ENGINEERING AND TECHNOLOGY UNIVERSITY

Energy Engineering

CYBERSECURITY ANALYSIS OF AN ELECTRIC VEHICLE BASED ON ITS PERFORMANCE

THESIS TO OBTAIN THE BACHELOR DEGREE IN ENERGY ENGINEERING

MANUEL EDUARDO MAR VALENCIA

Code: 201410143

Advisor:

Julien Noel

Lima – Peru

August 2018

The thesis
CYBERSECURITY ANALYSIS OF AN ELECTRIC VEHICLE BASED ON ITS PERFORMANCE
Has been approved by

[Nombres y apellidos del Presidente de Jurado]

Julien Noel

[Nombres y apellidos del Tercer jurado]

Dedication:

This research is dedicated to my parents and family who has always been with me.

ACKNOWLEDGMENTS

I wish to acknowledge the following people for their help in this research

- Julien Noel for his help in all areas of this research
- Alissa Gilbert for being clear and concise in all aspects cybersecurity issues
- Eric Dietz for giving me the opportunity to work in his laboratory.
- Ximena Guardia for her limitless corrections and observations

CONTENT

LIST OF TABLES

Page.

LIST OF FIGURES

Pág.

RESUMEN

El presente estudio trata de responder las preguntas ¿qué tan vulnerables son los vehículos eléctricos ante una eventual penetración de sus comunicaciones y cuál sería el efecto en sus sistemas físicos y principales parámetros? Para responderlas, fue necesario tener un vehículo eléctrico físico, el cual fue provisto por el laboratorio Integrado de Tecnología Inteligente Energética del Purdue Polytechnic Knoy ubicado en Indiana West Lafayette.

El mencionado vehículo no posee todas las características de un vehículo moderno; no obstante, se asemeja a uno, ya que posee un motor eléctrico, un sistema de celdas de batería y lo primordial para un análisis de ciberseguridad, un controlador que recibe y envía mensajes en formato CAN bus, protocolo utilizado en casi todos los vehículos modernos. La instrumentación utilizada consta de diferentes tipos de software para la recolección de datos, análisis y comprobación de hipótesis.

Los resultados arrojaron varios comentarios respecto a lo frágil que puede ser un motor eléctrico y su controlador una vez decodificados los mensajes CAN. Uno de los principales descubrimientos fue que el grado de variabilidad de los datos en condiciones normales no afecta el rendimiento del vehículo en absoluto, ya que la prueba estadística dio un p-valor menor a 0.05, el cual era límite permitido de la corriente del vehículo establecido. Otro punto a considerar fue que hubo un tiempo de 117 segundos en el que el vehículo estuvo bajo eficiencias por debajo del 60% en condiciones normales. Además, cuando se varió la frecuencia del motor entre 60 y 80Hz (en condiciones inestables) hubo una reducción del 4% de eficiencia del vehículo, este experimento fue muy útil para saber que un Variador de Frecuencia no solo puede mejorar la eficiencia sino también disminuirla. Hay que recalcar finalmente que los límites de trabajo de la batería o motor una vez cambiado del original, puede disminuir drásticamente su vida útil, acortando la vida del vehículo per se.

Palabras clave: vehículo eléctrico, ciberseguridad, decodificar.

ABSTRACT

Electric vehicles have become a very important technology for transport, however, the analysis of their cybersecurity has been little studied by manufacturers and universities.

This study tries to answer the questions: How vulnerable are electric vehicles to an eventual penetration of their communications and what would be the effect on their physical systems and main parameters? To respond to this investigation, it was necessary to have a physical electric vehicle which was provided by the Purdue Polytechnic Knoy electric vehicle laboratory located in Indiana West Lafayette. The aforementioned vehicle does not have all the characteristics of a modern vehicle, however, it resembles one since it has an electric motor, a battery cell system and a CAN bus protocol in the controller, which is used in almost all modern vehicles. The instrumentation used consists of different types of software for data collection, analysis and hypothesis testing.

Results show several comments about how fragile an electric motor and its controller can be once the CAN messages have been decoded. One of the main findings is that the degree of variability of the data under normal conditions does not affect the performance of the vehicle at all, since the statistical test gave a value less than the p value established. Another point to consider is that in 117 seconds the vehicle was under efficiencies below 60%, which generates high power losses in the vehicle.
In addition, when the engine frequency was changed between 60 and 80Hz (in unstable conditions) there was a 4% reduction in vehicle efficiency,
this experiment was very useful to determine that a frequency converter can not only improve efficiency but also decrease it. Finally, it must be emphasized that the working limits of the battery or motor once changed from the original can drastically reduce its useful life, shortening the life of the vehicle per se.

Key words: electric vehicle, cybersecurity, decoding.

INTRODUCTION

Cyberspace is the electronic media that computers have to facilitate interaction through hardware, software and protocols for communication [1]. Every day, 3 billion people use internet according to the International Telecommunications Union [2]. Internet is a must between the companies nowadays, making them vulnerable to cyberattacks for the amount of information involved.

According to a report from the FBI from June 2016, 4000 ransomware[1] attacks occurred in United States. Diving deeper, ransomware attacks on businesses have become more frequent as well. Between January and September 2016, ransomware attacks on business increased from once every 2 minutes to once every 40 seconds according to Kaspersky [3].

Nonetheless, cyber-attacks do not occur only in the virtual medium. The physical security constituted by computers, buildings, means of transportation, electric and gas network, and so forth, is a major component. For example, the electric grid, specifically the smart grid, has already been cyber-attacked. In 2016 in Kiev, Ukraine, some hackers controlled the communications of their electric grid, shutting down relays, which caused a blackout for hours [4].

Another influential physical component are cars, mainly modern cars, which are composed of several communication protocols. Car hacking will become one of the most worried about issues in the industry in the following years, due to its rapid technological progress like the self-driving cars of many companies such as Tesla, Google and Mercedes [5]. Electric cars are a tendency now, they use the electric grid in the charging process where the physical and communication system are connected, and consequently they could be also a target of cyber-attacks, both to the car and the grid.

