The University of Western Australia

School of Electrical, Electronic and Computer Engineering

Final Year Research Project Thesis

Autonomous SAE Car

Safety System Redesign with New Microcontroller and Electrical Circuit

Yi Zhang

22543809

Word count:6842

Supervised by Professor Dr.

Thomas Bräunl

Table of Contents

List of Figures

List of Tables

Abstract

Designing a reliable electrical safety system for autonomous driving vehicles is critical in providing safe operations for passengers as well as protecting the internal components of the vehicle. Autonomous driving is a complex engineering project. A vehicle that reaches the L4 level of autonomous driving requires the support of hardware technology, involving system engineering. In addition to excellent software systems, it is necessary to consider the requirements and challenges of the hardware device's mechanical and electronic parts. Additionally, the electrical connections across the systems and installations in the vehicle must reach the ISO26262 standards of electronic, electrical and programmable devices.

In exploring safety system hardware, this paper is a "design and build" project focusing on the development of the safety system of a SAE car. The major works are as follows:

1. A printed circuit board (PCB) designed as independent hardware, the selection of electronic components, installation and test process.
2. A comparison between the new schematic and previous one.
3. A Launchpad TMS570LC43x from Texas Instruments, which will be introduced as the controller of the safety system with a code generation tool (HALCoGen) and a compiler (Code Composer Studio).
4. As a result, the new safety functions code is obtained which was converted from previous one.
5. In order to increase the reliability and operability, a new dashboard design process is demonstrated. Future development is considered during the process.

Nomenclature

SAE	Society of Automotive Engineers
IO	Input/output
RAM	Random Access Memory
UART	Universal Asynchronous Receiver/Transmitter
ECU	Electronic control unit
ASILs	Automotive safety integrity levels
MCU	Microcontroller unit
ECC	Error-Correcting Code memory
TCM	Tightly coupled memories
DCL S	Dual core lockstep
SCU	Snoop control unit
PCB	Printed Circuit Board
LCD	Liquid Crystal Display

1. Introduction

1.1 Motivation

The Driverless car is an advanced and popular project in the engineering field. It can potentially reduce road accidents that are caused by human driver intervention as well as increasing safety by eliminating aggressive driving behavior. Many companies, including General Motors, BMW, Toyota and Tesla, have invested funds and resources into research and development activities in the Driverless car industry. Autonomous driving can provide many potential benefits. Theoretically, traffic collisions caused by human error as a result of driving while intoxicated, poor judgement and road rage can be eliminated by autonomous driving. Alternatively, autonomous driving can free the driver from steering, allowing those who do not know how to drive to use their car independently. Also, autonomous driving can save the cost of hiring a driver. Although this will result in the loss of jobs of paid drivers, the industry will make more profits by autonomous driving and will provide new jobs.

Figure 1:Tesla Mode S [1]

Though autonomous driving is a new trend in the automotive industry, it still needs improvement. An accident led to the death of Joshua Brown, whose 2015 Model S traveled 74 miles per hour when colliding with a tractor trailer that turned left and was crossing the highway [2]. Autopilot radar and camera cannot recognize white trucks in amongst a bright sky. Hence, people are still worried about the reliability of Driverless cars.

The motivations of autonomous driving are listed as follows:

- Reduce road traffic accidents that mainly involve human error, such as fatigue and drunk driving.

- Save people time from driving.
- Reduce traffic congestion.
- Significantly reduce greenhouse gas emissions.

1.2 Background

Autonomous driving is an undergoing project of the Renewable Energy Vehicle (REV) team at The University of Western Australia (UWA), led by Professor Thomas Bräunl. At first, the Renewable Energy Vehicle (REV) project modified a BMW X5 by implementing a driver assistant system, which helps the driver to avoid objects in its path [3]. Then the team developed a formula SAE (Society of Automotive Engineers)-electric vehicle as a testbed of the autonomous vehicle study. The formula SAE vehicle was created by UWA Motorsport and converted to the electric car in 2010 and the complete drive by wire system was implemented by previous team members [4]. The main functions that need to be built for autonomous driving are localization, path planning, mapping, collision-free driving, and object detection. To satisfy data demand for these functions, formula SAE car has been equipped with odometry sensors, Inertial Measurement Unit (IMU), Global Positioning System (GPS), Light Detection and Ranging (Lidar) and cameras. Nvidia Jetson TX1 was installed on the car as a processor and will be upgraded to Nvidia Jetson AGX. In order to increase the redundancy of the SAE safety system， a hardware safety system was created and can monitor human inputs, control systems, and performs actions according to trip initiator.

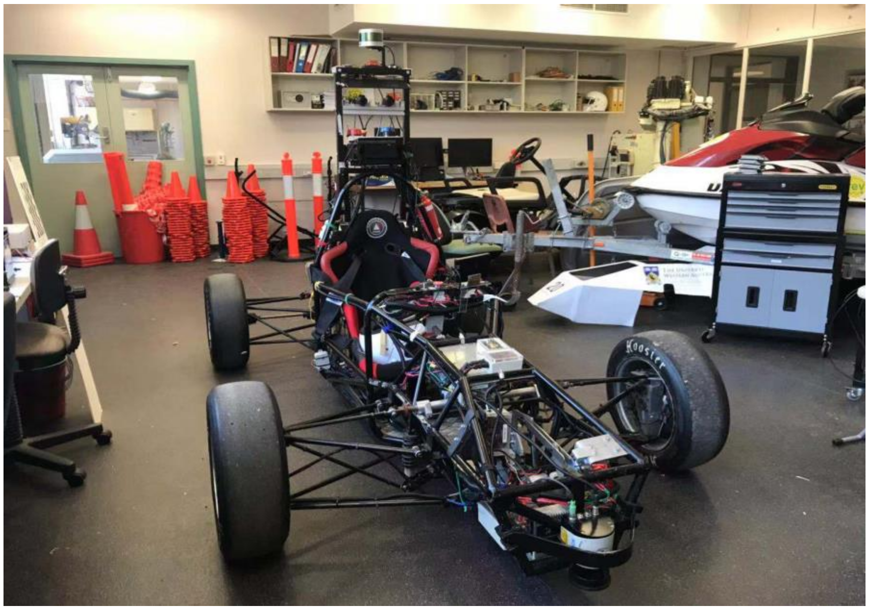


Figure 2:Autonomes SAE car

This dissertation outlines the safety system modifications to be carried out on UWA's REV [3] Autonomous formula SAE car. The safety system of formula SAE vehicle is one of the most critical systems, which can analyze and identify risks and divert the formula SAE vehicle away from hazards. The safety system consists of two parts: (1) low-level circuit; (2) safety supervisor. This dissertation mainly deals with the new controller for both the low-level circuit and safety supervisor in order to provide more reliable and accurate real-time safety protection.

1.3 Project goals

The goals of the REV Autonomous drive is to develop the formula SAE vehicle as follows.

(1) Mapping the cones track and running smoothly

Previous students in 2018 completed a demonstration for driving following cones track. In 2019, this team mainly focused on increasing the accuracy of localization, optimizing path planning, using computer vision to improve the cones track and redesigning reliable safety systems.

(2) **Driving automatically around internal UWA roads without prior planning and human operations.**

This goal is considerably more challenging than the first one due to pedestrians and other dynamic obstacles on the road. The SAE car needs to respond in real time to avoid collisions in complex environment, which requires cars with advanced hardware such as more lidar, radar and better algorithm. Hence, Professor Thomas Bräunl has offered a new autonomous shuttle bus as test platform in 2020.

1.4 Problem identification

In order to achieve the goals of the project this year, there are two main outcomes required, which are the new controller for safety system and dashboard design. Previous safety systems had some limitations in terms of reliability, flexibility and accuracy, and potential for further development. First, the safety supervisor and low-level safety circuit are based on the breadboard design. The breadboard is unreliable because it can easily cause a short circuit. Second, low-level security circuits are not programmable. The team set a specific location for the braking server, which needs to be adjusted manually. In the actual test driving, this position may be slightly shifted due to the vibration during the driving. This will cause the system to issue a brake command incorrectly. Resolving this problem requires manual adjustment and is inaccurate. The last is that there is no room to install more components in the current closed box. The size of the box matches the size of the breadboard, which is covered in wires, making it difficult to add more components. In addition, vehicle dashboards are not enough to provide more space for future development.

1.4.1 Safety System

1.4.1.1 Controller of Safety Supervisor

The safety team has a new PCB for the Safety Supervisor which was completed by Junwen. The previous safety supervisor design is based on Microchip’s 8-bit microcontroller PIC16F88 [4]. This device was selected in that time since its features reach the follow function requirements.

Tableau 1:function for safety supervisor system [4]

Function
The high-level control system can monitor the heartbeat
Cut off drive power in trip condition
Implement an "arming sequence" and prevent the throttle from being activated immediately after the drive is enabled
Apply the brake to a low-level controller via a hardwired signal
The audible notification of a fault was provided
Provide feedback on the status of the trip system
Allows high level control operations based on low level safety systems
Physical intervention required to restart the system after a failure

Although the PIC16F88 also has a watchdog timer module, it can supervise the operation of the security monitor itself by resetting the microcontroller when the timer expires. It still cannot meet industry standard (ISO26262 & IEC61508). Hence, the team needs to find a better controller to satisfy the previous function requirements and the improvement of new safety system.

1.4.1.2 Controller of Low-Level System

In order to protect the low-level circuits, which still including Arduino, accelerator and brake delay circuit. All of them were mounted into a box in the nose of the vehicle [5]. The boxes are using the old print circuit board, which are disorganized and have no space to introduce any new component, and the current low-level circuit is nonprogrammable.

1.4.2 Dashboard Design

The dashboard is too small to install the additional device for further development, the existing dashboard is covered with wires of various devices, and the wires are disorganized. Those wires are not reliable and may break easily. The new dashboard should be designed for arranging the wires more reasonably and organized. Besides this, the operations to run the SAE vehicle need a lot of steps.

