Hazard Analysis for Mechatronics:

Formula Electric Vehicle Control System

Team 28, Controls Freaks
Abhishek Magdum
Dharak Verma
Jason Surendran
Laura Yang
Derek Paylor

October 20, 2022

Table 1: Revision History

Date	**Developer(s)**	**Change**
Oct 19, 2022	Dharak Verma, Abhishek Magdum, Laura Yang, Derek Paylor, Jason Surendran	Initial Revision

Contents

List of Tables

1 Introduction

The automotive industry comprises arguably one of the most safety-stringent engineering fields. Numerous stakeholders contribute to this phenomenon - national (and international) government entities producing region-specific safety requirements, industry bodies (eg. SAE, ISO) maintaining guidelines, and consumer demand for safety performance and features. There is also a history of safety-related scandals in this industry, most notable the Ford Pinto and Takata Airbag case studies. Fundamentally, motor vehicles are highly complex systems with many failure modes, where the consequences of failure are extreme due to the sheer energy inherent to heavy machines moving at high speeds.

Our project, developing a FSAE Formula Elecrtric vehicle control system, inherits some of these concerns, though the scope of hazards is greatly reduced due to this being a competition-only vehicle following strict SAE hardware safety guidelines.

For our purposes, a Hazard is present when a combination of system and environment conditions has the potential to cause harm.

2 Scope and Purpose of Hazard Analysis

The purpose of the Hazard Analysis is to identify critical considerations where hazards may arise. Consequent effects, the failure modes/reasons, mitigation ideas, and resulting safety requirements are to be addressed.

Out of scope hazards primarily consist of hardware reliability concerns, and specific hardware failure modes that are already self-managed. There are several fail-safe systems already in place at the hardware level as per SAE competition rules, such as battery contactor emergency-stops, cell voltage management systems, etc.

3 System Boundaries and Components

The "system" that is refereed to in this document, consists of the following components:

- Simulink Model Components
    1. Mode Selection Ring
    2. Cooling Control Ring
    3. Accumulator Management Ring
    4. Tractive Motor Ring
    5. Vehicle Dynamics Ring
- Version Control (Git)

4 Critical Assumptions

One critical assumption that our control system will be based off is that the required FSAE rules/guidelines are pre-vetted for being safe and functional. Internal testing for our control system will be conducted for baseline safety but features must still follow the FSAE rules. Since the FSAE rules are applied to all formula teams, with similar rule sets being used in the past, it is unlikely such rules will be invalid. Moreover, our system will assume basic hardware reliability. Our responsibility on the FSAE team is to produce software. The software is assumed that it can be run successfully on the target embedded hardware, which should communicate successfully with the upstream and downstream hardware components in the system.

5 Failure Mode and Effect Analysis

Table 2: Failure Mode and Effect Analysis Table

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
Vehicle Dynamics	Invalid torque requests to AMK motor controllers	Unintended vehicle acceleration or deceleration	a. Erratic pedal sensor inputs to control system, causing unintentional commands to motor controllers b. Simultaneous acceleration and break sensor inputs to control system, with inputs being sampled in incorrect order due to driver not releasing one pedal before depressing other	a. Filtering of pedal sensor data before issuing of torque requests to motor controllers b. Prioritization of break sensor inputs over acceleration sensor inputs	a. SR1	H1-1
Thermal Management	Cooling fans and pumps are not ramped up/down with thermals of the accumulator and motors	Accumulator or motor drives overheat, potentially causing thermal runaway	Control system logic incorrectly handles thermistor sensor inputs and fails to send appropriate command to ramp up cooling system	Create default logical case to fall back on in event of unknown thermal state, where fans and pumps are set to maximum safe operational levels	a. SR2	H2-1
	Cooling system ramps up too fast, causes low voltage battery to brown out	Vehicle startup sequence fails due to electrical and embedded hardware not receiving required power	a. Initial thermistor sensor readings trigger edge case in control logic, setting fans and pumps to max load b. Thermistor sensor readings are outside bounds, causing unknown behaviour	a. Ignore thermistor sensor readings during vehicle startup sequence, set hardened values for cooling system until remaining electrical and embedded hardware is initialized b. Create default logical case to fall back on in event that thermistor sensor readings are rational bounds	a. SR2	H2-2

6 Safety and Security Requirements

SR1	The control system shall prevent unsafe or erratic operation of the vehicle's propulsion and breaking systems
Rationale	Unintended vehicle acceleration or deceleration can cause the driver to lose control and result in a potential accident.

SR2	Cooling control shall ensure that the accumulator and motor drives stay within safe operational temperatures
Rationale	If the accumulator or motor drives operate at temperatures outside their specified ranges, both vehicle performance and driver safety will be compromised.

SR3	The control system shall filter the pedal input signals and monitor for erroneous signal data
Rationale	The control system needs to be aware when it is getting erroneous driver input data and proceed to a safe state

SR4	The control system shall monitor temperature sensor signals for erroneous signal data
Rationale	The control system needs to be aware when it is getting erroneous temperature data and proceed to a safe state

7 Roadmap

The following safety requirements will be implemented as a part of the capstone timeline:

- SR3
- SR4

The following safety requirements may be implemented in future versions:

- Replicate signal monitoring and fault detection for all control system inputs
- Torque Vectoring to help the vehicle stay on its intended path based on driver input