[1] Type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid [65]

In this context, the aim of this work is to analyze and then propose a system to protect and assure the safety of electric cars and passengers. In order to that, it will be necessary to collect data from the car and analyze it, decode the messages, apply reverse engineering and penetrate the vehicle to recognize its vulnerabilities.

The idea is to identify cyber security parameters that have to be taken into account for the safeguard of electric cars, but using a methodology that can be applied to other energy sectors that use cyber data or cyber communication for the operation of their systems. This methodology consists in recording data from the sensors of the car, the battery management system and the Curtis controller, once data is collected it has to be processed in excel and other statistic software.

Scope

This research examines, analyzes and determines the vulnerabilities of an electric vehicle constructed in the INSET lab located at the Knoy Polytechnic of Purdue University in Indiana, United States with collaboration of General Motors and The Computer Information and Technology Department.

The scope of this investigation is limited by the technology implemented in the vehicle, which has a lack of sensors and networks that reduce the complexity of the study. Therefore, the data collected and the results will be oriented only in the physical layer of the car system, which is further explained in the methodology section.

On the other hand, the data was analyzed using the different type of Software CommTool, Kvaser, SPS that record real time data of the car parameters, receiving Control Area Network (CAN) messages which are later decoded to be analyzed.

Background

The smart grid architecture, which involves electric vehicles, is vulnerable to cyber -attacks. For example, in 2007 a demonstration of the Aurora Generator Test by Idaho

National Laboratory showed that by using simple programs hackers, you could take control of a power plant’s circuit breaker and physically damage a generator [4].

On the other hand, in 2016 an attack occurred on the Ukranian electric utility Ukrenergo in Kiev, where hackers used sabotaging malware called Crash Override. Hackers exploited the weakness of the Ukranian utility’s to shut down the control relays of the utility plant and plunged the region into darkness for hours [4].

Smart grid infrastructure use communication protocols like Ethernet, LAN, RS485, etc. to ensure the grid [6]. In the Ukrainian event, the communications were hacked by a virus and security systems did not work as expected. The mentioned protocols are communication networks that interconnect components inside modern vehicle including EVs [7] and could make those ones vulnerable for the grid and the people.

In January 2015, two cybersecurity researchers Charlie Miller and Chris Valasek demonstrated how vulnerable cars are to cyberattacks, they controlled the air conditioning, radio and windshield of a Jeep Cherokee. Charlie Miller stated after this event *“This might be the kind of software bug most likely to kill someone”* [8]. This indeed represents an issue that will possibly affect millions of cars in some years.

Moreover, in 2016 the Federal Bureau of Investigation (FBI) gave a warning about the problems that may occur in vehicles:

> *“Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy and greater overall convenience. With this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cybersecurity threats”* [9].

Modern cars have cameras, microphones, GPS, and cellular connection; therefore, they are targets for hackers. In addition of the mentioned risks, electric vehicles (EVs) have other vulnerabilities to be aware of from a charging infrastructure point of view, EVs charging is much more than a single step such as a plug-and-go procedure (process of charging an electric vehicle). Significant communication must be made between the car and the charging point to ensure that every electric car on the grid receives the required amount of energy and electricity flow. In some cases, specifically where remote EV charging is provided by using an app or credit card, financial transactions and personal data must also be managed appropriately and securely [10].

Automotive cybersecurity is a new topic, however, in the last couple of years some manufacturers such as GM, Ford and Volkswagen have promoted more conferences and research about it, making this sector more important between researchers. Autonomous vehicles have some problems the reduced security and privacy that may be vulnerable to information abuse. Services such as Onstar (GM) or tomtom can be used to manage the well control of the vehicle, both services cost around 200-600 per year.

Nonetheless, for most researchers digging deep in this topic is limited by the legal actions manufacturers can against them. Penetrate the vehicle without permission is illegal in United States. On the other hand, in Peru this research is limited by the lack of high technology in the automotive park also there is no any industrial incentive. Therefore, this would be one of the first research about this topic in Peru.

Justification and motivation

There is a lack of information on cybersecurity of EVs issues, which represents an opportunity to look for a solid proposal on this area. This research will contribute to several agents like car manufacturers, people in general and companies such as Tesla and General Motors (GM), which are currently working on this issue.

Tesla CEO Elon Musk said: *"I think one of the biggest concern for autonomous vehicles is somebody achieving a fleet-wide hack"* [11]. Meanwhile the General Motors executive Jeff Massimilla has lead a 9 months study of cybersecurity for their (GM) cars [12]; as a result, it can be inferred that it exists an important concern of automotive cybersecurity. An illustrative example are the variable-frequency drivers which are digital devices that are highly vulnerable. Any hacker can read the minimum frequency to stop machines by penetrating the network [13]. The same problem is repeated in other types of control with digital devices, except from the direct torque control, although this is not the most efficient one [14].

Finally, not only companies will be benefited, but also the scientific community by using this proposal as an approach to EVs automotive cybersecurity. Peru does not have this technology yet, but Enel and the regulatory entities are already evaluating the feasibility to implement the EVs and the Smart grid, then a complete framework needs the cyber-security section.

The methodology implemented in this document can be applied in such a variety of sectors like communications, transportation, power plants and so on. Almost all industrial processes have cyberspace networks. However, it is necessary to analyze each case individually because their vulnerabilities are not the same neither the hardware or software. For instance, the energy sector is full of SCADA systems and communications, which could be an entrance for an attacker. In addition, inside a power plant contactors or turbines can be manipulated by accessing the SCADA.

General Objective

- Analyze the cybersecurity vulnerabilities of an electric vehicle based on its performance

Specific Objectives

- Explore and analyze the vulnerabilities of an electric vehicle in terms of mechanical and electrical performance.
- Decode and access the first layer of cybersecurity. of an electric vehicle using reverse engineering
- Give recommendation and observations about the results in terms of attack mitigation.