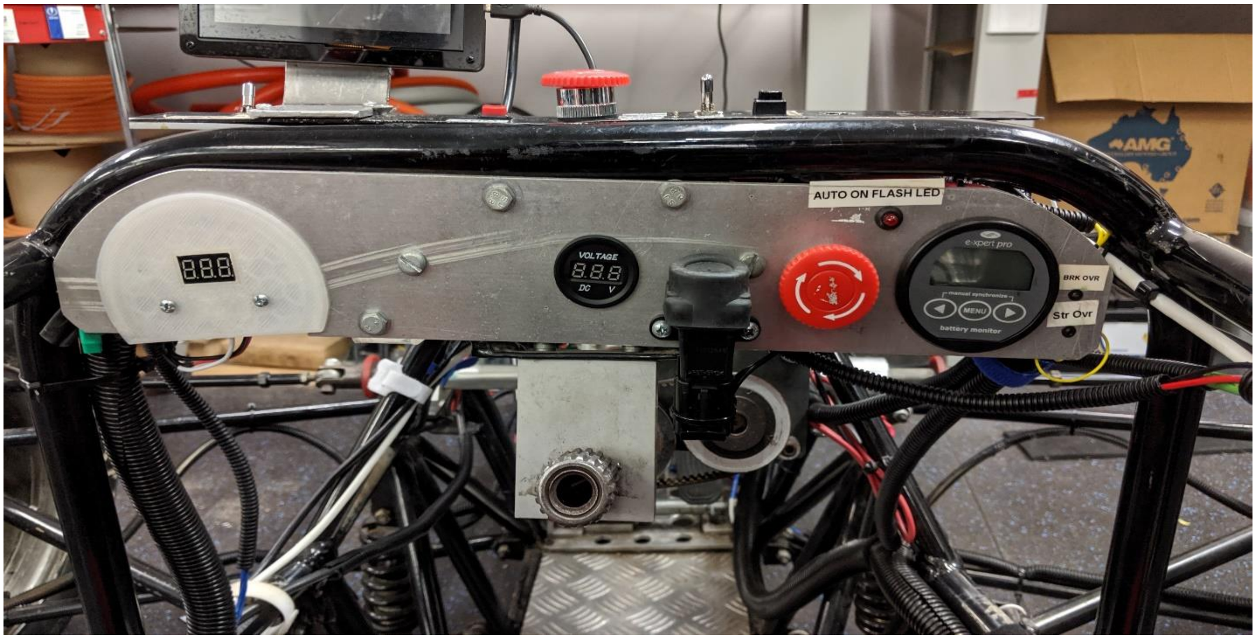


Figure 3: Currently Dashboard View

2. Literature review

2.1 ISO 26262

ISO26262 is derived from the basic functional safety standard IEC61508 for electronic, electrical, and programmable devices [6]. It is mainly used in the automotive industry for specific electrical components, electronic devices, programmable electronic devices, and other components specifically used in the automotive sector. International standards for functional safety of electronic and electrical products [7].

ISO26262 was officially started in November 2005. It has been around for about 6 years and was officially promulgated in November 2011, becoming an international standard.[8] The entire automotive industry is becoming increasingly complex, and the security of these systems needs to be strengthened. Modern cars use "Drive-by-wire" systems, such as line-controlled throttles, and drivers push accelerators and sensors [9]. An electronic control unit (ECU) receive an electrical signal sent by the pedal. The ECU replaces the metal cable that was previously connected to the accelerator pedal and the mechanical throttle control panel. The ECU is better than the mechanical method since it can do more analytical work, for example, it can analyse engine speed, the pedal position and then sent commands to the throttle[10].The goal of ISO 26262 is to establish a uniform functional safety standard to meet the needs of all automotive electronic systems. [11]

2.2 Functional safety in automotive

The safety of integrated silicon devices has relied heavily on the driving force of automotive design, especially in the past 20 years [12]. Because the quality and attributes of the product are reliable and safe, they are particularly important for vehicle manufacturers and suppliers, so they need to ensure that their products are developed, researched and validated. Due to the above, a common way of measuring and recoding the safety of an electronic vehicle subsystem is provided by the ISO 26262 functional safety standard [11]. This standard which allows for the standardization of certain practices throughout the automotive industry ensures that development methods and operating software and hardware that deal with faults and fault-related risks are guaranteed in addition to inspections [13]. ISO 26262 defines four levels of vehicle safety integrity (ASIL) A, B, C and D based on system failures that can potentially affect drivers and other road users. ASIL was identified at the beginning of the system development process to help select appropriate design processes and methods to achieve a certain degree of product integrity. ASIL D has the most stringent requirements [14].

A microcontroller unit (MCU) is a key component in an ECUs. It is not possible to meet ASIL C certification requirements with a traditional automotive MCU [15]. A new chip architecture is required to ensure processing results, data integrity of bus traffic, and data security and reliability in memory while meeting stringent response time requirements. According to the IEC 61508 [16][17] standard, the causes of dangerous faults include the following factors:

- Software or hardware system specification is incorrect
- Missing safety requirements specification
- Hardware random failure

- system cause failure
- human error
- Environnemental impact (temperature, machinerie, etc.)

From a complete system perspective, hazard assessment and safety integrity requirements include the following factors [18]:

- Ensure stable power supply and clock signal integrity in the case of voltage drops, false signals, etc.
- Redundancy or authenticity checks for processing and communication, including signals to and from sensors and actuators.
- Provide fault detection function.
- Provide fault management strategies, including defining security status and fault protection in the case of fault tolerant architecture, emergency operating mode, and controllable system shut down.
- Enhanced software development processes include the use of formal specifications, a subset of programming languages, and code verification tools.
- Strong support from silicon chips

2.3 REV SAE Safety System

Currently, the safety system includes low-level safety circuit and safety supervisor, which was designed by Thomas Drage [4] and Jordan Kalinowski [5] in 2013 and the safety supervisor made two notable changes as below in 2014[19]:

- The low-level safety box can trip the safety supervisor which allowed by a signal in series with the dash e-stop
- Add a ‘dead man’s switch’ on the dashboard which allows to simulate the heartbeat bit by a person in the car.

The low-level system was designed to detect the physical outputs of SAE control system and the human interaction against the car. The low-level safety circuit is a separate circuit which was non-programmable in order to increase its reliability. The advantage of this is that the low-level circuit will not stop functioning if faults occur in code run on the system or if the microcontroller has troubles since it is separated from the Arduino microcontroller and it also can disable low-level autonomous parts system in physical way. It uses combinational logic and comparators which can drive relays physically to cut off the connections of the autonomous system. The combinational logic performs various functions by judging driver actions. The driver actions are determined by comparing three analogue inputs (steering current, brake hall sensor, brake servo hall sensor) to the set voltage. The outputs can be explained as below [5].

- The low-level circuit will turn off power that can drive motors and unlock the steering wheel and send emergency brake command if brake applied and servomotor not causing braking or the steering motor current more than the threshold.
- the relay will cut off the power supply to the steering motor, allowing the driver to control the steering direction. If the driver try to turn in different directions or apply the brake to the automatic system, an emergency brake command is also sent.

The emergency brake command will trigger an emergency brake on the low-level system through the emergency interrupt line by the safety supervisor (designed by Thomas Drage, 2013).

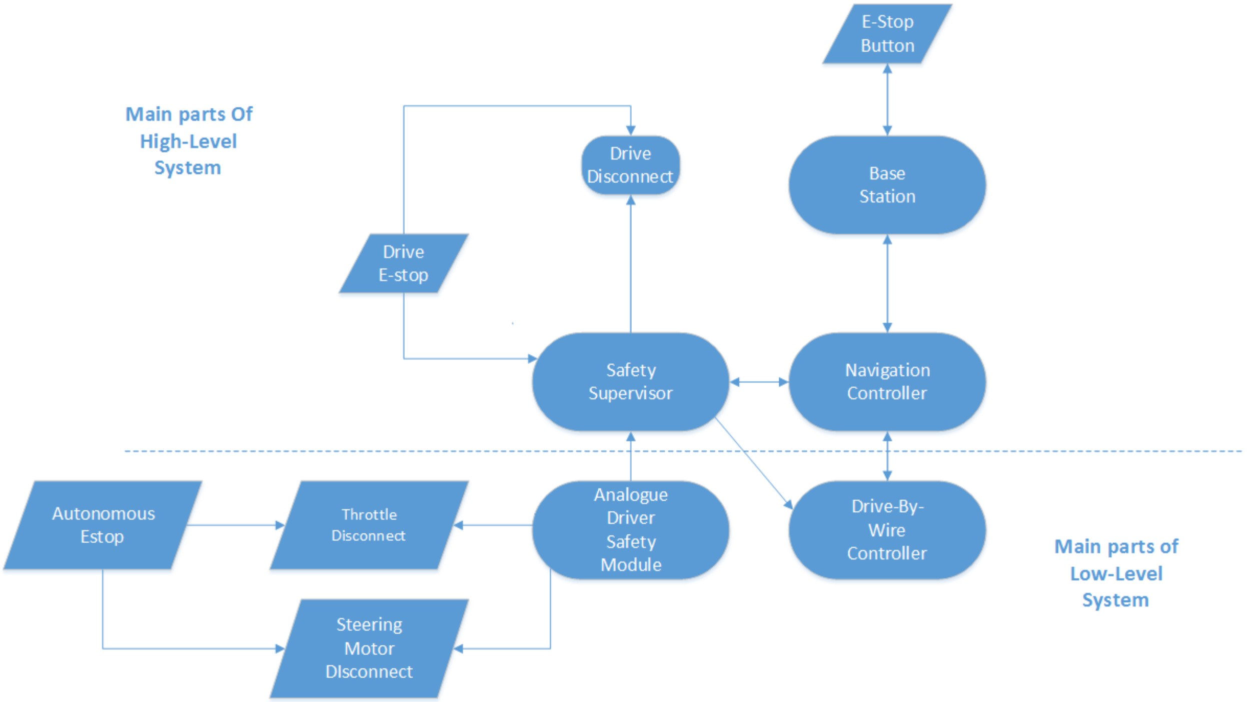


Figure 4: Main components and the structure of SAE safety system

The safety supervisor system is designed to add a level of redundancy to the safety system of the car. Additional risk reduction can be achieved by implementing the system as an independent device compared with combination with the high- or low-level control system. It still can monitor the control systems, human action against the car and carry out the independent actions in trip status.

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 analyses and identify the risks. Secondly, it can detect failures and stop the vehicle when failures occur. Lastly, it can stop the vehicle quickly when it is required. 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.

2.4 TMS570LC43 Microcontroller

The new controller TI Hercules TMS570LC43 is specifically designed for automotive and transportation applications, which can improve reliability and make the safety system meet industry standard (ISO26262 & IEC61508). It is part of the Hercules TMS570 series high-performance automotive class ARM®Cortex® -R MCUS. It provides related documentation, tools (Code Composer Studio [20]and HALCoGen) and software to help develop ISO 26262 and IEC 61508 functional safety applications. The main features of TMS570LC43 is shown below [21]

- The TMS570LC4357 device integrates two ARM Cortex-R5F floating-point CPUs that operate in lockstep mode, providing an efficient 1.66 DMIPS / MHz, running at up to 300MHz and delivering up to 498 DMIPS.
- The TMS570LC4357 device has 512KB of data RAM and 4MB of integrated flash which have single bit error correction and double-bit error detection.
- It has 64-bit wide data bus interface which can implement electrically erasable and programmable memory.
- Built-in self-test (BIST) for CPU, high-end timers and on-chip [21]
- RAM Voltage and Clock Monitoring
- Error-Correcting Code memory (ECC) on Flash and RAM Interfaces

Compared to the PIC16F88 used by currently safety supervisor system, the advantage of TMS570LC43 is shown as below

- Reach the industry standard ISO26262 and IEC 61508.
- The TMS570 MCU has taken measures in space and time to reduce common faults. In space, one of the CPU images is flipped and then perpendicular to the other CPU, and the distance between the two CPUs exceeds 100 μm; at this time, the operations of the two CPUs are interleaved for 2 clock cycles, and the operation result is sent to the special comparison module. Perform real-time comparisons. If there is a problem with the CPU operation, error processing is performed immediately [22].
- Allow team to find out unexpected problems when debugging and taking a test drive by

receiving the notification of error messages from the TMS570LC43

- The compiler software base on C language provided by TEXAS Instruments and a tool named by HAlCoGen [23] can debug which still can download the program directly to the MCU. The team can use this tool to upgrade the safety supervisor codes was created by Thomas Drage.
- It provides the SafeTI Design Kit [24], which provides several recommendations for the safety team to enable the development of ECU certification to ISO 26262 ASIL D.
- ECC can increase the reliability of safety system.

