System Design and Development for Safety Related Applications

Dylan M. Banning[1]

University of New South Wales at the Australian Defence Force Academy

The implementation of Electrical / Electronic / Programmable Electronic control systems require additional design rigor throughout all stages of product development to ensure the equipment under control remains in a safe state of operation. This report describes the principles of functional safety used in the development of an electronic throttle control system designed for implementation in a safety related application. The design and development of the system shall use industry related safety standards and procedures alongside a framework used in the management of complex technical projects to produce a detailed design of a functional electronic throttle control system. The overall system architecture and the methods used during its design demonstrate the fundamental principles of functional safety key to the implementation of a safety related control system.

Contents

Nomenclature

Automotive Safety Integrity Level (ASIL) - One of four levels to specify the items or elements necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk, with D representing the most stringent and A the least stringent level.
Element- System or part of a system including components, hardware, software, hardware parts and software units.
Failure- termination of the ability of an element to perform a function as required.
Fault-abnormal condition that can cause an element or an item to fail.
Item- system or array of systems to implement a function at the vehicle level to which ISO 26262 is applied.
Other Technology- technology different from Electrical/ Electronic (E/E) technologies within the scope of ISO26262.
Random Hardware Failures- failure that can occur unpredictably during the lifetime of a hardware element and that follows a probability distribution.

[1] PLTOFF, School of Engineering & Information Technology. ZEIT4501

Safe State- operating mode of an item without an unreasonable level of risk.
Safety Goal- top level safety requirement as a result of the hazard analysis and risk assessment.
Low demand mode- where the safety goal is only performed on demand, in order to transfer the Equipment Under Control (EUC) into a specified safe state, and where the frequency of demand is no greater than one per year.
High demand mode- where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demand is greater than one per year.
Continuous mode- where the safety goal retains the EUC in a safe state as part of normal operation.

I. Introduction

With the mounting societal pressures of increased vehicle performance at reduced manufacturing costs and fuel consumption the use of programmable electronics in road vehicles over the last 20 years has increased significantly. As electrical technology begins to become more advanced with increased capability at less cost, the vehicle manufacturing industry like many others use Programmable Electronic Systems (PES) to enhance performance and improve operating efficiency.

Electronic Throttle Control (ETC) is a control system inspired by fly-by-wire technology from the aviation industry which replaces the mechanical linkages between the accelerator and the throttle valve with electrical signals controlled by PES to provide a number of performance benefits.

Due to the safety related nature of ETC when in operation, the use of PES raises concerns about the security of such systems. To overcome the concerns of Sudden Unintended Acceleration (SUA) in automobiles and assure the reliability of ETC under conditions of fault or failure, the system must be designed with consideration for the functional safety of Electrical/ Electronic/ Programmable Electronic (E/E/PE) components implemented in such safety-related systems.

II. Project outline

The following section provides an overview of the project and describes how the project is structured and managed in order to achieve the required outcomes.

A. Aim

The aim of this project is to explore and understand the concepts of safety related system design in accordance with functional safety standards in the context of ETC. At the beginning of the project, current Formula SAE Australia regulations prohibited the use of electronic throttle control in the internal combustion engine racing category due to the safety critical nature of its implementation. As a result, the motivation behind the development of this project is aimed at designing a PES that provides the functionality of ETC while its compliance with functional safety standards can be verified for its safety related application. The design procedure for a PES system in accordance with functional safety standards meets the aim of the project as it provides maximum exposure to the concepts of safety related system design and development.

B. Goals

The primary goal of this project is to provide maximum exposure to the concepts used in functional safety design engineering. In order to extract the maximum information surrounding the concepts of engineering design and functional safety the secondary goal of the project is to design and verify an ETC system that has the functionality required for an Australian Defence Force Academy (ADFA) Formula SAE racing car and is compliant with industry functional safety standards. The design and verification of such a system provides the ADFA Formula SAE team with system leading research for possible implementation into future race car design.

C. Methodology

The project is structured around the combination of the system engineering and safety lifecycles. The grouping of the standard system engineering lifecycle and the safety lifecycle allows for efficient project management with clear milestones and deliverables related to both the functional and safety aspects of ETC system design. The majority of the project follows the framework of the system engineering process with a slight variation due to the combination of preliminary and detailed design. The decision to merge the two stages of design was a made at the completion of the system design review, as the next stage in design was at the component level and as a result, the systems electrical / electronic design occurred during detailed design. Figure 1 is a chart that shows the combination of the system engineering lifecycle and the safety lifecycle with the design documentation required at each stage of product development.