CHAPTER I

REVIEW OF THE RELEVANT LITERATURE

1.1 Electric Vehicles: A Growing Sector

The electric vehicle (EV) market has intensely grown since the spreading of the first mass-market models [15]. In 2011 only 50 000 vehicles were sold, while in 2016 these sales reached 565 000 EVs [15]. It is estimated by the International Energy Agency (IEA), that the amount of EVs (Hybrid Electric Cars and Pure Electric Cars) will possibly reach between 40 and 70 million in stock by 2025 [16] as it is shown in **Figure 1.1**.

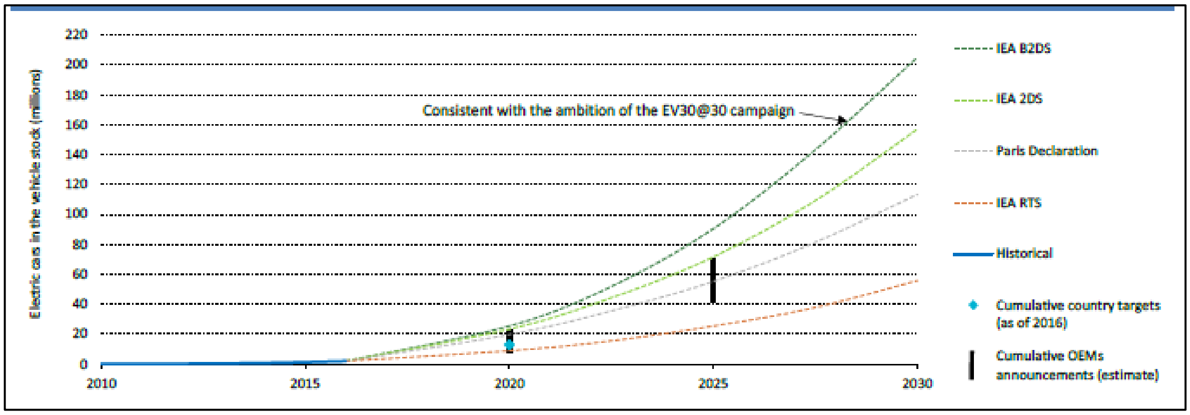


Figure 1.1 Deployment scenarios for the stock of electric cars to 2030
Source: Development of Electric Vehicle [16]

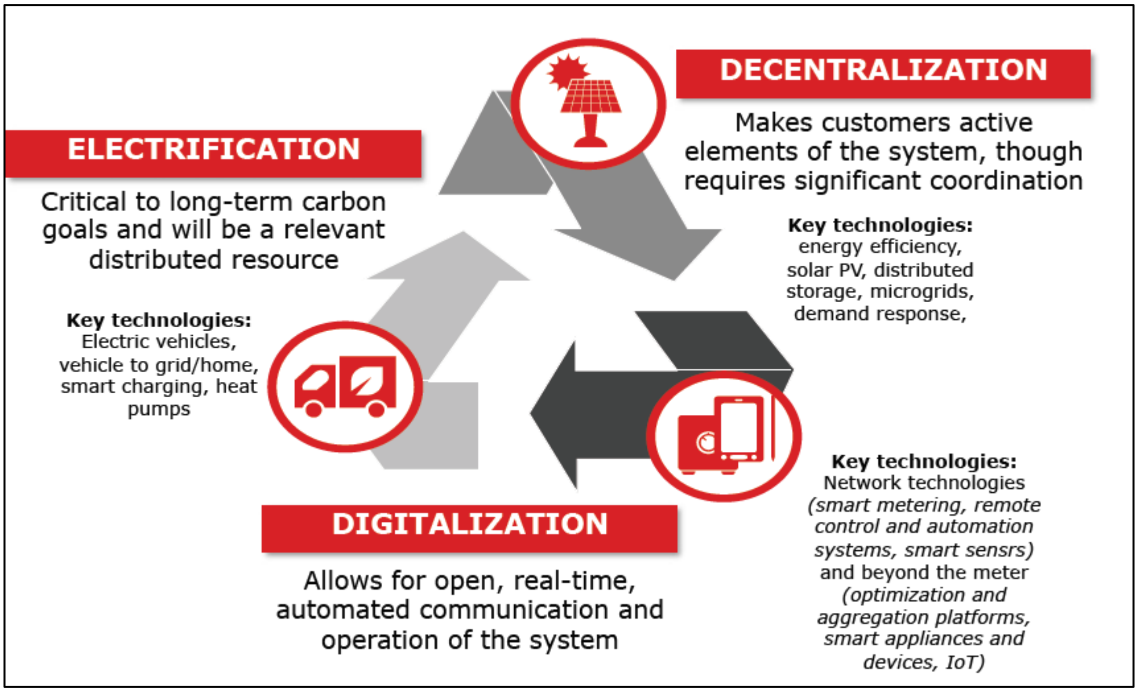
EVs are commonly divided in two groups, the hybrid-electric vehicles and the battery electric vehicles defined as:

- **Hybrid Electric vehicles (HEVs):** *"Passenger cars that draw energy for mechanical propulsion from both consumable fuels and an electric power storage device"* [17].
- **Battery-electric vehicles (BEVs):** *"Passenger cars that draw energy for mechanical propulsion solely from a rechargeable electric power storage device such as a battery"* [17].

Automakers are working on the integration of electric vehicles and the variable renewable energy. This can help by saving money on a co-marketing, installation of solar panels and storage systems. For instance, Sono Motors, a German startup, have created a vehicle that has a battery system which is partly energized by solar cells. [18]

1.1.1 Trending Sectors

According to the World Economic Forum, there are three trends that are disrupting the electric grid: Electrification, decentralization and digitalization. These trends create a virtuous cycle for long-term carbon reduction and a more reliable system. Electric Vehicles and Vehicle to Grid (V2G) are two key technologies for the electrification trend as it is show in **Figure 1.2**. Both are currently being studied and applied in many countries but OECD (Organization for Economic Co-operation and Development) countries have more advanced plans [19].