3. Hardware Safety Supervisor Design

3.1 Safety Supervisor Circuit diagram revise

ISO 26262 standard requires electronic components in SAE vehicles to be reliable. In order to have better consistency and control, they should be proficiently put in a suitable place. The safety supervisor circuit and low-level safety circuit was redesigned using Printed Circuit Board instead of unreliable bread board design.

Before designing the PCB, the team needs to sort out the functions of new the safety system, referring to the previous system and figure out inputs and outputs of the old one. These works can help the team save time and the cost of designing a new one, because the team can refer to the well-designed parts from the previous one, keep it in new diagram. If there is some unreliable designs in the old diagram, the team can avoid it in the next design work. There are 14 conditions that will trigger the safety system to execute the functions, and more than 20 outputs can be achieved, which was listed by Thomas Drage, Jordan Kalinowski. Here is an example shown below:

IF	WHEN	THEN	WHY	HOW
Lost Heartbeat (no change of state for a certain time)	Autonomous driving in progress	1. High level control program stops (zero throttle) 2. Trip sent to safety supervisor	Signal from remote emergency stop lost or high level controller frozen	High level controller

After this necessary preliminary work, the team use Eagle CAD to connect the component in schematic. Due to the previous inputs and outputs being previously figured out, the team only needs to find the model of the component from various resource libraries and connect them correctly referring to previous I/O. The improvements and advantages of new diagram will be introduced in section 3.5. The placement of components will be the final appearance of the finished PCB. Therefore, the placement of components requires consideration as to whether components need to be pulled out or inserted frequently, for example, terminal blocks on the controller, USB and Ethernet interfaces. They are placed on the edge of the PCB. This will facilitate access to the source. In addition, the PCB will be designed to be as small as possible to reduce the space requirements of the compact SAE vehicle. Also, because Eagle CAD can provide wire widths on PCB, it needs to be as wide as possible to improve reliability. However, the two requirements are contradictory. The shrinking of the PCB means that the components will get closer, which means that the wires that connect them will be closer. There needs to be some space between the wires, or they will interfere with each other. After consideration, the system will be installed in an enclosed box on a small platform in front of the dashboard. The design team decided to meet the minimum size requirement first. If the size is too large, it will affect the driver's view. Surprisingly, you must also satisfy the minimum volume requirement. With minor modifications, the maximum width of the wire can be set to 20 mil (about 0.5 mm). After completing the schematic and layout, the PCB model was sent to the factory for manufacturing. The ultimate size of the PCB is 174*163mm.

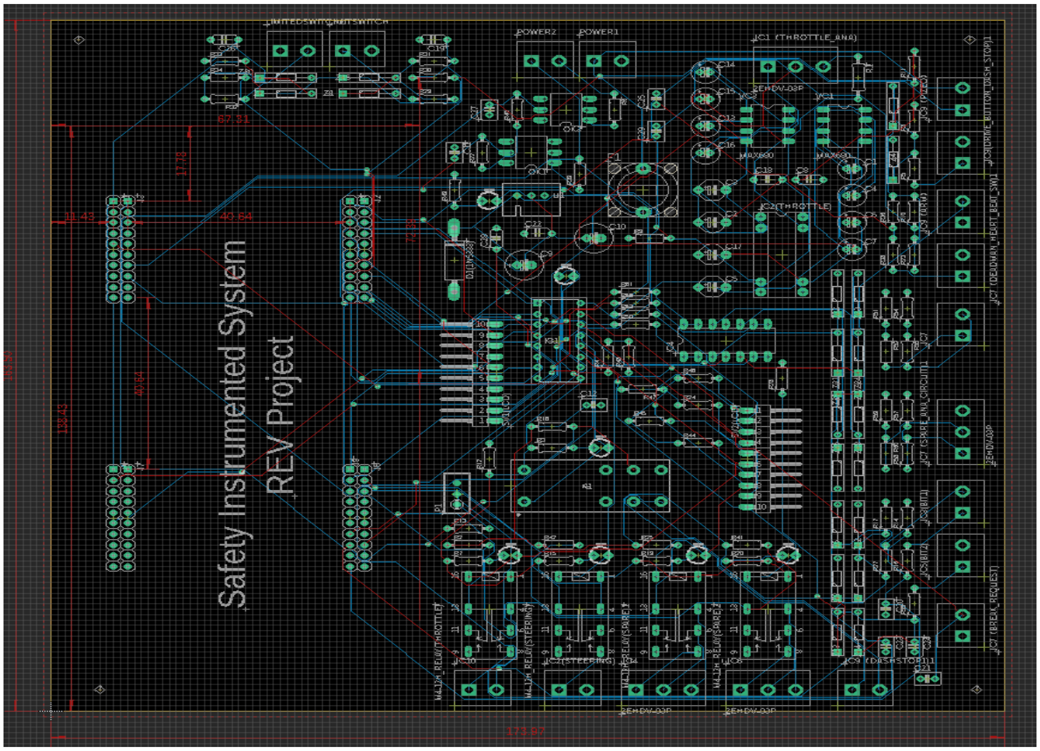


Figure 5: SAE new Safety supervisor circuit layout designed using EagleCAD

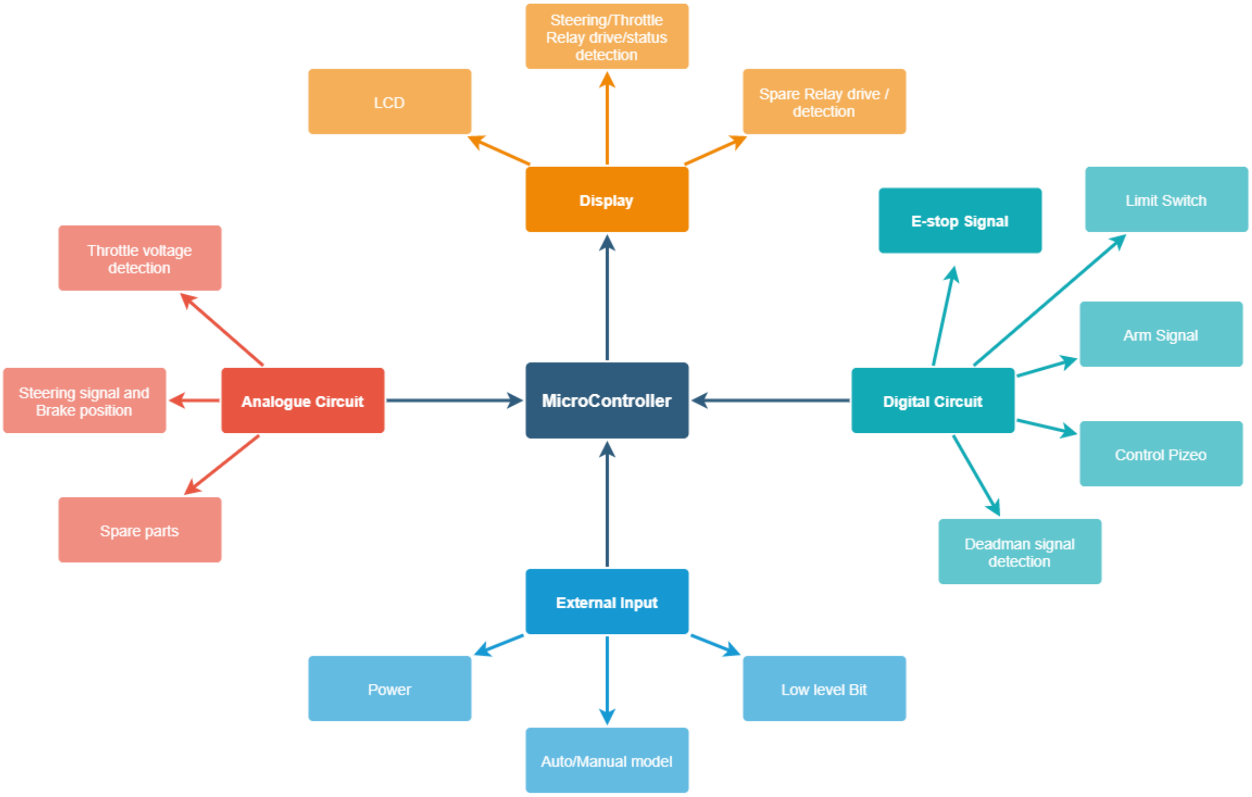


Figure 6: Overview diagram with all sub-systems

3.2 Software state machine

The software performs four main functions, which were designed by Thomas Drage [4]. It includes monitoring the heartbeat signal, acting on tripping initiated by the navigation controller, reporting tripping initiated by the analog hardware security module, and allowing the security "arm" of the autonomous system. The microcontroller receives commands consisting of a single ASCII character continuously from the navigation controller through its UART and sends a reply message consisting of a variable length string and a newline character.

Tableau 2: Command set of safety supervisor [4]

Command	Description
E	Emergency Stop
+	Heartbeat high value
-	Heartbeat low value
B	Set brake interlock on
H	Set brake interlock off
A	Sound Piezo alarm

The arm sequence is designed to mitigate the risk of a hardware or software failure causing the vehicle to accelerate during the period after the driver system is enabled. Sequential startup has been realized, and its operation is as follows:

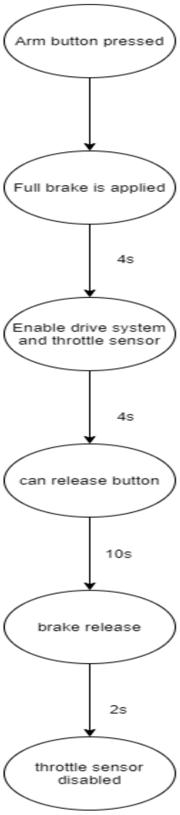


Figure 7: Safety system simple state diagram

The operator needs to hold the arm button for 8 seconds to keep the drive enabled and prevent accidental startup. When the drive is enabled, there is a delay of 4s before the latch is locked, giving the operator the opportunity to cause problems immediately after the drive is enabled by simply releasing the button to disconnect the drive power. During the 16 seconds process, the driver will be cut off if the system detects the throttle voltage. Hence it can give operator time to leave this vehicle before it starts moving. Insufficient heartbeat signals or trip conditions caused by the emergency shutdown of the navigation controller, driver safety module or dashboard will cause the driver to be disabled and the alarm to be activated.