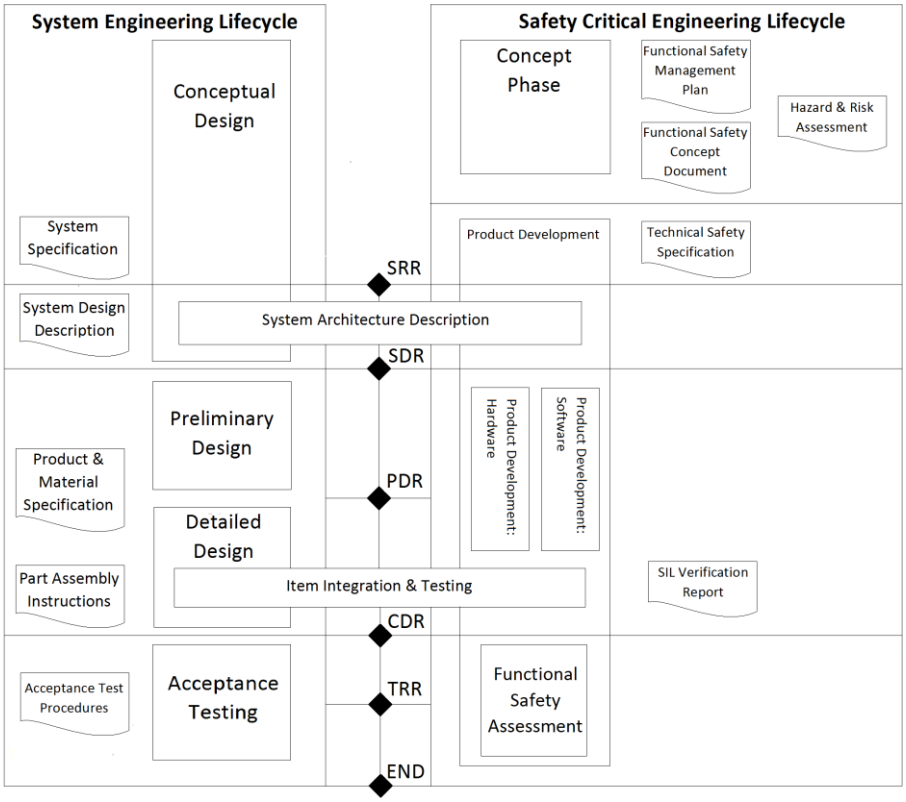

Figure 1. Project Outline and Design Documentation

III. Background Information

The following section looks into three separate areas relating to safety related system design:

1) The basic concepts of throttle control for internal combustion engines while providing an overview of the operational benefits of implementing an ETC system.
2) An introduction to functional safety and the origins of safety related PES.
3) A review of automotive incidences where E/E/PE components have failed with serious consequences.

A. Electronic Throttle Control

Electronic Throttle Control (ETC) sometimes called drive-by-wire uses, electronic signals from E/E/PE technology to control the position of the throttle valve within the throttle body. The throttle of an internal combustion engine uses a valve to regulate the amount of air that enters the engine, which in turn controls the fuel/air ratio, thus increasing or decreasing engine power output.

The power output produced by the engine depends on the fuel/air ratio, therefore to regulate the amount of air entering the manifold, the throttle valve acts as a variable obstruction to the air entering the intake manifold to manipulate the air pressure available to the engine for use in combustion. When the valve is fully open, the intake manifold is filled with air at ambient atmospheric pressure (assuming no performance enhancements) therefore producing a maximum fuel/air ratio. If the valve is fully closed or partially open, a vacuum develops as the air behind the valve drops below the ambient atmospheric pressure allowing controlled variation of the fuel/air ratio. Figure 2 show's a Cross Section of a Typical Throttle Butterfly Valve.

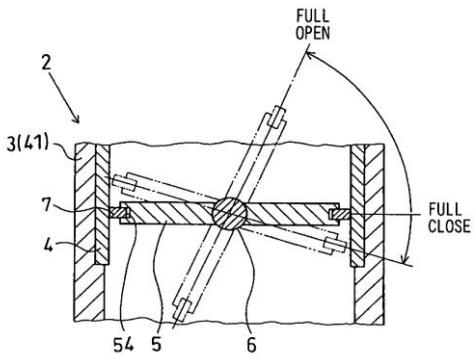

Figure 2. Cross Section of Typical Throttle Butterfly.
Source: http://www.freepatentsonline.com/7168682-0-large.jpg

Traditional methods of throttle control rely on a mechanical cable to provide the linkage between the accelerator pedal and the throttle body. Shown in Figure 3 is a simplified ETC schematic where the traditional mechanical linkages have been replaced with E/E/PE technology.

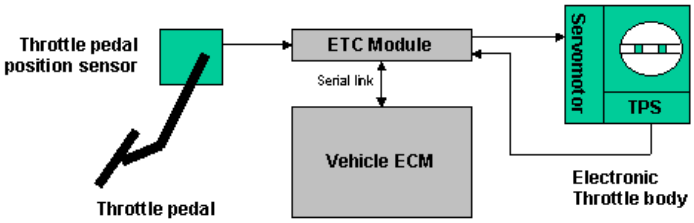

Figure 3. Electronic Throttle Control Schematic.
Source: http://www.picoauto.com/applications/electronic-throttle-control.html

Once an ETC system is implemented into a vehicle it can support a number upgrades for added vehicle functionality, performance and safety. Technology such as Electronic Stability Control (ESC) requires electronic control of the throttle in order to interface with existing vehicle stability functionality such as Anti-locking Braking System (ABS) and Traction Control (TC) to compare actual vehicle direction with the desired direction. Should there be any discrepancy between what the driver wants and what the vehicle is doing the ESC technology applies both the brakes and accelerator to the relevant entities on the vehicle to reduce or remove any developed under or over steer. Other advantages associated with the implementation of ETC includes improved fuel economy and throttle performance, as the typically unstable inputs from the user can be electronically modified to optimally suit the operating conditions of the vehicle.