Critical to long-term carbon goals and will be a relevant distributed resource

Key technologies: Electric vehicles, vehicle to grid/home, smart charging, heat pumps

Makes customers active elements of the system, though requires significant coordination

Key technologies: energy efficiency, solar PV, distributed storage, microgrids, demand response,

Allows for open, real-time, automated communication and operation of the system

Key technologies: Network technologies *(smart metering, remote control and automation systems, smart sensrs)* and beyond the meter *(optimization and aggregation platforms, smart appliances and devices, IoT)*

Figure 1.2 Three trends of the grid edge transformation
Source: Global Electric Vehicle Outlook [19]

1.1.2 Worldwide overview

Many OECD governments are incentivizing the use of EVs by creating subsidies, tax breaks and special driving privileges. For instance, Norway offered the most expensive subsidy of 17000 euros in the region [20], which bring up successful results, as it is shown in **Figure 1.3**.

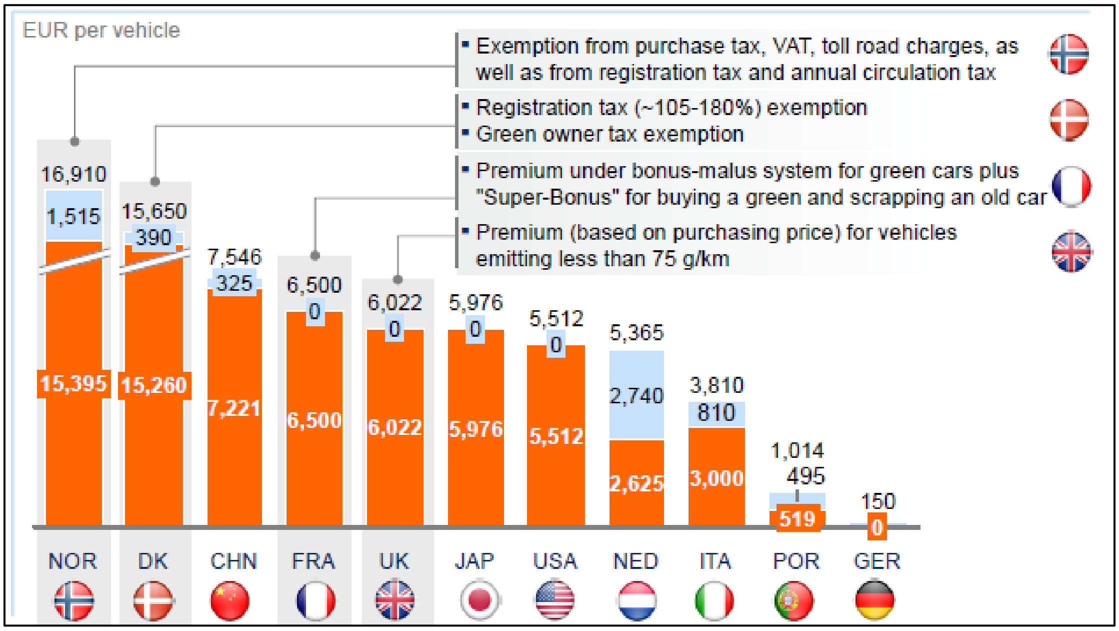


Figure 1.3 National Purchasing Subsidies
Source: European Alternative Fuel Observatory Top 5 [21]

The results for Norway are remarkable, they have 33.8 % of the EVs stock in Europe, Iceland has 9.8% and Switzerland and Sweden almost reach 4 % each one [21]. On the other hand, in July of 2017 France and UK decided to stop the sales of diesel and gasoline fueled cars by 2040. Consequently, many car manufacturers started to make plans to sell more EVs such as Volvo [22] .

Countries with big cities and with a high people density such as India and China need to work in the EVs promotion. India is in a nascent stage, the government is trying to create opportunities for Indian manufacturers but they are also creating subsidies for consumers [23].

On the other hand, China's policies have been working since 2006 by cutting taxes for HEVs, moreover in 2009 the government create subsidies of 60 000 Yuan (9000$ American Dollars) for Battery Electric Vehicles. The standards and legal framework have accompanied these policies to manage the correct promotion, besides one of the main targets for China is to reach 5 million EVs in 2020 [24]. Both countries decided in 2017 to sell only EVs by 2030 as a policy to reduce carbon emissions.

1.2 The Technology

The EVs are already a developed technology. Electronic, mechanical and electric components have had an excellent advancement the last decade. However, the principles of operation have not changed at all, the main source of energy comes from the batteries or any storage device which drives the electric motor that produce torque [25]. **Figure 1.4** shows a common architecture of Battery Electric Vehicles.