3.3 Code Converting

The previous code was developed using MikroElektronika's ANSI C PIC compiler [4]. The team needs to copy the code from old PIC microcontroller into new controller and update the inputs/outputs to suit. The official development environment used by the TMS570LC43x LaunchPad development board is TI's CCS (Code Composer Studio, code debugging tool). First, to briefly introduce this software, Code Composer Studio consists of tools for developing and debugging embedded applications. It has compilers, source code editors, project build environments, descriptors, debuggers, emulators, and many other functions which provide by TI family. CCS IDE provides a single user interface to help users complete each step of the application development process. With sophisticated and efficient tools, users can quickly get started and add functionality to their applications using familiar tools and interfaces. Basically, the team needs the same serial commands and roughly the same logic to develop the code based on the previous one. There will be some changes needed and the old code did not have an LCD to display things on. The timers and the way set pins will be different on the new controller. For the LCD part, the code can just cycle through and test each relay one at a time, displaying the result for 5 seconds, then do the next one.

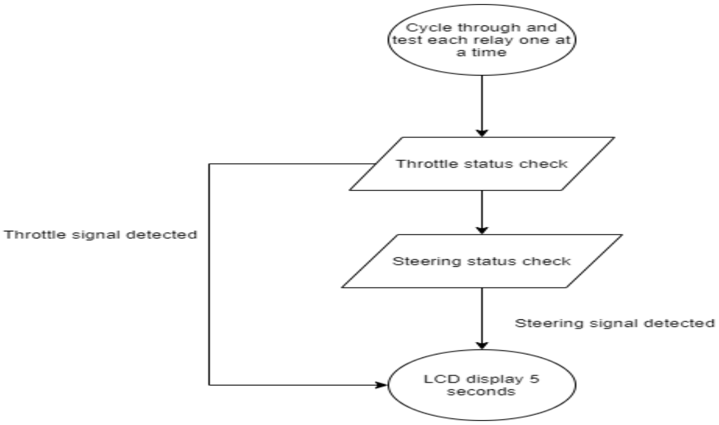


Figure 8: LCD display state diagram

The team listed pin connection on the new MCU with corresponding signals so that the previous code can be converted more conveniently. Pin configuration can be setup by HALCoGen. Users can use HALCoGen to generate hardware abstraction layer device drivers for Hercules microcontrollers. It provides a graphical user interface that allows users to configure peripherals, interrupts, clocks, and other Hercules microcontroller parameters. After configuring the Hercules device, the user can generate peripheral initialization and driver code that can be imported into ccs.

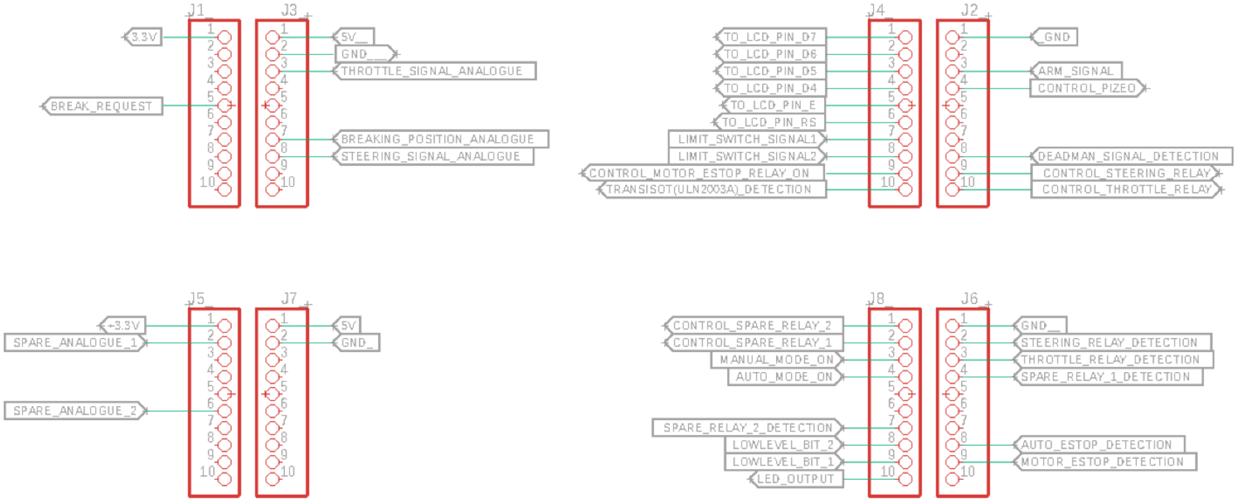


Figure 9: New Safety supervisor inputs and outputs

3.4 PCB Soldering and testing

Soldering PCB board must follow the industry process to ensure it fulfills industry standard.

1. After getting the circuit board, observe whether the circuit is damaged or not

2. Use a multimeter to measure whether there is a short circuit between the power supply and the ground
3. Soldering the power supply part first and debug the power supply successfully
4. Soldering CPU, resistor, capacitor, crystal oscillator and reset circuit. Then retest the power and ground in case short circuit and thermal breakdown happen during welding
5. Soldering the serial port and connect it to the computer for serial input and output debugging
6. Soldering other devices

After soldering part has been completed, the team needs to test the function performance of the PCB board. The test part can be divided into two parts: test before power on and test after power on. After soldering a circuit board, when checking whether the circuit board can work normally, usually not directly supply power to the circuit board, but follow the steps below to ensure that there is no problem at each step and then power on:

1. Whether the connection is correct: check whether the circuit connection is correct according to the schematic diagram
2. Check the installation of components: whether the installation of diode polar capacitor and micro chip is correct. Check whether the soldering of each device has pseudo soldering
3. Check the power supply interface has short circuits or not: Check whether there is a short circuit between the power supply and each level. In circuit design, self-recovery fuses should be added to protect circuits.

The following steps after power on should be checked:

1. Observation of power on: Observe whether the circuit has abnormal phenomena, such as smoke, strange smell, touch the outer package of the integrated circuit to test whether it is hot or not. If an abnormal phenomenon occurs, turn off the power supply immediately
2. Static test: Check the level status whether is up to expectations step by step. In general, the debugging sequence of the subcircuit is carried out according to the direction of the signal, and the output signal of the previously debugged circuit will be used as the input signal of the subsequent stages, thus creating conditions for the final adjustment.
3. Dynamic test: Add code to test the system with software.

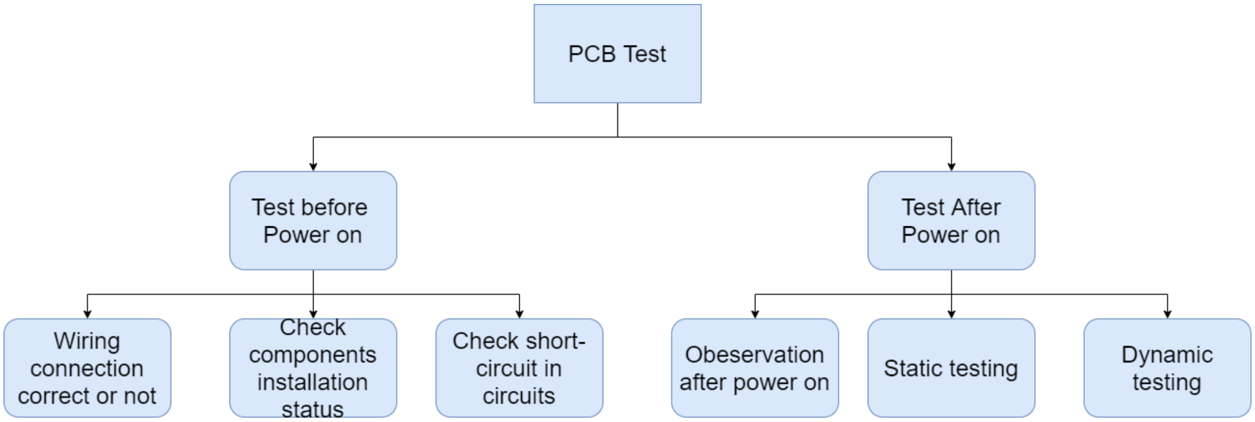

PCB Test
Test before Power on
Test After Power on
Wiring connection correct or not
Check components installation status
Check short-circuit in circuits
Obeservation after power on
Static testing
Dynamic testing

Figure 10: PCB testing process

3.5 Result & Discussion

3.5.1 New Analogue circuit

In order to enable the safety system to detect the real-time analog signal input, the analog circuit is introduced into the PCB circuit. There are two different analog circuit designs in the new PCB design. One is higher costs and more complex design. It consists of two voltage converters MAX680 [25] and a precision isolation amplifier ISO124P [26]. This design refers to the low-level control PCB from the previous team's design. The MAX680 increases the + 5V voltage to ±10V and then provides two sets of positive and negative voltages to ISO124P. The circuit is used to amplify the signal from the throttle and send the amplified signal to the pin on the controller. The microchip unit on the controller then analyzes the signal.

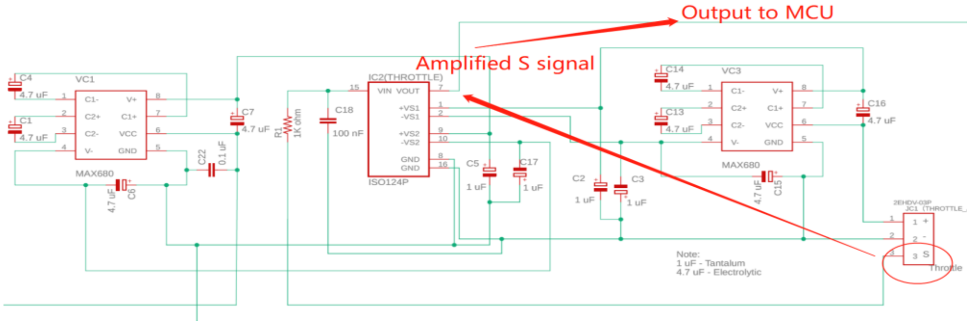


Figure 11: Analogue Circuit for throttle signal detection

The previous throttle signal was a digital signal transmitted via an optical coupler, so the safety system could only determine whether it was a 5V signal or a 0V signal. The functions of the safety system can only be used when there is a signal or no signal. However, with the analogue signal, missing parts between 0 and 5V can be detected. The safety system can effectively capture the current throttle signal, and the team can set up more safety features. For example, when the throttle signal is greater than 2 v, the accelerator signal will be shut down immediately. The analogue circuit increases the flexibility. In addition, if there is external interference, the previous system will sometimes display errors, but with analog circuits, it becomes more reliable.

