee.uwa.edu.au/theses/2018-REV-PathPlanning-Lai.pdf. [Accessed 30 10 2019].

[11] W. L. W. Lai, “Check list for safety tripping version 1.2,” The university of western Australia, Perth, 2018.

[12] T. Instruments, “Hercules TMS570LC43x LaunchPad Development Kit,” Texas Instruments, [Online]. Available: http://www.ti.com/tool/LAUNCHXL2-570LC43. [Accessed 30 October 2019].

[13] S. ABC, “ What’s The Difference Between Analog And Digital Circuits?,” 2019. [Online]. Available: https://www.scienceabc.com/innovation/whats-the-difference-between-analog-and-digital-circuits.html. [Accessed 30 October 2019].

[14] I. Maxim Integrated Products, “MAX680/MAX681 datasheet,” Maxim Integrated Products, Inc, 2019. [Online]. Available: https://datasheets.maximintegrated.com/en/ds/MAX680-MAX681.pdf. [Accessed 30 October 2019].

[15] T. Instruments, “ISO124 ±10-V Input, Precision Isolation Amplifier datasheet,” Texas Instruments Incorporated, 2018. [Online]. Available: http://www.ti.com/lit/ds/symlink/iso124.pdf. [Accessed 30 October 2019].

[16] P. T. CORP, “Incorporated,” Powertip Tech CORP, [Online]. Available: http://www.farnell.com/datasheets/40247.pdf?_ga=2.17453497.1899947761.1572361752-1748841153.1563626560&_gac=1.186345051.1572395090.CjwKCAjwxt_tBRAXEiwAENY8hRSirkcPf5IFN2SZT-9bWo3hgfnr5UTw8U9DuUsC8BDawd1VzUs7gxoC8vgQAvD_BwE. [Accessed 30 October 2019].

[17] M. Ps, “OKI-78SR Series datasheet,” Murata Power Solutions, Inc. , [Online]. Available: https://www.tme.eu/Document/e2b8dc7cfb11c9b787f619dbf3fde2f5/oki-78sr.pdf. [Accessed 30 October 2019].

[18] “M4 Forward Relays,” Ningbo Forward Relay Corporation LTD., [Online]. Available: http://ultran.ru/sites/default/files/catalog/svetodiody/brend/datasheets/m4.pdf. [Accessed 30 October 2019].

[19] “50 SERIES Forcibly guided contacts relay 8 A,” Finder, [Online]. Available: http://www.farnell.com/datasheets/2237920.pdf?_ga=2.23288122.1899947761.1572361752-1748841153.1563626560&_gac=1.121391610.1572395090.CjwKCAjwxt_tBRAXEi

wAENY8hRSirkcPf5IFN2SZT-9bWo3hgfnr5UTw8U9DuUsC8BDawd1VzUs7gxoC8vgQAvD_BwE. [Accessed 30 October 2019].

[20] "ULN2003 Datasheet − production data," STMicroelectronics group of companies, [Online]. Available: http://www.farnell.com/datasheets/1690348.pdf?_ga=2.256465547.1899947761.1572361752-1748841153.1563626560&_gac=1.225141480.1572361752.CjwKCAjwxt_tBRAXEiwAENY8hX8tO1oHwQObqqz1oUqD759L93WNGdPtSwj2KYkjOd4gZKGl1BZfVxoClUYQAvD_BwE. [Accessed 30 October 2019].

[21] "Headers(Sockets) for pluggable terminal blocks ／ ECH & EHD series," Dinkle enterprise, [Online]. Available: https://download.altronics.com.au/files/datasheets_P2542.pdf. [Accessed 30 October 2019].

Appendix A: Function list

Function number	IF	WHEN	THEN	WHY	HOW
1	Steering motor over current	Safety supervisor is armed	Low Level Safety circuit causes a trip of the safety supervisor, by wiring the relay contacts in series with the safety supervisors e-stop feedback	Stop autonomous driving if human has taken over	Safety Supervisor
2	Steering motor over current	Autonomous system powered	- Steering motor is disconnected -Indicator of excess steering force light	Allow human to take over steering if interference detected. Protect mechanical system from over-torque.	Low Level Safety Circuit
3	Heartbeat stop remote is pressed	Safety supervisor is armed	- Trip signal sent to high level controller (Jetson) which stops autonomous driving and relays trip to safety	Bystander initiates emergency stop (e.g. car out of control or environmental hazard)	Remote Stop -> High Level Controller -> Safety Supervisor