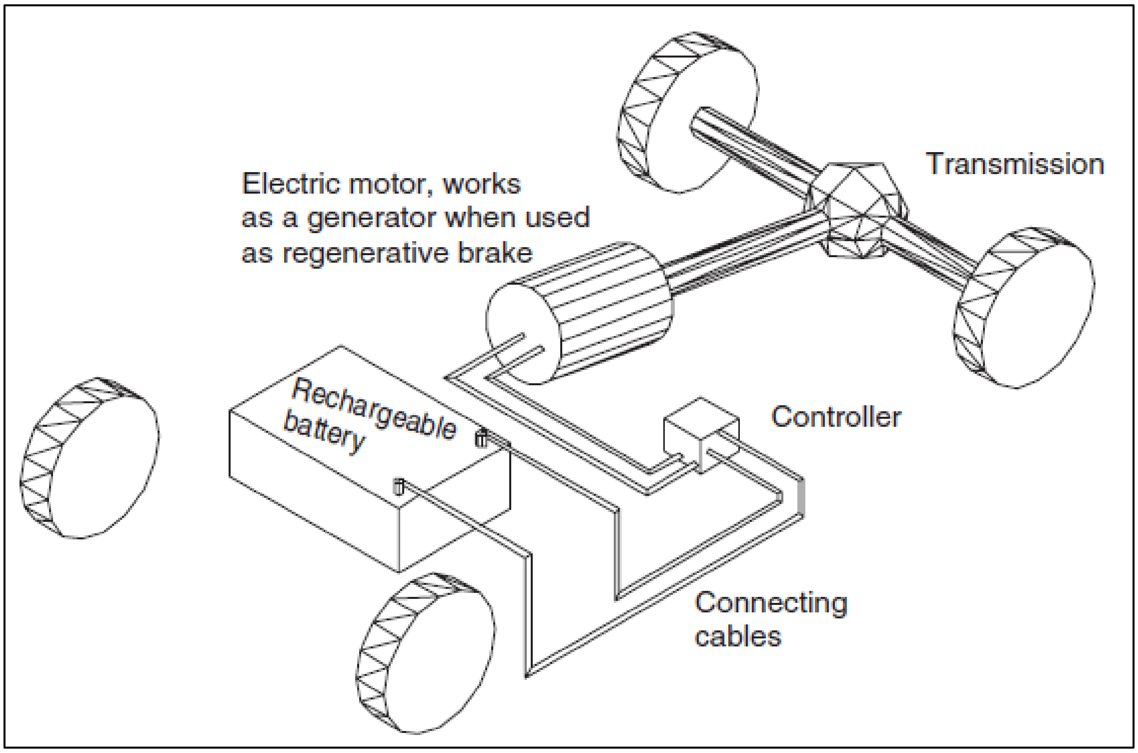


Figure 1.4 Rechargeable Battery Electric Vehicle
Source: Design Analysis and Application [14]

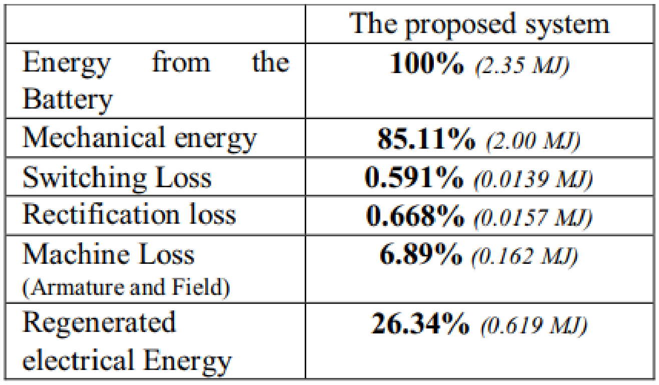
1.2.1 Electric Engine Motor

The electric engine motor is the heart of EVs, because it converts electrical energy to mechanical motion. These electric machines have been widely studied in electrical engineering, therefore the technology is highly consolidated. The requirements of electric machines for EVs are much more demanding than that for industrial applications [14]. There is a list of the requirements below:

- High torque and energy density because the vehicle needs to be as light as possible.
- Wide speed range due to rapid changes when driving.
- High efficiency over wide torque and speed changes
- Low acoustic noise. While driving, it is important to keep the limits of noise in the human range.

1.2.1.1 DC Motor

The DC Motors have been used in many EVs applications mainly because of its control simplicity. Due to efficiency, car manufacturers prefer to use AC machines rather than DC, however, using a regenerative breaking energy system efficiency of DC machines could improve significantly the energy availability. In **Table 1.1** it is shown a study of the regenerative braking system which takes advantage of 25% the energy battery [26].



	The proposed system
Energy from the Battery	**100%** *(2.35 MJ)*
Mechanical energy	**85.11%** *(2.00 MJ)*
Switching Loss	**0.591%** *(0.0139 MJ)*
Rectification loss	**0.668%** *(0.0157 MJ)*
Machine Loss (Armature and Field)	**6.89%** *(0.162 MJ)*
Regenerated electrical Energy	**26.34%** *(0.619 MJ)*

Table 1.1 Energy distribution of a regenerative breaking cycle
Source: Regenerative Breaking of Series Wound Brushed DC Electric Motors for Electric Vehicles [26]

In cities, the breaking process is more common due to traffic, as it is shown in **Figure 1.5.** The urban driving cycle has more speed changes, while the highway driving cycle does not [26].

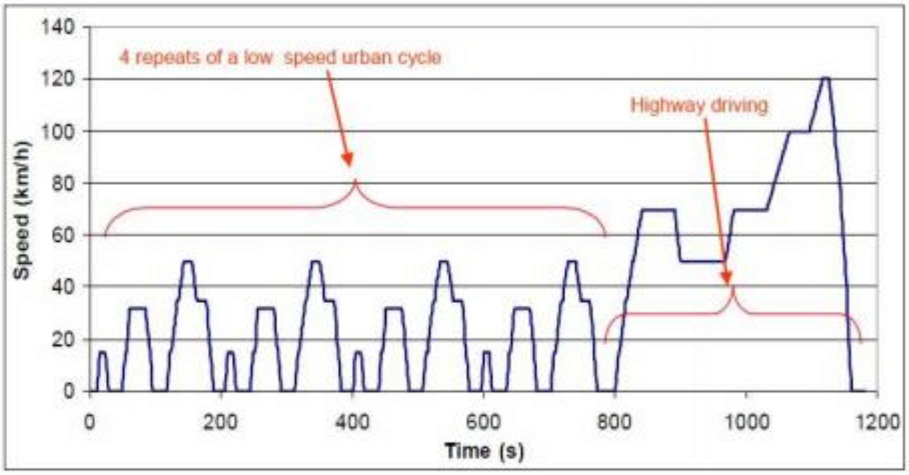


Figure 1.5 Driving Cycle in highway and urban area
Source: Regenerative Breaking of Series Wound Brushed DC Electric Motors for Electric Vehicles [26]

1.2.1.2 Permanent Magnet Drives

Permanent magnet (PM) are widely used in electric vehicles due to their high power density, high torque density, wide operating range and so on. [27]. The range of power speed is greatly influenced by the PM rotor structure and it is possible to improve the speed range by optimizing the rotor design [28]. **Figure 1.6** shows the different shapes of permanent magnet, which will affect the final characteristics of the motor, then in **Figure 1.7** these differences are shown in terms of torque and RPM.