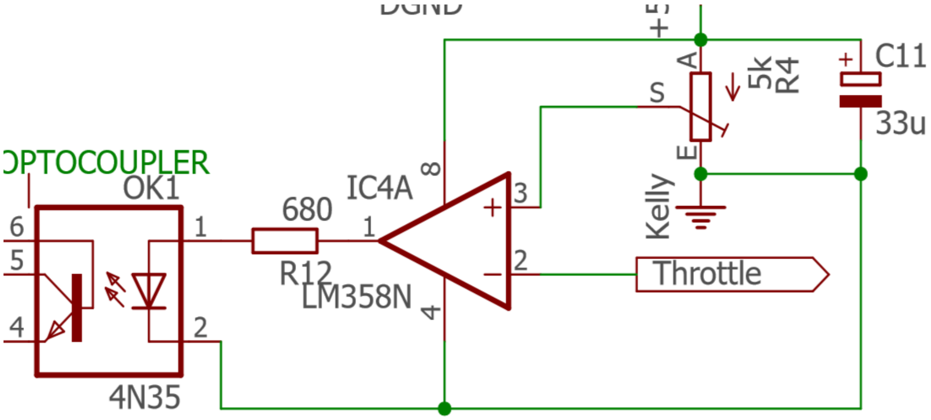


Figure 12: Previous design for throttle signal detection [4]

The other analogue circuit consists of a combination of a diode and an amplifier. It is used in the circuit that receives the brake position and steering wheel signal.

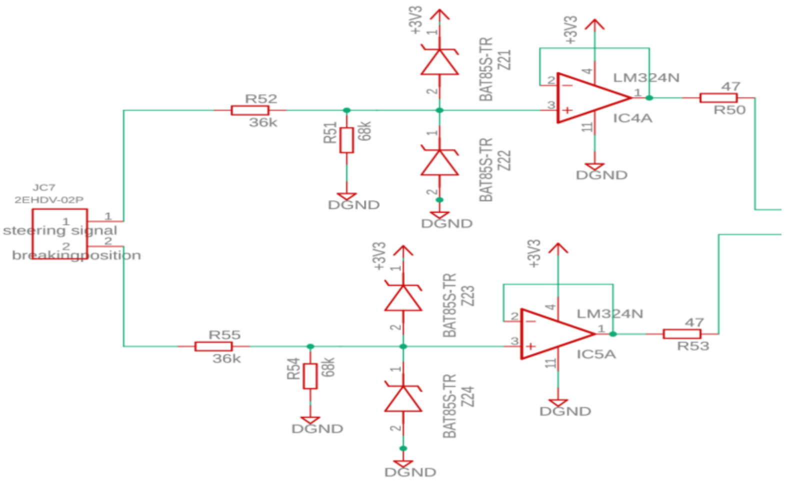


Figure 13: Digital Circuit for new Safety system

3.5.2 New Digital Circuit

Digital circuits have also been introduced into new PCB circuits. Low level control signal, piezo, dead-man button and emergency stop button signal are all input by digital circuit. The digital circuit introduces a protection mechanism, which will be introduced in detail in 3.5.3. The pull-up circuit in the blue box on the left is designed to increase the driving current. In addition, there is another pull-up circuit inside the microcontroller. These pull-up circuits allow the microcontroller to carry less load (and to detect the signal easily).

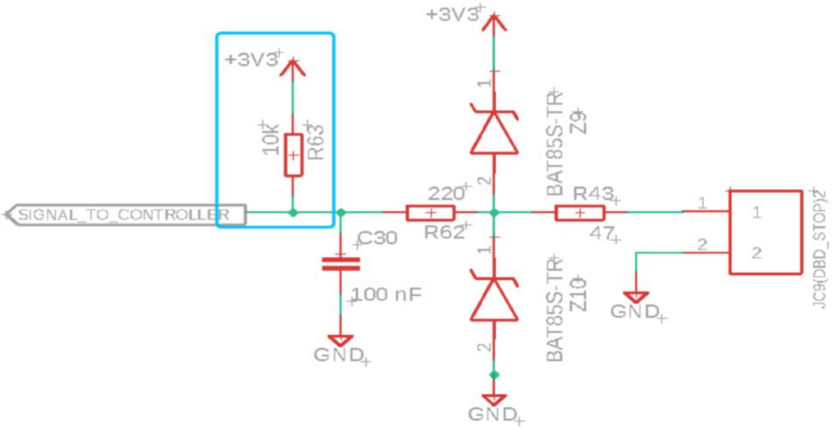


Figure 14: Dashboard stop button function design

3.5.3 PCB Protection

From the digital circuit shown in section 3.5.2, the team added two protection designs in the figure to improve signal stability and the protection circuit. The R62 resistor and the C30 capacitor can be regarded as a low-pass filter. The two diodes BAT85S-TR can filter currents that are too high or too low. This design can protect the signal from external interference and make the signal more stable and accurate. The protection design of these two diodes is also used in analogue circuit.

There are five relays on the new PCB. Four of these used M4-12 relays and cooperative diodes after referring to previous low-level control PCB designs. Two of the four relays are used to cut off throttle signals and steering motor signals, respectively, and the remaining two are used for future development components. The other relay is K1 50.12.9.012.1000. It is used to cut off the BMS (battery monitoring system) signal. Relay detection has been 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, another can also be used to check whether the relay is working properly. The principle is that the relay should work when there is a signal, and both switches will be connected to the upper circuit. At this point, the 3.3v current used as the relay signal will be directly grounded, short-circuiting the connection to the controller. If the relay does not work properly, the 3.3v current will not be short-circuited, but will be connected to the controller.

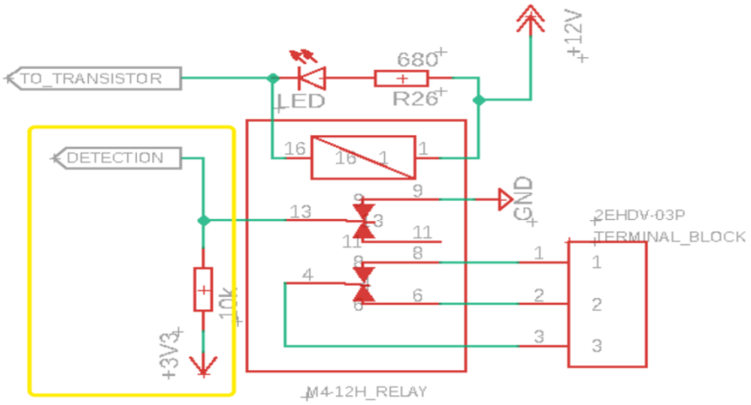


Figure 15: The relay design for Throttle and Steering signal

3.5.4 Test Result

The team used multimeter and oscilloscope to test the PCB board followed the industry standard. Since the name of the component also were printed on PCB board, so it is easy for the team to complete the soldering process successfully, the PCB board also performed very well. In order to connect the LCD monitor with the PCB board, team used a 10-core cable and crimp pins to connect the housing then it can connect to the socket on both PCB and LCD monitor.