B. Functional Safety Overview

Functional Safety is a developing discipline of engineering which aims to increase the level of engineering "rigor at every stage of design, installation and operation of PES" (Punch 2013, p. 6) used in safety related applications to assure system reliability. To assist system designers, contractors and owners with the execution of functional safety design, the safety lifecycle has been developed to provide engineering guidance for the implementation of PES in safety related applications.

Traditionally safety related control functions use mechanical or hardwired electrical systems to provide overall system control as they have well understood failure modes and behavior. With the benefits of flexibility, increased functionality and ease of use provided by programmable electronics, traditional mechanical control systems are being replaced. This increased use of programmable electronics has provided significant benefits to control systems but has resulted in a reduction in the predictability of system failure and its failure behavior (Punch 2013, p. 5).

The initiation of functional safety standards originated in 1987 when the United Kingdom Health and Safety Executive (UK H&SE) released 'Guidelines for the use of PES for Safety Related Applications' which studied accidents involving PES control systems (Punch 2013, p. 5). The study categorized the accident causes and developed a concept for the safety lifecycle from these categories. After the UK H&SE released the results of its study, global standards organisations began to formalise the recommendation to eventually develop the current international accepted standard of IEC61508 which encompasses E/E/PE systems performing safety related control or protective functions (Punch 2013, p. 6). From this parent standard, application specific functional safety standards have been developed for specific E/E/PE control industries. The most applicable functional safety standards for the implementation of ETC in a Formula SAE racing car are AS61508 'Functional Safety of Electrical/ Electronic/ Programmable Electronic safety-related systems' and ISO26262 'Road Vehicles-Functional Safety'.

Functional safety system design relies on the three key design principles, redundancy, multiplicity and diversity to achieve system reliability applicable to its assigned safety integrity level. Redundancy uses identical functioning parts to achieve higher system reliabilities. Multiplicity is the incorporation of multiple shutdown paths or protection devices to enhance system safety integrity. Diversity uses different devices performing the same functionality to reduce the probability of system failure being affected by common failure modes.

C. E/E/PE Vehicle Failures

The following section outlines incidences that have occurred to road vehicles as a result of E/E/PE component failures within electronic throttle control systems. The analysis of these events is part of the concept phase of the functional safety lifecycle and provides valuable information that can assists the identification of possible hazards or unwanted events in the safety related implementation of ETC.

1. Audi 5000 Sudden Acceleration

Audi mid-sized automobiles manufactured after 1982 were sold in the USA as the Audi 5000. During 1983-1987 Audi in the USA had to recall its 5000 series models due to a large number of sudden unintended accelerations (SUA). Audi initially responded by suggesting the drivers of the cars were at fault because of confusion between the pedals (Safety Research & Strategies, Inc 2009).

After significant investigation by the regulating authorities in the US there were a number of recommendations put forward to the manufacturer. The recommendation of particular interest to this project is the replacement of the idle stabilisers. The idle stabiliser is fitted to a vehicle to maintain uniform idle speed when operating under different conditions. The operation of the idle stabilizers is done via the electrical movement of a valve to regulate the airflow into the engine. The regulating authority concluded that incidences of SUA where initiated by the malfunction of the electronic idle stabiliser causing an initial unintended acceleration forcing the operator into a state of confusion and panic and the depressing the wrong pedal forcing the vehicle further into unintended acceleration (Safety Research & Strategies, Inc 2009).

2. Porsche Electronic Failure

In 2010 a Porsche Panamera had an isolated incident where all electronics shut down. Electromagnetic interference from nearby radio and TV towers affected the communication link between the transponder key and the Engine Control Unit (ECU) triggering the shutdown of the vehicle and all electronics with the occupants trapped inside. The transponder key is an additional security mechanism fitted to disarm the vehicle immobiliser and start the vehicle. In this incident a small family was trapped inside the car and was unable to unlock the doors or lower the windows due to the immobilisation of the vehicle placing them into a serious and potentially fatal situation. Eventually the window was smashed and the occupants were safety released from the vehicle (Hagon 2012).

3. Toyota Safety Defects

In 2009 a Lexus ES350 experienced a sudden unintended acceleration causing it to reach speeds of 100 MPH before it crashed and killed the 4 occupants in the car. This accident triggered Toyota's largest recall between 09 -11. The product recalls during 2009 and 2011 were consequences of a poorly designed pedal and floor mats fitted to both new Toyotas and Lexus models as well as random software failures caused by the addition of extra functionality intended to improve vehicle safety should an unintended acceleration occur (Vlasic & Apuzzo 2014). The exact cause of the fatal crash is unknown but it was concluded that it was either an obstructed accelerator pedal due to a floor mat or a sticky accelerator pedal caused by the poorly designed pedal mounting (Bensinger & Vartabedian 2009).