			supervisor - Motor disconnected via e-stop loop - Heartbeat transmission stops		
4	Lost heartbeat (no change of state for a certain time)	Safety supervisor is armed	- Blinks on and off at normal state but stays on - Safety supervisor detects heartbeat timeout and trips (disconnect motor via e-stop loop)	Signal from remote emergency stop lost (fail safe) or high level controller (Jetson/ROS) frozen.	Safety Supervisor
4	Lost heartbeat (no change of state for a certain time)	Autonomous driving in progress	- High level control program stops autonomous driving (zero throttle) - Trip sent to safety supervisor	Signal from remote emergency stop lost (fail safe) or high level controller (Jetson/ROS) frozen.	High Level Controller
5	Throttle voltage error (throttle above zero threshold)	-No power on traction motor controllers -A positive	- LED on top dash blink- ACL - Apply the brake via a hard-wired signal to the low	The car could unexpectedly take off - warning to operator.	Safety Supervisor

		throttle signal after enabling the motor controllers	level controller - Arming sequence resets and motor power disconnected via e-stop loop.		
6	Dash E-STOP pressed (If HBT and ACL don’t also light then it either came from the dash e-stop, low level safety box or was commanded by the high level controller.)	Safety system is armed	- Estop loop disconnects the motor controllers - ESTOP lights on all trips - Apply the brake via a hard-wired signal to the low level controller	Allow human stop the car	Hard wired
7	Extreme steering occur (Steering sensor out of bounds [ER6])	Autonomous driving is in progress	Initiate the trip by signal to high level controller (Jetson)	Protect the steering system	Low Level Controller
	Abnormal brake action occur, brake moves without servo command (e.g. human tries to	Safety supervisor is armed	Low Level Safety circuit causes a trip of the safety supervisor, by wiring the relay contacts in series with the safety	Stop autonomous driving if human has taken over	Safety Supervisor

	press brake during driving)		supervisors e-stop feedback		
8	Abnormal brake action occur, brake moves without servo command (e.g. human tries to press brake during driving)	Autonomous system powered	- LED on front dash blinks – BRK Over - Throttle signal set to zero (by relay in Low Level Safety circuit) - Control of steering motor returned to driver (relay disconnect)	Person has pressed brake or brake fault (unknown to operator)	Low Level Safety Circuit -> Safety Supervisor
9	No new speed command received in 100ms by high level system when demo program running	Autonomous system is on	Reset speed to zero	In case demo program crashes	High level controller
10	The low level controller fails due to main loop freeze	Always	Reset the controller	Reset to normal state	Low-level controller WDT [ER2]
11	If anything is abnormal to the heartbeat	Periodically	check the HB battery level, warning/error will be print to screen.	Ensure HB system run well	HB battery level check in High Level Controller

12	No new command in 300 ms [ER5]	Always	SAE will trip as Jetson is not responding		Low Level Controller -> High Level Controller
13	Connection to safety serial port is failed	Autonomous system is on	Control program will exit		High Level Controller
14	Trip signal sent from high level controller	Autonomous driving is in progress	- Disconnect drive power in trip condition - If not reset, re-trip high level controller		Safety Supervisor