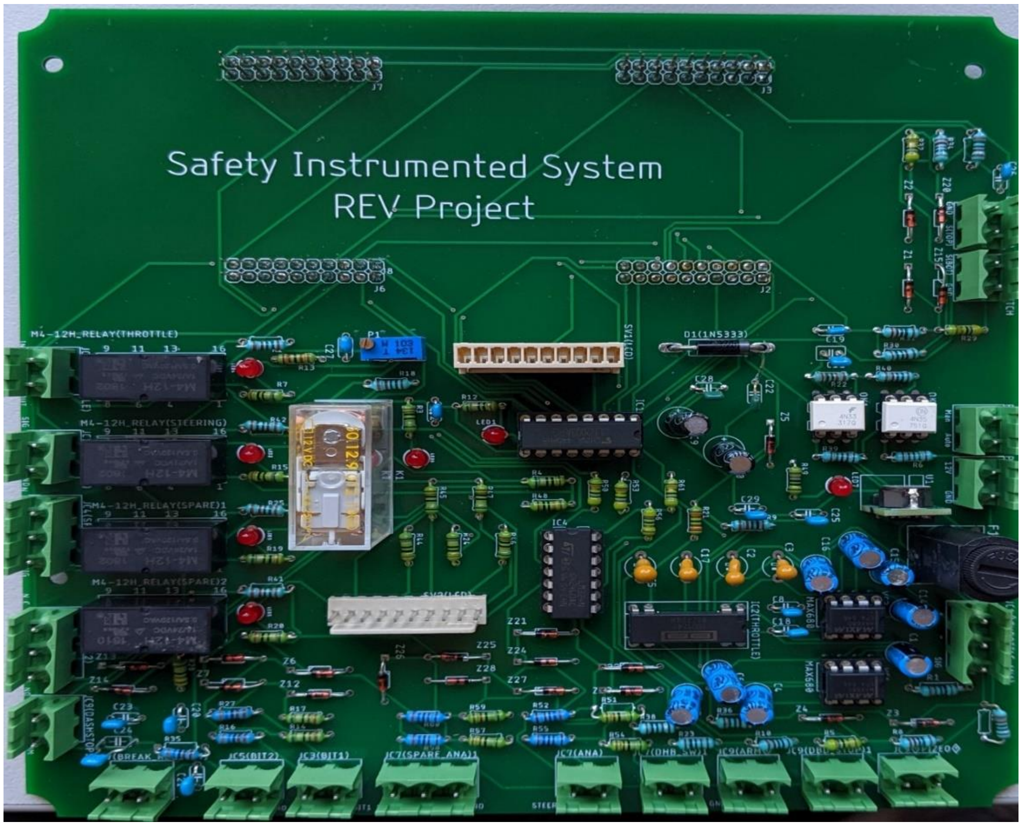


Figure 16: Safety supervisor PCB

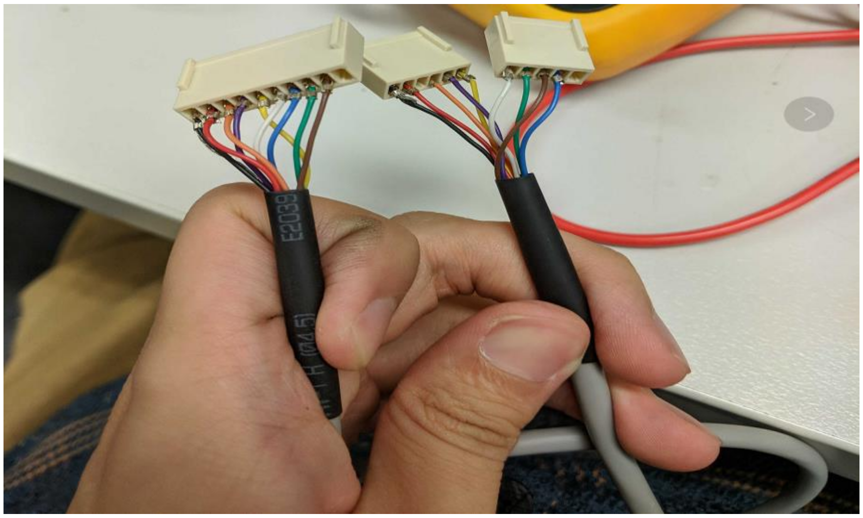
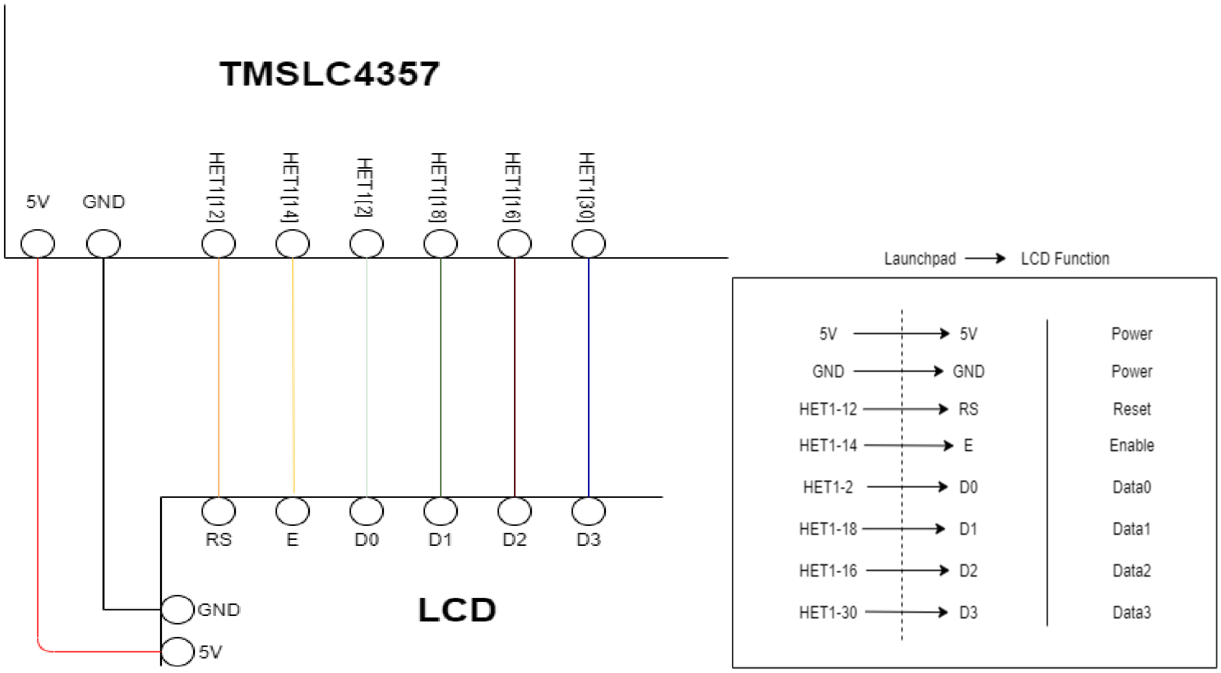


Figure 17: LCD-MCU connection cable

For the software part, the team tested how to drive such a display which needs to activate relay and check relay status from a TMS LaunchPad. The connection was as shown in Figure17. Additionally, the final display result as shown in Figure 18.



Launchpad →	LCD	Function
5V →	5V	Power
GND →	GND	Power
HET1-12 →	RS	Reset
HET1-14 →	E	Enable
HET1-2 →	D0	Data0
HET1-18 →	D1	Data1
HET1-16 →	D2	Data2
HET1-30 →	D3	Data3

Figure 18: LCD connection pin

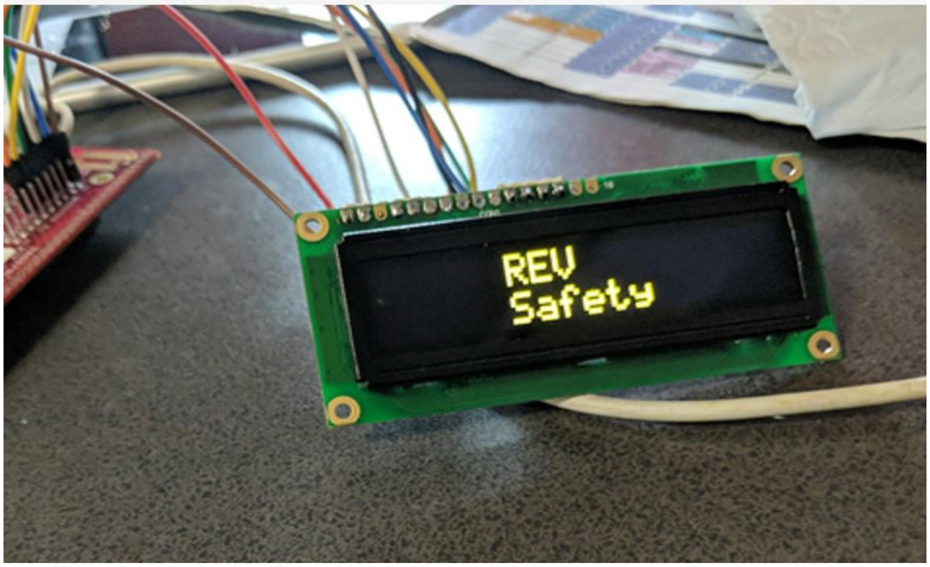


Figure 19: Test result of LCD

4. Dashboard Design

4.1 Overview

Existing dashboards have two parts, and because they are placed vertically and horizontally, they are referred to as "vertical dashboards" and "horizontal dashboards" in the following discussion. Both sections have secondary monitors that show the status of the vehicle and various buttons that trigger the security system. Before triggering the autopilot mode, the driver or tester runs the appropriate startup program on a touch screen on the left side of the dashboard. Then pull up two emergency switches and press the ARM button to start the autopilot mode. The components used in this process (touch screen monitors, emergency stop buttons, etc.) have taken up quite a bit of 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. There were some problems with the two parts of the dashboard that made it difficult to improve on the original, so the team decided to redesign the entire dashboard using the Siemens NX design software. In conclusion, the team needs a larger, more reliable dashboard and fewer buttons on the dashboard to make it look simpler and easier to operate.

4.2 Vertical dashboard design

On existing dashboards, speedometers are arranged from left to right, current operating voltmeters for low-level systems, motor emergency switches (motor emergency stop buttons), and battery monitoring systems (BMS). The steering wheel and alarm buzzer are also installed in the lower center of the dashboard. The steering wheel takes up most of the space above the vertical dashboard and blocks the components below. The previous design positioned the three monitors so that the driver could read the values from them while driving. The speedometer is installed on the far left so that the driver can control the speed when driving on the UWA internal road in manual mode. In addition, it could help drivers check if the vehicle is traveling at a set speed while on autopilot. The voltmeter of the underlying system is relatively small and is installed in the middle. The BMS is installed on the far right so that the team can monitor the battery voltage while charging. However, this arrangement means that the motor's emergency stop button must be placed in the shaded area below the steering wheel. When the driver is in an emergency, he can turn off the electric motor by pressing the e-stop to stop the vehicle quickly. However, the buttons are under the steering wheel and are hard to touch. This can be a significant hazard, so the team needs to move this button to a more easily accessible location.

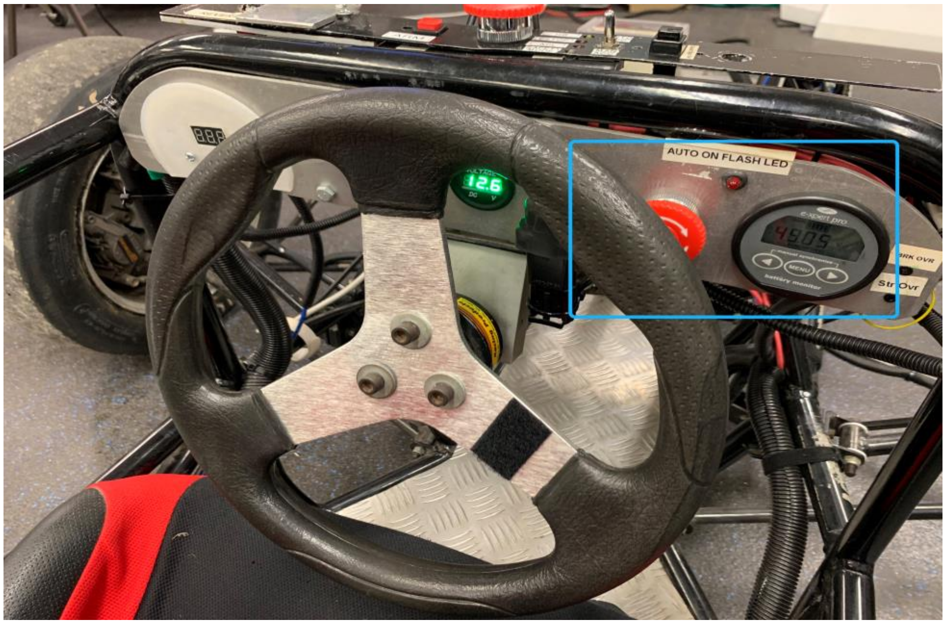


Figure 20: Current vertical dashboard

Considering that there is no obvious defect in the currently displayed position, the team decided to move the position of the BMS. Another consideration is that most people are used to using the 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 right and the easiest to touch.

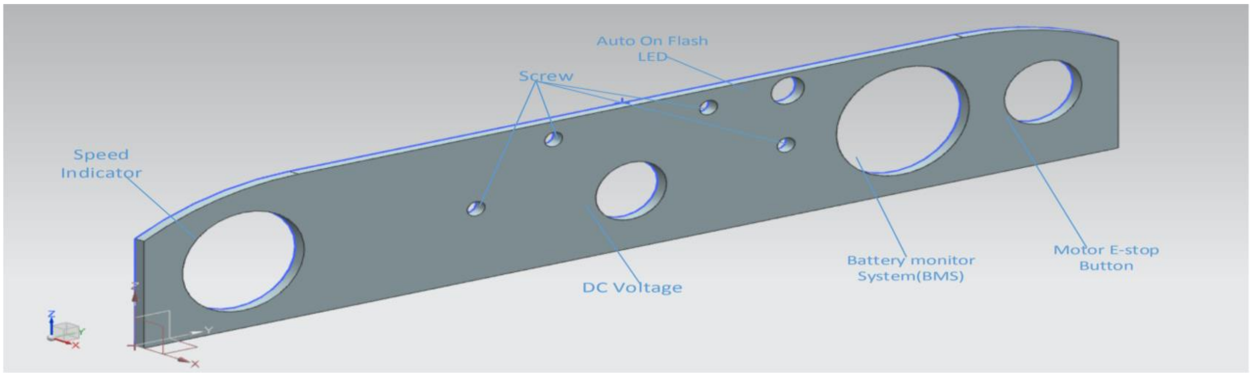


Figure 21: New vertical dashboard design

4.3 Horizontal dashboard design

The horizontal dashboard has a variety of buttons and touch screens that can be used to control the on-board computer. Because of the plethora of buttons on the existing dashboards, the new safety system removed some of the original designs, such as the HB LED, which displays heartbeat signals. The current dashboard has two serious barriers. One is that the touch screen is fixed vertically to the bracket and blocks the driver's view. Another is that the dashboard does not fully protect the wires connected to the dashboard component. The current dashboard is a simple metal sheet with no other protection underneath. The wires are covered with metal plates at the top but are exposed elsewhere. Furthermore, the wires are not well anchored and are supported directly through the interface to the component.