4. Jeep Sudden Unintended Acceleration

Jeep Cherokee and Grand Cherokee models between 1991 and 1995 were recalled after a series of reported incidents involving sudden unintended acceleration. After investigation by the regulatory authorities in the US it was found that there were two main causes for the SUA accidents. The first relates to human error with the driver rearranging or missing steps in the vehicle start up routine getting the brake and accelerator pedals confused and depressing the accelerator instead of the brake. The other is the inadvertent energizing of the servo control motor used for cruise control within the vehicle. The accidental activation of the cruise control motor causes the servo to depress the throttle automatically without user knowledge and control.

To overcome this problem Jeep now manufactures its vehicles with a standard brake to shift interlock which forces the driver to activate the brake before shifting gear therefore preventing unintended activation of the accelerator and forcing the deactivation of cruise control should it be inadvertently energized(Safety Research & Strategies, Inc 2009).

5. Ford Cable Defects

Ford discovered a manufacturing defect with the cruise control cable in a series of models ranging from 1997 to 1999. Theses faulty cruise control cables caused the throttle cable to stick causing sudden unintended acceleration. Ford was forced by the regulating authorities to redesign the cable in order to rectify the defect (Safety Research & Strategies, Inc 2009).

IV. System Design

The following section explains the implementation of both the system engineering and safety lifecycles in the design and development of the ETC system. Included in this section is the analysis of the relevant background information and its inclusion in the final system design.

A. System Definition

The first stage of the ETC system design is the definition of system functionality and safety requirements. To derive the system safety requirements, a Hazard and Risk Assessment (H&RA) must be carried out to firstly identify the safety goals of the system.

The H&RA firstly identifies any hazards or unwanted events associated with throttle control that may occur to "the Equipment Under Control (EUC) and EUC control system" (Punch, p. 53). Within the scope of this project, the EUC is the SAE racing car and the EUC control system is the ETC. Potential causes and the consequences of each cause are identified, and an initial risk assessment is conducted, based on the likelihood and consequence of the cause to establish an initial level of risk without the implementation of controls. After the initial risk assessment, all potential controls, including preventive risk controls used to minimize the likelihood of an unwanted event before it occurs and the mitigating risk controls which minimize the likelihood of the unwanted consequence are identified. A residual risk analysis is conducted, again assessing the likelihood and consequence of each hazard or unwanted event, but this time with the inclusion of the identified controls. The result is a level of risk for the hazard and given that the risk is deemed acceptable by the end user, each design influencing control becomes a safety goal. Once a control has been identified as a safety goal, it is assigned an Automotive Safety Integrity Level (ASIL) between A and D.

To assign an ASIL it requires a risk assessment of the probability, severity and consequence of a particular safety goal failure. An ASIL defines the minimum requirements with regard to the reliability that the safety goal must meet in order to produce a system that is safety compliant. The higher the letter in the alphabet, the higher the minimum requirements for safety goal design acceptance. For the electronic throttle control system, Table 1 provides a summary of the HR&A with the identified system safety goals and there assigned ASIL.

Table 1: Summary of identified safety goals for ETC system.

SG Number	Method of Implementation	SG Description	ASIL Allocation
1	E/E/PE	Emergency Cut-off	B
2		Throttle Control	B
3		Power distribution	A
4		Engine Over speed	A
5		Single Start Switch	A

Once a safety goal has been assigned and its respective ASIL and a demand mode has been determined, each safety goals, functionality and method of implementation is broadly described in the ETC system Functional Safety Concept (FSC) document. Each safety goal identified for the system has a defined safe state which it is responsible for achieving should it be activated by a hazard or unwanted event. A systems safe state defines a mode of operation where the EUC is considered safe. Each safety goal identified for the ETC system is responsible for removing the vehicle from the identified hazard or unwanted event and placing it into is safe state. After defining the safe state for each safety goal, a broad description outlining the functionality required and the modes in which each safety goal operates is documented in the FSC document.

Once a functional description of each safety goal has been developed, the formal system design requirements are derived to ensure the implementation of each safety goal is within the system design. The safety specific formal requirements are then documented in the Technical Safety Specification (TSS) to directly influence system design and increase overall reliability.

From a functional perspective, the system specification contains requirements which describe the functionality of the throttle control system. The specification of ETC system requirements is done using formal language and is broken down into a series of categories including performance, interface, environmental, quality and safety, these requirements provide coverage of all aspects of system implementation. The method used to construct the requirements of the system follow a framework containing a clear performance statement, a method of verification with a brief procedure and concludes with a statement of rationale to justify the addition of the requirement. The same requirement framework applies for all categories of ETC requirements including the safety requirements detailed in the TSS.

An important part of ETC system design is the specification of the external interface requirements which describe, in detail, the characteristics of connections between the throttle control system and its external interfaces. The importance of these requirements is to allow the integration of the ETC system into the FSAE

racing car upon completion of system design and verification. Other requirement categories include environmental, which defines the conditions the systems must be capable of working in, system quality requirements to enhance overall system maintainability and flexibility with specific examples of maintainability and flexibility include the requirement to use the same type of fastener when securing the system to the car to allow the same tooling to be used when remove components of the system. An example of flexibility may include having a minimum of 50% additional input and output ports within the systems processor to allow for future expandability.

To allow the efficient management of all formal system requirements, the TSS is included as a safety requirements sub section within the system specification therefore collating all system level requirements and defining the systems functional baseline.