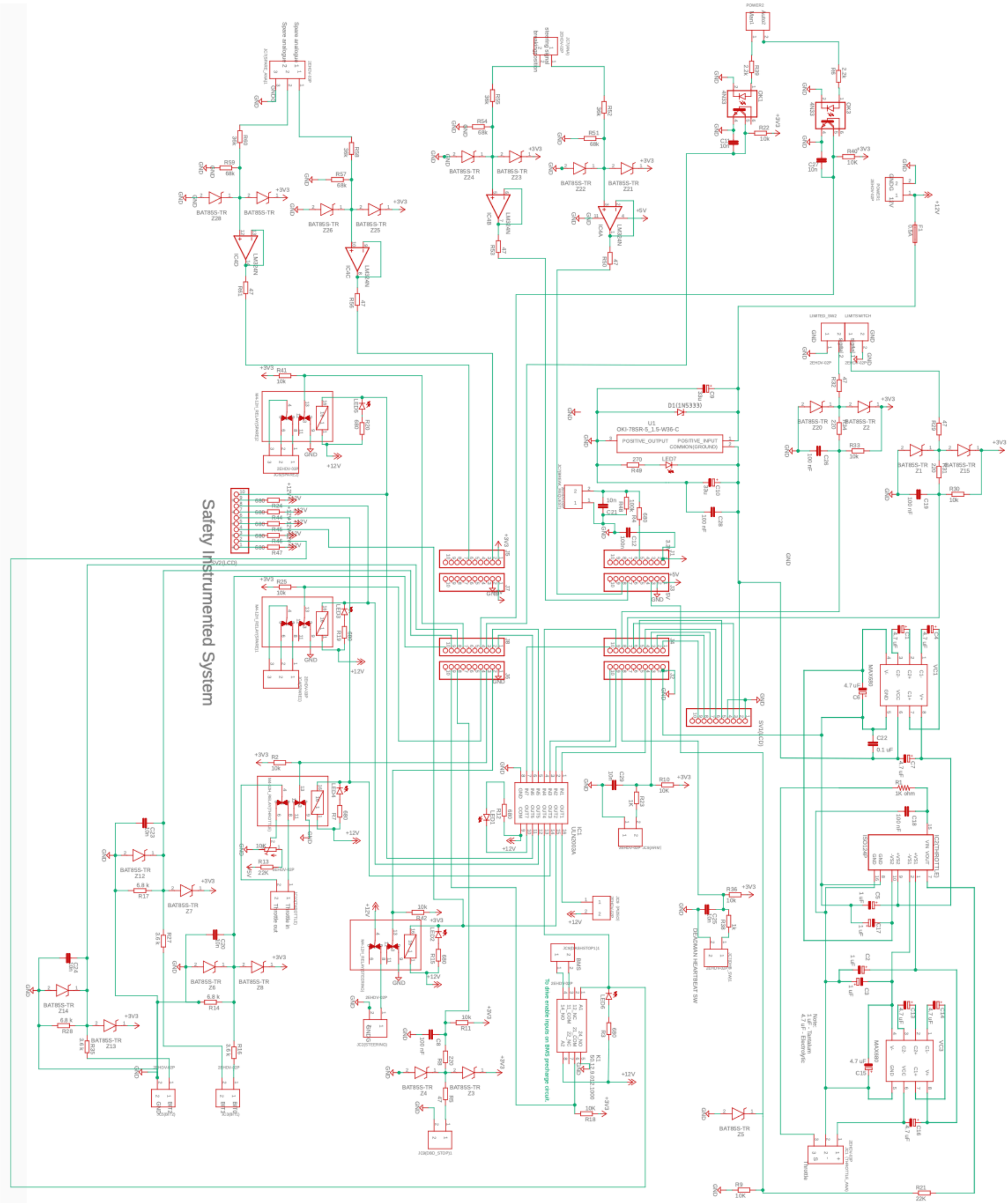
Appendix B: PCB part list

Summary			total number:	
capacitor:	4.7 uf		8	**R5048**
	1 uf		4	R2628A
	100 nf/0.1 uf		7	**R2930A**
	33 uf		2	R4797
	10 nf		8	**R2910A**
Fuse	0.5A	F456	F456	
box			1	H0363
terminal block:	2EHDV-03P		4	P2533
	2EHDV-02P		15	P2532