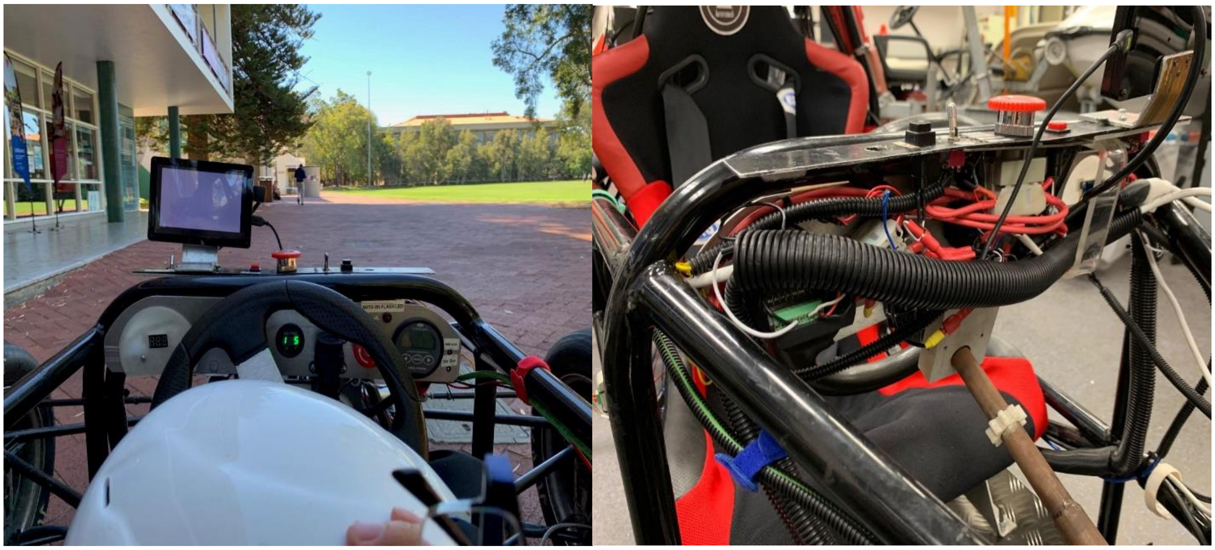


Figure 22: Current horizontal dashboard

The team initially considered placing the monitor horizontally so that the driver's view could be greatly expanded. But it also means the driver cannot see the display while sitting in the car. He/she must stand up and check, which is difficult to monitor in real time, and it is not always easy to get in and out of the car. This simple solution of placing the monitor horizontally needs to be simplified. In addition, better protection structures are needed to protect the reliability of the wires. Finally, the team considered the concept of a folding dashboard.

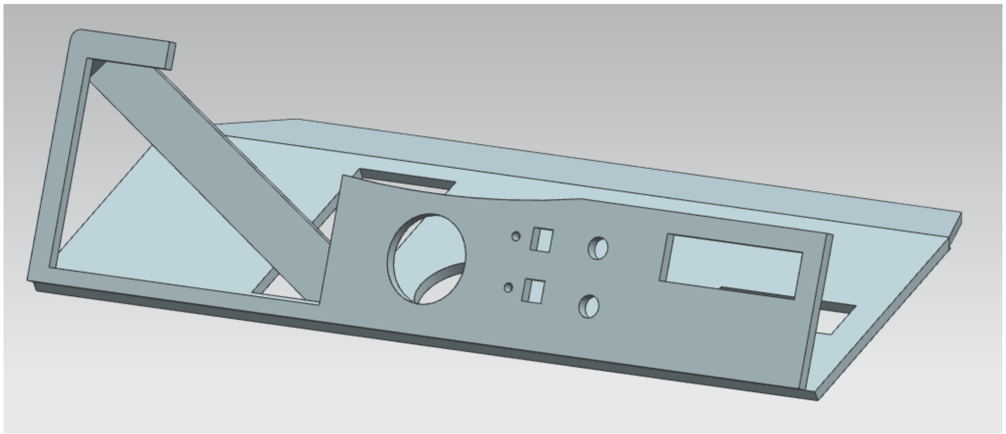


Figure 23: New horizontal dashboard design

The new horizontal dashboard is divided into two parts, which are connected by hinges. The upper part is a metal plate for component installation and the left side has an embedded display installation area. The lack of corners is designed to reduce the size of the circuit board and reduce the effect of blocking the driver's view. On the other hand, it ensures that the display's large sockets can be easily installed into the embedded structure. The autopilot emergency stop button is installed in the middle of the license plate. The area around the emergency stop button (round hole) will be emptied to avoid interfering with the surrounding components in an emergency. There is also a small arc on the top edge of the middle section. Its role is to minimize the size of the plate to provide a wider view. The original ARM and DEADMAN buttons (square holes) are also retained and their signals are sent directly to the new system. To the left of the switches are their corresponding indicators, which show whether a signal was sent to the security system when the button was pressed. The reverse button and the manual automatic mode switch are also retained. At the far right of the table is a new LCD monitor that shows the real-time status of the safety system.

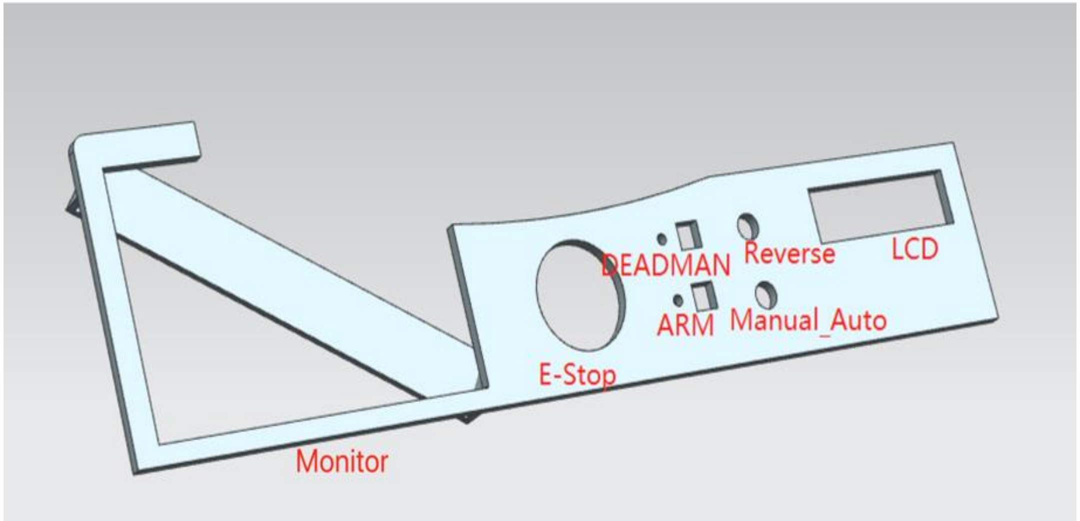


Figure 24: Horizontal dashboard components

The bottom of the horizontal dashboard is fixed. The end of the wire connected to the safety system will be fixed here. Most of the wires will be fixed, and only a small portion of the wires will be free to move to connect to the components (the maximum upper perimeter when folded, about 14 cm). In addition, the team introduced a downward sloping edge up the front of the board. It could be designed to protect the wires from objects flying in from the front, such as rocks, and water splashed by wheels. The hole on the bottom panel corresponds to the hole on the top. The only difference is the rectangular hole on the left. This is a hole reserved for the right interface of the display to facilitate the passage of wires.

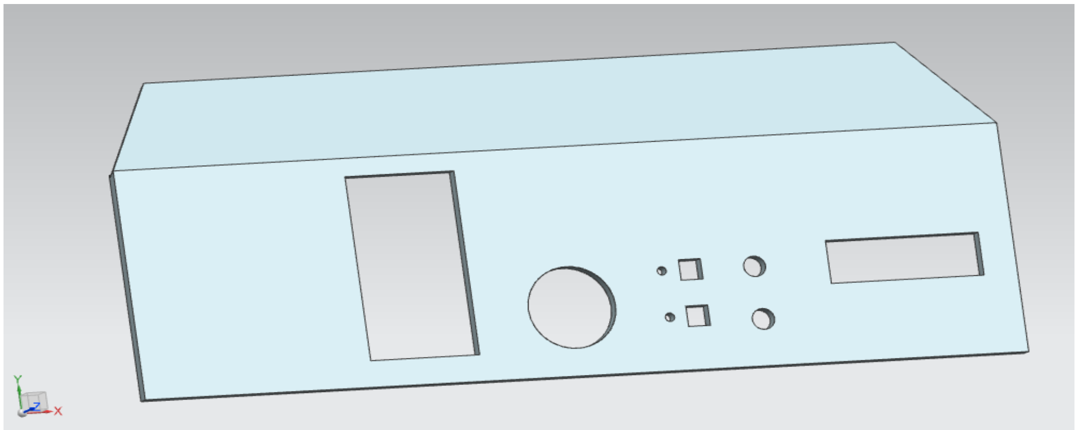


Figure 25: The bottom part of horizontal dashboard

4.4 Result & Discussion

The new dashboard has the following improvements and advantages over previous dashboards: first, the location of the components is more reasonable; The emergency button is placed in a position where it is easy to touch and there are no obstacles around. Then, removing the LED makes the dashboard look simpler and more straightforward. The new LCD display displays the status of the safety system in real time, allowing drivers to monitor the vehicle more effectively. The foldable design allows the driver to have a wider view during manual driving, then improving driving safety. The larger dashboard has a front and bottom edge to better protect the wires below.

The new dashboard is more compatible with new safety systems and provide better support for increased vehicle safety. These models have been submitted to the University of Western Australia mechanical workshop for manufacture. The vertical dashboard is mounted under the frame, so accurate dimensions are required. However, due to device limitations, the design team was unable to provide very accurate sizing, and because the previous dashboard was designed a long time ago, the team was not sure how to fix the dashboard to the frame. Therefore, professionals and professional tools are needed to determine the final dimensions. The vertical dashboard that the team is currently measuring is 440mm long and 80mm wide. The horizontal instrument panel is shorter than 440mm. The widest dashboard is 130mm. The final size will approach this size. The new dashboard will be made of 2mm-thick aluminum, but the final product will depend on the material in the shop, which may vary thickness but is larger than 2mm.

5.Conclusion and Future work

The project is to look at the industry standards for safety systems and the autonomous vehicle safety research. The team needs to create new hardware to let electronic control units of SAE car reach the industry standard, at the same time, make improvement in the software functionality and really utilizing the TI controller for safety. The PCB part was completed and tested well. It provides more safety functions and reliable components than the previous one. The software part has converted from the previous system and set the pin configuration already. The team only tested the display part of the software function due to the Covid-19 pandemic, so the more complex in-car test need to be processed in the future, and currently the TMS570 is used to develop the golf autonomous car which is a new project for the REV team. The new dashboard models have been sent to the UWA mechanical workshop and they will not be complete until the impact of Covid-19 lessens. It can improve the interaction between the car and operator and increase safety of the car by adding the reliable operation buttons, and LCD could show any errors from the safety system which stop the car or prevent it from starting the information drivers needs to know, especially to help get the car started.