After specification of both the functional and safety requirements of the ETC system, a broad system level solution is identified and documented in the System Design Description (SDD). The upper level of solution for the ETC system involves the identification of the applicable subsystems and key components contained within each subsystem. The ETC system is broken into 6 subsystems which perform specific functionality and allow for the accurate definition of subsystem boundaries and identification of key system components. Figure 4 shows the identification of the ETC subsystems and the inclusion of key electronic components that make up each subsystem.

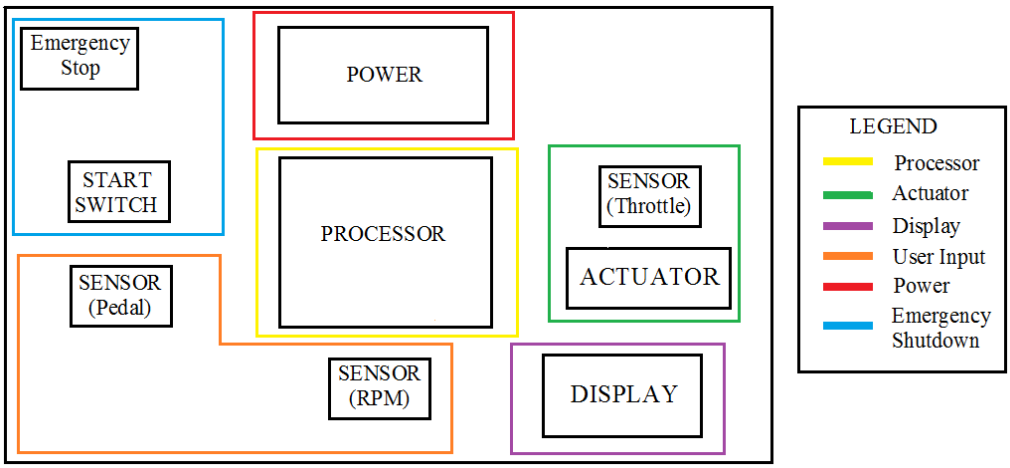

Figure 4. Electronic Throttle Control Subsystem breakdown.

Included in this initial system architecture is the Emergency Shutdown subsystem, this subsystem is a consequence of the requirements derived from the emergency cut-off and single start switch safety goals identified as necessary design inclusions during the hazard and risk assessment. The emergency shutdown subsystem is responsible for providing the user with the ability to disable the vehicles engine in the event of an emergency, while the single starter switch prevents accidental pedal activation during system initialisation therefore it is considered important safety related design characteristics to prevent or mitigate sudden unexpected or uncontrolled vehicle acceleration.

Included in the SDD is a further detailed description of the ETC systems external interfaces describing the details of external connections including plug types, wire specifications and electronic signal characteristics. Once the initial system architecture has been approved at the System Design Review (SDR), the design then progresses to the next stage of development.

B. System Design

The detailed design phase of the project involves the functional description and selection of lower level components that make up the respective ETC subsystems. The first stage of design involves the development of the systems detailed architecture with consideration for the minimum design requirements of each safety goal, to ensure the system meets the required level of reliability. Key architectures based on the redundancy, multiplicity and diversity outlined in the functional safety standards are applicable to the system, with their inclusion enhancing diagnostic coverage and increasing the systems robustness against identified hazards or unwanted events. Table 2 shows the recognised architecture techniques applicable to the system and their method of implementation within the ETC system design.

Table 2: Summary of functional safety architecture techniques

Name	Description	Implementation Method
Reciprocal comparison by software in separate processors	Comparison of the data exchanged between two processors conducted in software	Software/Hardware
Monitored Outputs	Comparison of output calculated from independent inputs	Software
Sensor Valid Range	Limit valid reading to the middle part of the sensors electrical range	Hardware Implementation
Sensor Correlation	Comparison of sensors to detect in range failures	Software
Monitoring	Monitoring actuator operation	Software (Feedback)

The combination of the functional safety design techniques aimed at increasing system reliability and basic ETC system architecture produce the overall system design shown in Figure 5.