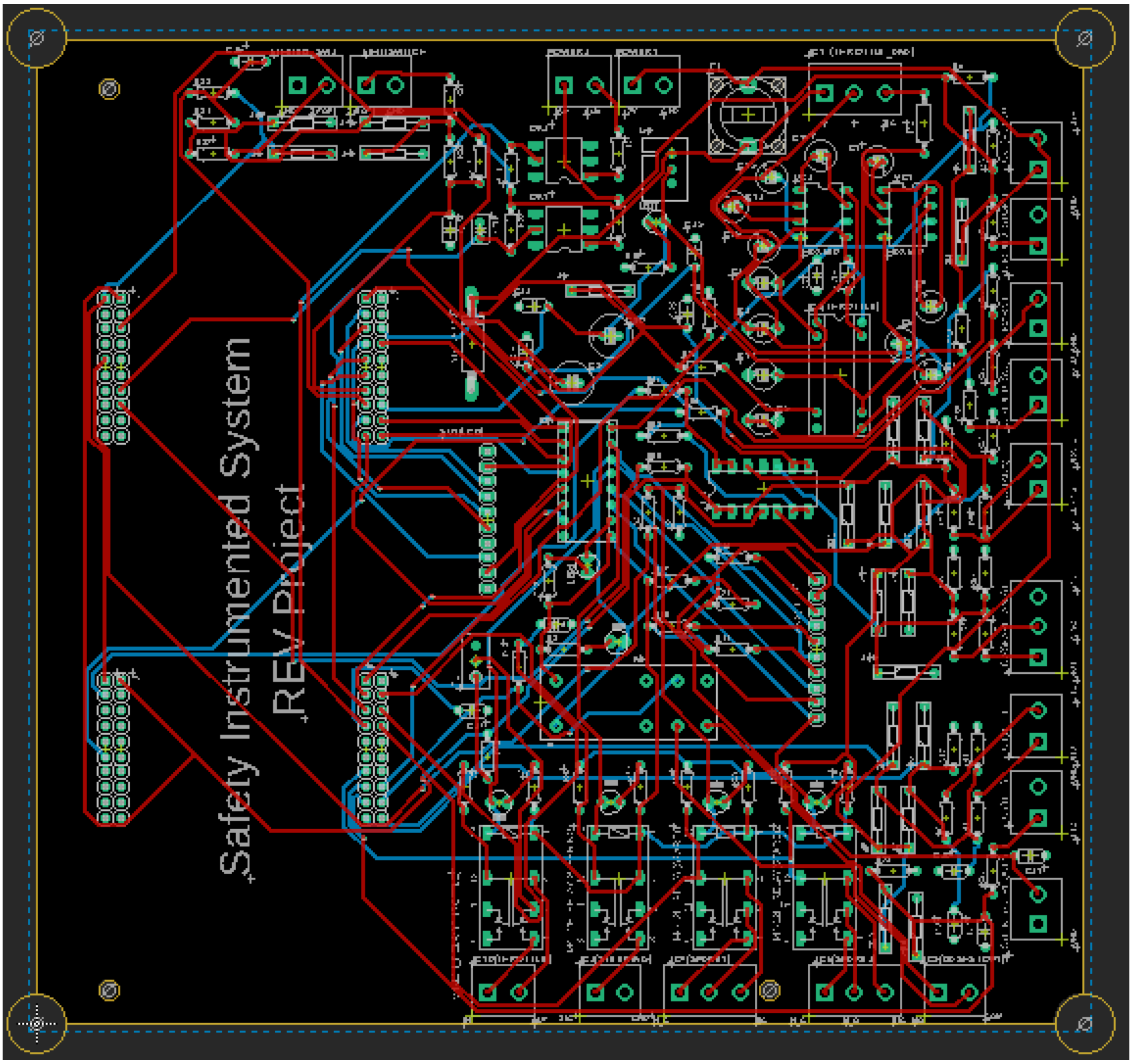
Relay:	K1 50.12.9.012.1000		1	
	M4-12H		4	S4150
COUPLER:	4N33		2	Z1646
LED			7	Z0004
Resistor:				
	1K		3	R7758 • 1k 0.6W 1% Metal Film Resistor PK 10
	10K		13	R7782 • 10k 0.6W 1% Metal Film Resistor PK 10
	680 ohm		12	R7754 • 680R 0.6W 1% Metal Film PK 10
	36K		4	506-5406
	47 ohm		7	R7726 • 47R 0.6W 1% Metal Film Resistor PK 10
	220 ohm		3	R7742 • 220R 0.6W 1% Metal Film Resistor PK 10
	68K		4	R7802 • 68k 0.6W 1% Metal Film Resistor PK 10
	3.6K		3	148-635
	6.8K		3	R7778 • 6k8 0.6W 1% Metal Film Resistor PK 10
	2.2K		2	R7766 • 2k2 0.6W 1% Metal Film Resistor PK 10
	100K		1	R7806 • 100k 0.6W 1% Metal Film Resistor PK 10
	10K POT		1	R2382A
	22K		2	R7790 • 22k 0.6W 1% Metal Film Resistor PK 10
	270		1	R7744 • 270R 0.6W 1% Metal Film Resistor PK 10
Diode:	1N5355		1	Z0418
	BAT85s		21	Z0044
	MAX 680		2	
LCD connector	LCD		2	P5500
Transistor:	ULN2003A		1	Z3000

Amplifier:	ISO124P		1	
	LM324N		1	Z2524
Converter:	OKI-78SR-5_1.5-W36-C		1	
Relay:	K1 50.12.9.012.1000		1	
Fuse			1	S5986
COUPLER:	4N33		2	Z1646

Appendix C : PCB schematic



Appendix D : PCB layout



Appendix E: Limit switch bracket