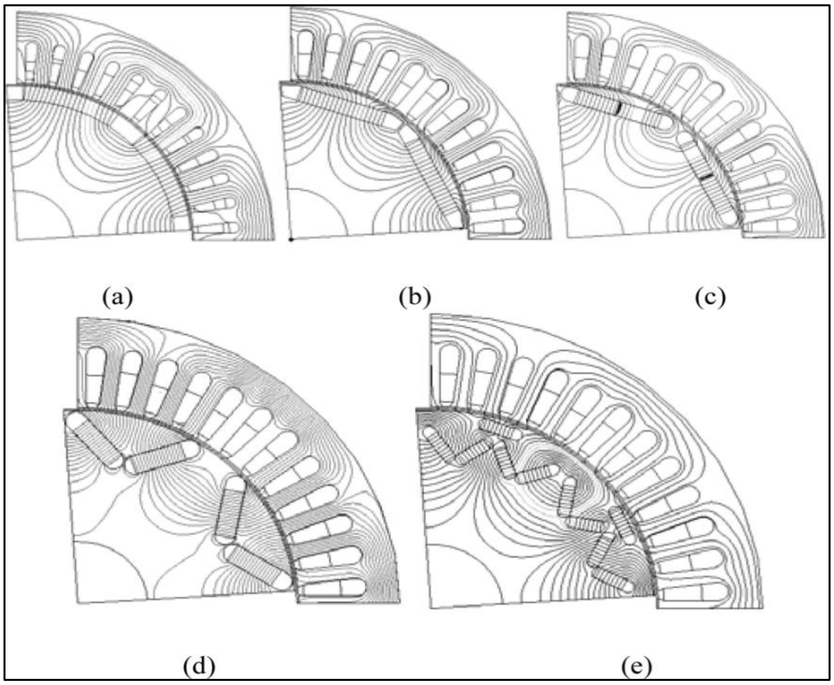


Figure 1.6 *a) surface PM motor, b) Conventional PM motor c) Segmented PM motor, d) V-shape PM motor, e) W-shape PM motor*

Source: Design and Analysis of a New Interior Permanent Magnet Motor for EVs [27]

The W-shape machine has an excellent performance in comparison with other kind of PM machines. It has a great flux weakening, high efficiency and wide speed range, so it is an optimum candidate for electric vehicles application. As it is shown in **Figure 1.7**, the torque and speed of the W-type exceeds the other types [28].

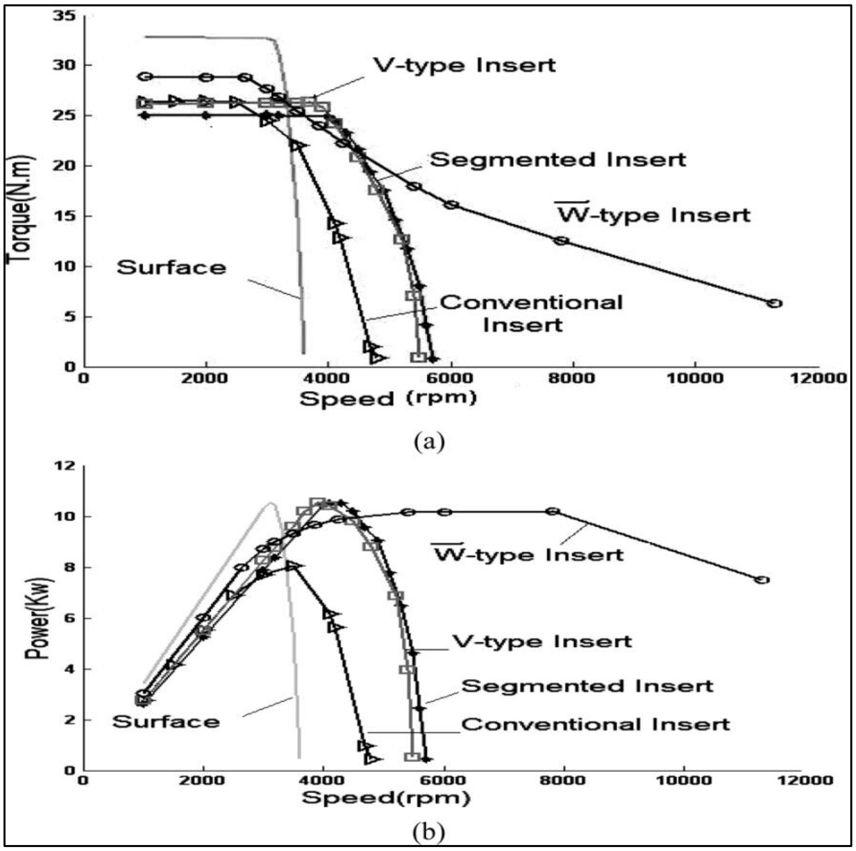


Figure 1.7 Comparison of different PM Motors
Source: Design and Analysis of a New Interior Permanent Magnet Motor for EVs [28]

1.2.1.3 Induction Motor

The induction motor, especially the squirrel cage, is the optimal motor for EVs, as they accomplish all the requirements mentioned. It has a lower cost in comparison to DC motors and a higher energy density; these advantages outweigh their major disadvantage, which is control complexity, however more power electronic to transform energy from DC to AC is required [14].