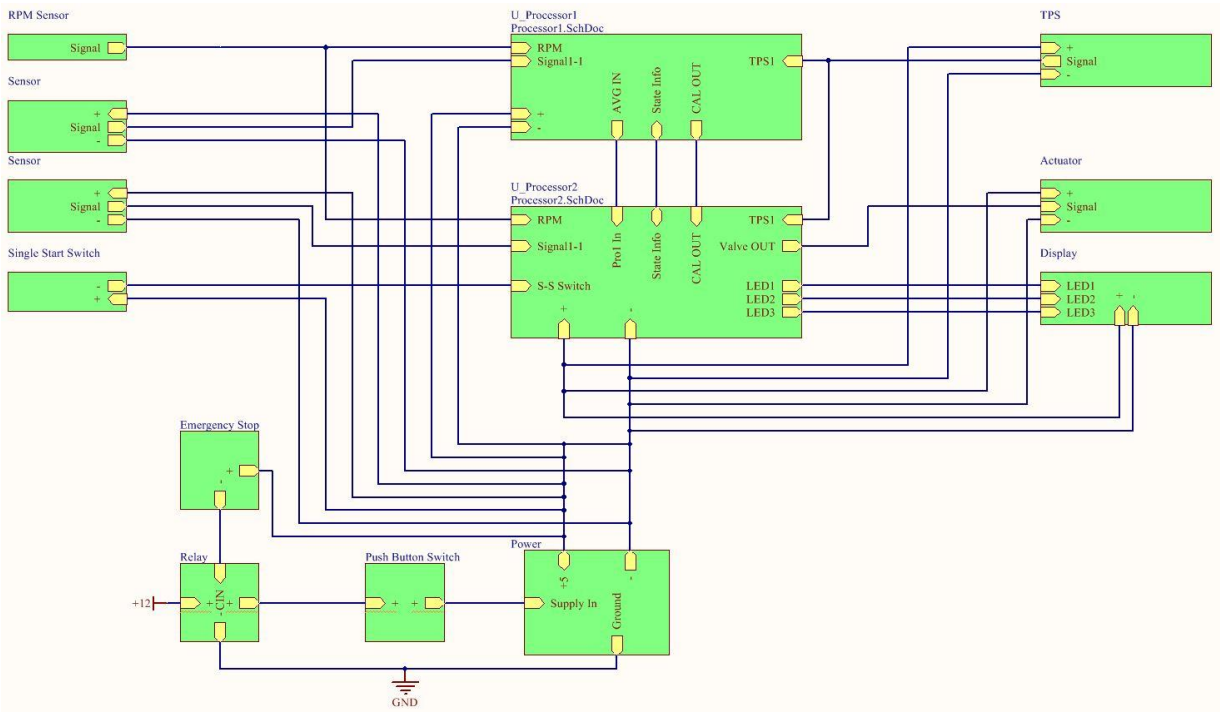

Figure 5. ETC System Schematic

After developing the detailed system architecture the next stage of system design requires the selection of subsystem design alternatives and component selection. The identification of the optimum design alternative and component selection requires the analysis of each alternatives performance against the systems functional baseline. Each subsystem has a number of alternatives suitable for the implementation of its functionality, therefore the selection of components requires consideration for the maximum performing design alternative and then the selection of the optimum components. To assist in the decision making process, a Multi Criteria Decision Analysis (MCDA) is used in the selection of the optimum subsystem design alternative and components.

The first stage in the development of a MCDA is the identification of the assessment criteria. The ideal MCDA criteria has the ability to differentiate between possible solutions while complementing the key design features of the system to ensure the accurate assessment of each alternative. Once the selection criteria has been developed, each one is assigned a weight between 1 and 25, where the highest weight is the considered most important, and the smallest weight is the least. Each design alternative is then scored relatively compared to the alternatives, with the highest score considered to have the best performance and the lowest the least for each of the respective criteria. Finally each alternatives score is multiplied by the criteria weight and added up to produce an overall score. The highest scoring alternative is considered the optimum solution.

Due to the safety critical application of the ETC system there is considerable importance placed onto the development of selection criteria motivated by the design principles of functional safety. Each criteria relevant to the safety related application of the system is assigned the highest weight symbolising its importance in overall system design.

Once the optimum design alternative for each ETC subsystem has been identified, the next stage is the selection of the appropriate components for each alternative. Again to assist in part selection, a MCDA is used where specific criteria relevant to the subsystem is developed. The highest importance is placed onto the safety related criteria identified for each subsystem.

The combination of the detailed system architecture, the process of component selection and the detailed definition of functionality for each subsystem is formally documented in the System Design Folder.

C. Reliability Analysis

At the completion of detailed design a reliability analysis is conducted on the relevant subsystems within the throttle control system. To assign an ASIL to a particular subsystem and therefore identify if it's relevant, each safety goal (Safety Related Control Function (SRCF)) is broken down broken down into a number of function blocks. A SRCF function block is a function specifically required to achieve the indentified safety goal. Once the relevant function blocks have been identified for each safety goal, the electronic component/s selected for the ETC subsystem are allocated to each function block and the component/s become a Safety Related Electrical Control System (SRECS). Each SRCF function block inherits its ASIL from the safety goal which passes it onto the SRECS. This breakdown of ETC safety goals assigns a safety integrity level to the relevant components within the subsystems. Figure 6 provides an overview of the progressive assignment of ASILs to respective ETC system components.