In the future work, replacement of the components will allow the electronic control unit to reach the industry standard. The team can design a new low-level system using another TI Hercules instead of Arduino. The reason to change is that the TMS570 has far more power and has built-in counters for wheel speed sensors, so the low-level Arduino and the wheel speed sensor Arduino could be combined into one new low-level. For the current safety system, the team need to mount the new dashboard and think about interface software for the Jetson, as it only shows the PC desktop right now, then complete the in-car safety system test.

Reference

[1] "Tesla, Inc," Model S | Tesla Australia. [Online]. Available: https://www.tesla.com/en_AU/models. [Accessed: 17-Aug-2019].

[2] R. Abrams and A. Kurtz, "Joshua Brown, Who Died in Self-Driving Accident, Tested Limits of His Tesla," The New York Times, 02-Jul-2016. [Online]. Available: https://www.nytimes.com/2016/07/02/business/joshua-brown-technology-enthusiast-tested-the-limits-of-his-tesla.html. [Accessed: 17-Aug-2019].

[3] The REV team. Autonomous BMW. REV Project, UWA. [Online]. Available: http://therevproject.com/vehicles/bmw.php

[4] Drage, T. H. (2013). Development of a Navigation Control System for an Autonomous Formula SAE-Electric Race Car. BE Thesis, School of Electrical, Electronic and Computer Engineering, University of Western Australia.

[5] Kalinowski, J. (2013). Conversion of a Formula SAE Vehicle to Full Drive-by-Wire Capability. REV Project, UWA.

[6] E. Bagalini, J. Sini, M. S. Reorda, M. Violante, H. Klimesch, and P. Sarson, "An automatic approach to perform the verification of hardware designs according to the ISO26262 functional safety standard," 2017 18th IEEE Latin American Test Symposium (LATS), 2017.

[7] X. Larrucea, P. González-Nalda, I. Etxeberria-Agiriano, M. C. Otero, and I. Calvo, "Analyzing a ROS Based Architecture for Its Cross Reuse in ISO26262 Settings," Communications in Computer and Information Science New Trends in Model and Data Engineering, pp. 167–180, 2018.

[8] J. Pimentel, "The Role of ISO 26262 Book 4 - Automated Vehicle Safety," 2019.

[9] M. Capelli-Schellpfeffer, "Electrical safety: Past performance, present challenge, future promise," 2010 IEEE IAS Electrical Safety Workshop, 2010.

[10] F. Dumitrache, M. C. Carp, and G. Pana, "E-bike electronic control unit," 2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME), 2016.

[11] N. Das and W. Taylor, "Quantified fault tree techniques for calculating hardware fault metrics according to ISO 26262," 2016 IEEE Symposium on Product Compliance Engineering (ISPCE), 2016.

[12] S. A. Bagloee, M. Tavana, M. Asadi, and T. Oliver, "Autonomous vehicles: challenges, opportunities, and future implications for transportation policies," Journal of Modern Transportation, vol. 24, no. 4, pp. 284–303, 2016.

[13] "What is the ISO 26262 Functional Safety Standard?," What is the ISO 26262 Functional Safety Standard? - National Instruments. [Online]. Available: https://www.ni.com/en-us/innovations/white-papers/11/what-is-the-iso-26262-functional-safety-standard-.html.

[Accessed: 12-Sep-2019].
14] X. Iturbe, B. Venu, J. Jagst, E. Ozer, P. Harrod, C. Turner, and J. Penton, “Addressing Functional Safety Challenges in Autonomous Vehicles with the Arm TCL S Architecture,” IEEE Design & Test, vol. 35, no. 3, pp. 7–14, 2018.

[15] G. Hwang, A. Freiwald, and H.-S. Ahn, “Microcontroller Approach to Functional Safety Critical Factors in Electro-Mechanical Brake (EMB) System,” SAE Technical Paper Series, 2014.

[16] H. Gall, “Functional safety IEC 61508 / IEC 61511 the impact to certification and the user,” 2008 IEEE/ACS International Conference on Computer Systems and Applications, 2008.

[17] “IEC 61508: SIL 3,” SafeTTy Systems Ltd. [Online]. Available: https://www.safetty.net/tt-design-examples/iec-61508-sil-3.

[18] M. Tlig, M. Machin, R. Kerneis, E. Arbaretier, L. Zhao, F. Meurville, and J. V. Frank, “Autonomous Driving System : Model Based Safety Analysis,” 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 2018.

[19] The REV team. UWA REV Autonomous SAE Vehicle: Engineering and Operation Manual. REV Project, UWA. https://github.com/braunl/SAEAuto/wiki

[20] “Code Composer Studio (CCS) Integrated Development Environment (IDE) CCSTUDIO (ACTIVE),” CCSTUDIO Code Composer Studio (CCS) Integrated Development Environment (IDE) | TI.com. [Online]. Available: http://www.ti.com/tool/CCSTUDIO. [Accessed: 11-Sep-2019

[21] TEXAS Instruments. (2015). Hercules TMS570LC43x LaunchPad Development Kit. Texas Instruments Incorporated. United States. [Online]. Available: http://www.ti.com/corp/docs/legal/trademark/trademrk.htm

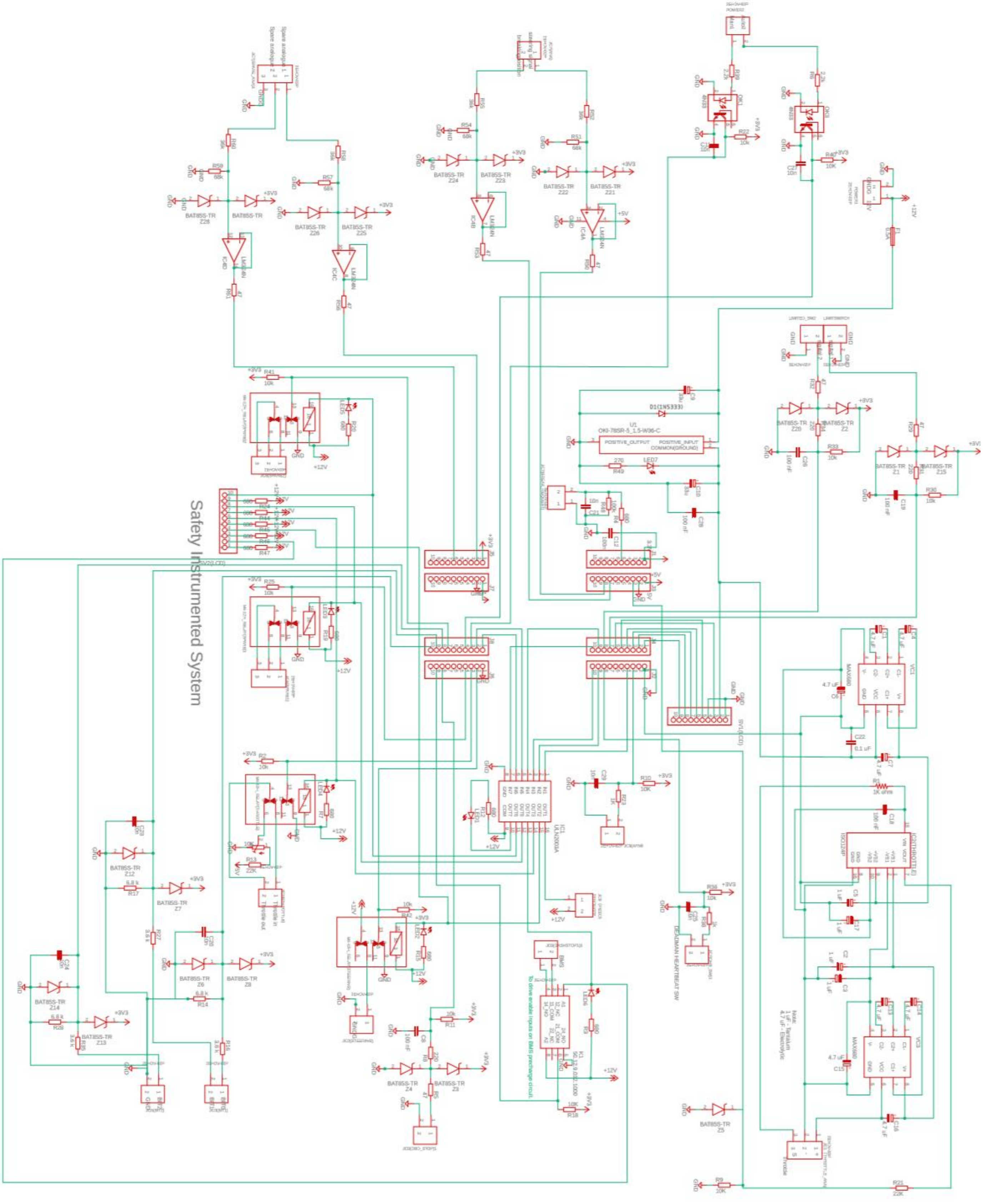
[22] “Texas Instruments TMS570LC43x User Manual,” Manuals Library. [Online]. Available: https://www.manualslib.com/manual/1285178/Texas-Instruments-Tms570lc43x.html. [Accessed: 12-Sep-2019].

[23] “Hardware Abstraction Layer Code Generator for Hercules MCUs HALCOGEN (ACTIVE),” HALCOGEN Hardware Abstraction Layer Code Generator for Hercules MCUs | TI.com. [Online]. Available: http://www.ti.com/tool/HALCOGEN. [Accessed: 11-Sep-2019].

[24] “SafeTI design packages for functional safety applications.” [Online]. Available: http://www.ti.com/ww/ en/functionaLsafety/safeti/SafeTI-26262.html

[25] 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 April 2020].

Appendix


Safety Instrumented System
Spare analogue 1
Spare analogue 2
LM324N
IC4A
IC4B
IC4C
IC4D
BAT85S-TR
Z1
Z2
Z3
Z4
Z6
Z7
Z8
Z12
Z13
Z14
Z15
Z21
Z22
Z23
Z24
Z25
Z26
Z28
R41
10k
R25
R2
R54
68k
R51
R57
R59
R22
R47
680
4N33
OK1
OK2
D1(1N5333)
U1
OKI-78SR-5_1.5-W36-C
POSITIVE_OUTPUT
POSITIVE_INPUT
COMMON(GROUND)
LED7
LED1
LED3
LED5
R49
270
C9
C10
C28
C21
C12
100 nF
MAX680
VC1
VC3
C22
0.1 uF
C7
4.7 uF
C6
R1
1K ohm
C18
ISO124P
IC1
ULN2003A
R30
10K
R23
C29
DEADMAN HEARTBEAT SW
R56
K1
R58
R11
R6
R5
R16
R14
R17
R28
R35
R27
C20
C23
C24
C15
C16
C17
C2
C3
C5
C13
C14
6.8 k
3.9 k
22K
R13
R21
R9
R18
18K
Throttle
Mat
1 uF - Tantalum
4.7 uF - Electrolyte
To drive enable inputs on BMS precharge circuit.
LIMITED_SWITCH
F1
0.5A
+3V3
+5V
+12V
GND