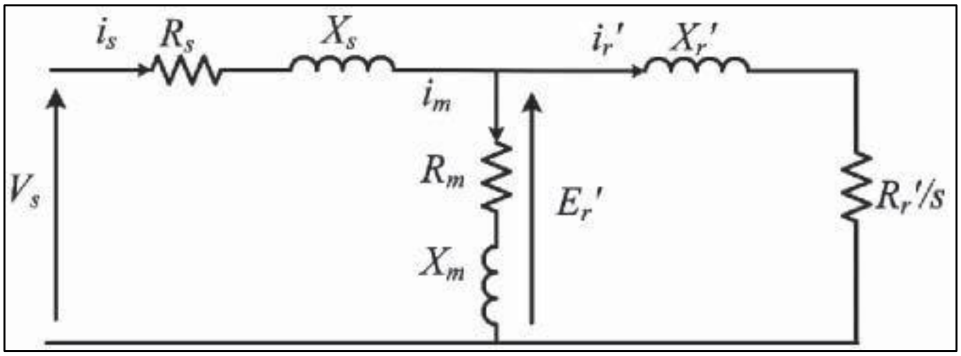


Figure 1.8 Figure Equivalent Circuit of an Induction Motor
Source: Design and Analysis of a New Interior Permanent Magnet Motor for EVs [27]

There are different types of control for induction motors such as the variable voltage, variable frequency, field oriented control and the direct torque control. The variable voltage and variable frequency are based on constant volts/hertz control for frequency to change the speed (RPM) and torque. Nowadays, almost all variable-frequency drivers are digital devices that are vulnerable because they have read and write capability. Moreover, any attacker is able to know the minimum frequency to stop machines [13]. The same problem is repeated in the other types of control with digital devices, except from the direct torque control, but this is not the most efficient one [14].

1.2.1.4 Tesla Dual Motor

By using two motors in electric vehicles, the torque can be controlled in both pair of wheels giving a digitally and independently controlling. The Tesla S (see **Figure 1.9**) is the first electric vehicle with two motors, which was released in 2015 by Tesla.

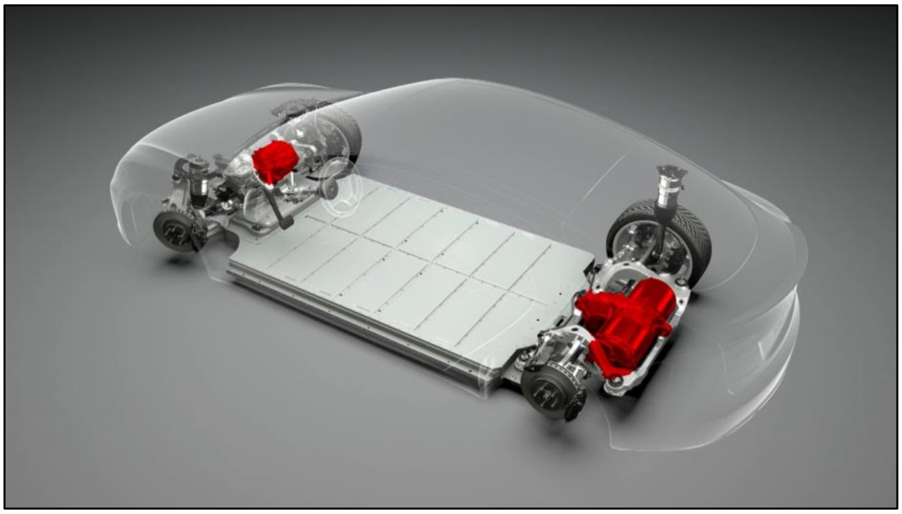


Figure 1.9 Architecture of Tesla Dual Motor EV
Source: Dual Motor Model S and autopilot [29]

This approach gives a better performance and mileage because one motor sleeps when it is no need. In addition, the specific term is idle torque and it is more efficient at different speeds [29].

1.2.2 Batteries

Electric Vehicles (EVs) are powered by stored electricity, mainly stored in batteries. There are many kind of batteries which vary by their size, energy density and other parameters depending on its construction material and technology [30]. **Figure 1.10** shows the benchmarking of the different kinds of batteries, comparing the specific energy (Wh/kg) and the energy density (Wh/l). Lithium batteries have the greater energy storage capacity in comparison to the NiMh ones, as it can be noticed from **Figure 1.10**.

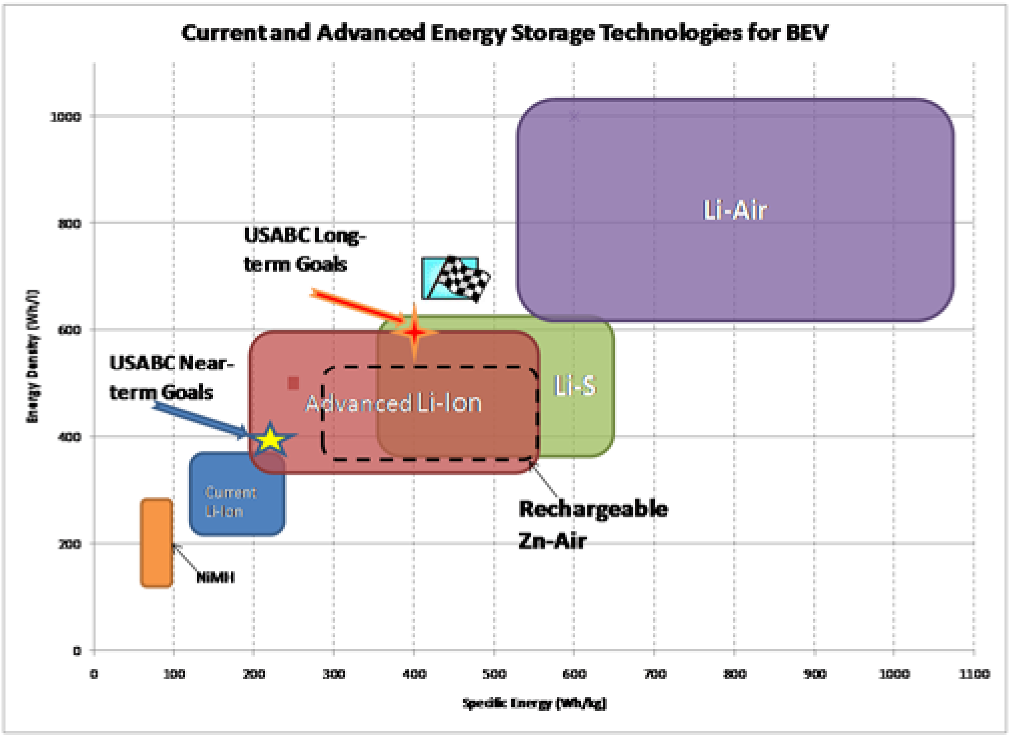


Figure 1.10 Energy density vs specific energy for energy storage in HEVs
Source: Lithium Ion Batteries [31]

- **Energy Density:** *"Amount of energy that can be stored in a given mass of a substance or system. The higher the energy density of a system or material, the greater the amount of energy stored in its mass"* [32].
- **Specific Energy:** *"The energy per unit mass of a fuel"* [31].