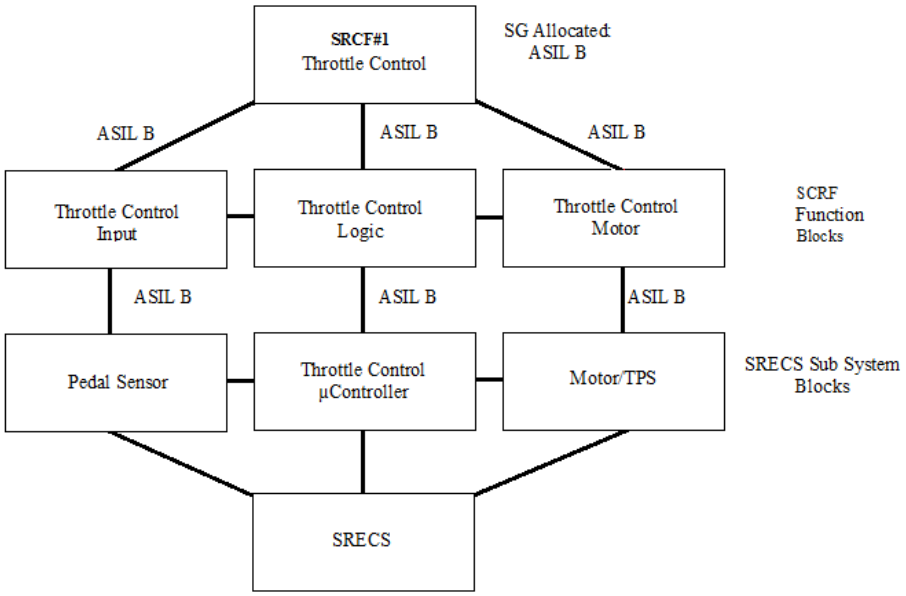

Figure 6. Safety Goal ASIL Breakdown

Once each SRECS has been assigned safety integrity level a reliability analysis is be conducted on each SRECS to theoretically verify that its design meets the minimum requirements of its ASIL. The first stage in the reliability verification process is the determination of each SRECS probability of failure. The method of calculation used to determine a SRECS probability of failure depends on its architecture and its operating mode of demand where its mode of demand defines the frequency at which the SRECS is expected to operate.

Functional safety standards have a number of documented architectures which describe the level of redundancy within a system and therefore define the calculation required to determine its respective probability of failure. The standard notation for functional safety architecture is for example 1oo1 which represents a simple series system with no redundancy therefore if '1 out-of 1' components fail the system fails (Punch p. 74). Other examples of documented safety architectures include but are not restricted to 1oo2, 2oo2 or 2oo3 also taking into account for diversity, architectures such as 1oo2D form part of the documented architectures within functional safety standards.

The mode of operation for the safety goals within the ETC system are considered as high demand with the exception of safety goals 1 and 4 which are low, continuous mode safety goals such as safety goal 2 are considered as high demand. The probability of failure for a high demand safety goal (i.e. one used continuously or often frequency during ETC operation) is a measure of the Probability of Dangerous Failure per Hour (PFH) and is directly proportional to the number of dangerous undetected failures (Punch, p. 74). For a low demand mode safety goal (i.e. one used not often during ETC operation) the output is a measure of the Probability of Dangerous Failure on Demand (PFD) which, depending on the SRECS architecture is a standard formula taking into account time intervals and both the dangerous detected and dangerous undetected failure rates.

Table 3: ETC System safety goal 2 reliability parameters

SG Number	SRECS Identifier	Method of Implementation	SG Description	FS Architecture	Demand Mode
2	2.1	E/E/PE	Sensor	1oo2	High
	2.2		Processor	1oo2	High
	2.3		Motor	1oo1	High
	2.4		Throttle Position Sensor	1oo1	High

Once both the architecture and the mode of operation have been defined for each safety goal (as shown in Table 3) the failure rate, ratio of dangerous to safe failures and level of diagnostic coverage for each component within a SRECS is determined. For the ETC system, the failure rates for respective components can be deduced from relevant reliability standards, the ratio of safe to dangerous failures is an assumption made under the guidance of functional safety standard AS61508. The level of diagnostic coverage is defined by the hardware design standard ISO26262-5 for each architecture technique implemented during detailed design. The safe to dangerous failure ratio defines the number of safe and dangerous failures from the overall failure rate, a dangerous failure is one considered to place the EUC into a hazardous or unwanted situation. Diagnostic coverage refers to a components ability to automatically detect an internal failure and is usually expressed as a percentage to allow the calculation of the number of detected and undetected failures. Once all the relevant parameters have been determined, a standard formula based on the SRECS architecture and mode of operation is used to determine its respective PFH or PFD and from the respective probability of failures an appropriate ASIL can be determined.

To combine the SRECS of each safety goal and therefore theoretically verify the safety integrity level of each safety goal the Reliability Block Diagram (RBD) analysis method is used as recommended by AS61508. Due to complexity of the ETC system, each SRECS can be characterised by one of the standard functional safety architectures, therefore allowing the combination of each safety goals SRECS to be simple series connections as shown in Figure 7 for the throttle control safety goal. To determine the overall probability of failure in a series connection it requires the addition of each SRECS PFD or PFH to calculate an overall probability value and to then determine an appropriate ASIL for each safety goal.

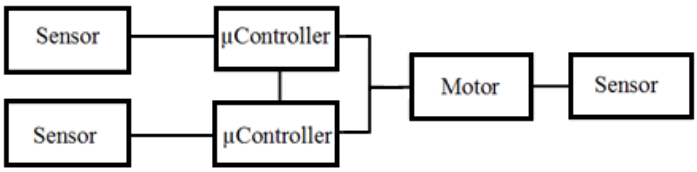

Figure 7. ETC system safety goal 2 Reliability Block Diagram

The result of the systems reliability analysis provides the theoretical verification of the design to show that the ETC system meets the minimum reliability requirements of each safety goal and its assigned ASIL. Each safety goal in the ETC system theoretically achieved the minimum requirements from the reliability analysis for its respective ASIL summarised in Table 1. The reliability analysis marks the completion of detailed design and is formally documented in the SIL verification report.

D. Acceptance Testing

Once detailed design has been completed and the reliability of the system has been theoretically determined, the system can move into production. In order to verify that the system achieves to both the performance and reliability targets outlined during conceptual, design Acceptance Testing and Evaluation (AT&E) will be conducted on the assembled product. The AT&E procedures for the ETC system consist of both functionality and reliability verification procedures.

Firstly to verify functionality and performance, test procedures are constructed from the verification statements assigned to each system requirement. Each verification statement describes a method of verification and a brief description of the process. From each statement, a detailed methodology can be developed to verify that the assembled product meets the functional and performance conditions set by each requirement.

Secondly to verify of the reliability characteristics of system components, the actual reliability data is obtained through operational evaluation of each component. Usually the data can be obtained from the manufacturer and is gathered through continuous monitoring of many replications of the same component to measure the failure characteristics over its lifetime of operation. Other evaluation techniques like proof testing are used to provide an initial estimate of reliability performance as the component is subjected to conditions well beyond the normally expected operating envelope to accelerate operational failures. Is the results of these tests are then scaled to reflect the expected reliability for normal operation.

V. Conclusion

System design for safety related applications includes additional layers of design rigor and verification to all levels of product development to ensure any E/E/PE components remain in a safe state in the event of component failure. The design and development of the ETC system for the ADFA Formula SAE racing team has provided maximum exposure to the concepts of functional safety and safety related engineering. The inclusion of the safety lifecycle as a framework for ETC system development provides the foundations for a detailed understanding of safety related design and verification for a system with specific reliability requirements. The design of a safety related E/E/PE control system has architectural design influences at the system and subsystem level, requiring significant consideration during the selection of components. The extent to which a system design is effected by its safety related application depends on the critically of its implementation which is identified during the EUC hazard and risk assessment. The higher the risk associated with an E/E/PE control system failure the greater system development is impacted to ensure compliance with the minimum reliability requirements.

VI. Recommendations

Recommendations for possible future work within the context of this project include the construction and verification of an ETC system with the safety related architectural recommendations made during this project. Further research into safety related system design could be conducted into performance enhancing functionality available to the racing car with the implementation of ETC. Some examples include, advance throttle mapping and Electronic Stability Control. Finally the integration of the ETC into future the SAE racing cars for use once approved by competition regulators.

Acknowledgements

Firstly thank you to my project supervisor Dr Ian Faulconbridge for his expert guidance and advice which has enhanced both my technical and professional mastery. Secondly I would like to thank Marcus Punch for his specialist assistance in the field of functional safety and system design for safety related applications. And finally thank you to my parents and close family, without their love and support none of this would have been possible.

References

Books:
Punch, M 2013, *Functional Safety for the mining & Machinery Based Industries,* 2nd edn, Marcus Punch Pty. Ltd., Tenambit NSW.
Faulconbridge & Ryan, R & M 2005, *Engineering a System: Managing Complex Technical Projects,* Argos Press, Canberra Australia.

Journal articles:
Safety Research & Strategies, Inc 2009, 'Sudden Unintended Acceleration Redux: The Unresolved Issue', *The Safety Record,* vol. 6, no. I3.

Newspaper & Magazines:
Bensinger & Vartabedian, K & R 2009, 'New details in crash that prompted Toyota recall', *Los Angeles Times,* 25 October.
Vlasic & Apuzzo, B & M 2014, 'Toyota Is Fined $1.2 Billion for Concealing Safety Defects', *The New York Times,* 19 March.
Hagon, T 2012, 'When car electronics go wrong', *Drive Australia,* 15 February.

International Standards:
International Organization for Standardization, ISO 26262, *Road vehicles-Functional safety Part 1 'Vocabulary' 2011(E*).
International Organization for Standardization, ISO 26262, *Road vehicles-Functional safety Part 2 'Management of functional safety' 2011(E*).
International Organization for Standardization, ISO 26262, *Road vehicles-Functional safety Part 3 'Concept Phase' 2011(E*).
International Organization for Standardization, ISO 26262, *Road vehicles-Functional safety Part 4 'Product development at the system level' 2011(E*).
International Organization for Standardization, ISO 26262, *Road vehicles-Functional safety Part 5 'Product development at the hardware level' 2011(E*).
International Organization for Standardization, ISO 26262, *Road vehicles-Functional safety Part 6 'Product development at the software level' 2011(E*).
Department of Defense, MIL-HDBK-217F, *Reliability Prediction of Electronic Equipment, 1995.*
Australian Standard, AS 61508, *Functional safety of Electrical, Electronic / Programmable Electronic Safety-related Systems Part 2 'Requirements for electrical / electronic / programmable electronic safety-related systems' 2011.*
Australian Standard, AS 61508, *Functional safety of Electrical, Electronic / Programmable Electronic Safety-related Systems Part 3 'Software Requirements' 2011.*
Australian Standard, AS 61508, *Functional safety of Electrical, Electronic / Programmable Electronic Safety-related Systems Part 6 'Guidelines on the application of AS61508.2 and AS61508.3' 2011.*

Rules:
SAE International, *Formula SAE Rules, 2013.*