According to technology review, the price of EV battery per kWh in 2011 ranged from 600$ to 1100$, after five years the cost per kWh was 500$ [33]. Nevertheless, in 2016 the Energy department said that batteries should reach 100$ per kWh to make EVs competitive against fuel cars. Furthermore, Tesla CEO Elon Musk stated: *"For now, the electric-car maker is engaged in a gradual slog of enhancements to its existing lithium-ion batteries"* [34].

Latin America is a very rich area of lithium deposits. Bolivia, Chile and Peru have big reserves of lithium that can be used to develop investigation and research to manufacture EVs batteries. Furthermore, according the battery benchmarking, lithium has more potential in electric mobility and batteries in general [35].

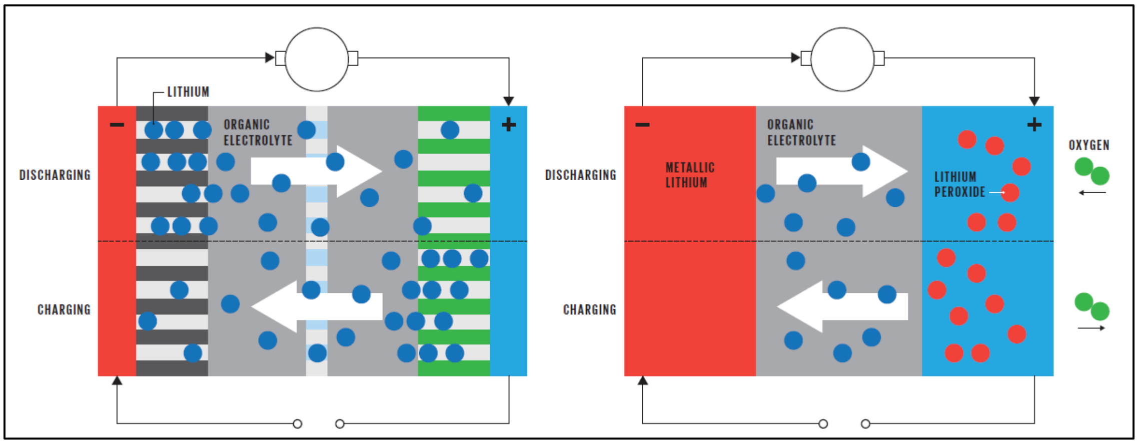


Figure 1.11 Explanation Graphic of Li-Ion (left) and Li-Air battery (right)
Source: Lithium Ion Batteries [36].

As it can be noticed from the previous figure, the Li-Ion battery puts ion inside the electrode while the Li-Air puts oxygen and lithium making them lighter [36].

Battery Monitoring

Batteries need to be managed to deliver energy in the car in the most efficient way possible. Their reasonable utilization can be improved by controlling parameters such as the driving cycle and the style of driver behavior. The actual batteries are made from several cell connected in parallel to deliver high voltages of 300V or 400V. Due to electric leakage, some of the cells may perceive unequal voltages and consequently reduce the lifespan of batteries [37].

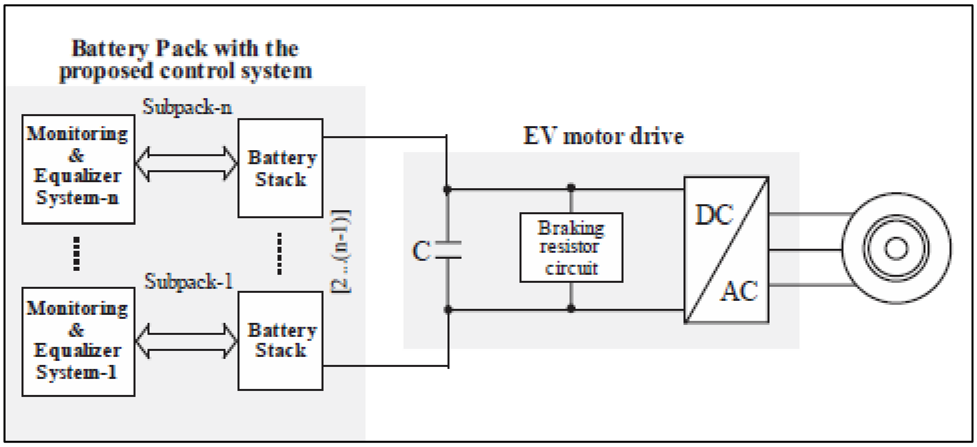

Battery Pack with the proposed control system
Subpack-n
Monitoring & Equalizer System-n
Battery Stack
Subpack-1
Monitoring & Equalizer System-1
Battery Stack
[2...(n-1)]
C
EV motor drive
Braking resistor circuit
DC
AC

Figure 1.12 Proposed control battery system

Source: Improved Monitoring and Battery Equalizer Control Scheme for Electric Vehicle Applications [37]

The approach given in **Figure 1.12** have some benefits:

- It can be supervised the main monitoring system for measuring the voltage of each cell unit of the battery stack
- Operation of the matrix power switches can be controlled
- The energy flow from the DC/AC converter to absorb energy by the battery stack and provide energy to weak battery cells, can be regulated

1.3 Cybersecurity

Cybersecurity is *"the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"* [38].

Cybersecurity is involved in all the critical sectors of society, all of these sectors are developed and digitalized. Making them an important target for attackers and vulnerable to setbacks. The critical sectors targeted by cybersecurity are shown in **Figure 1.13**.

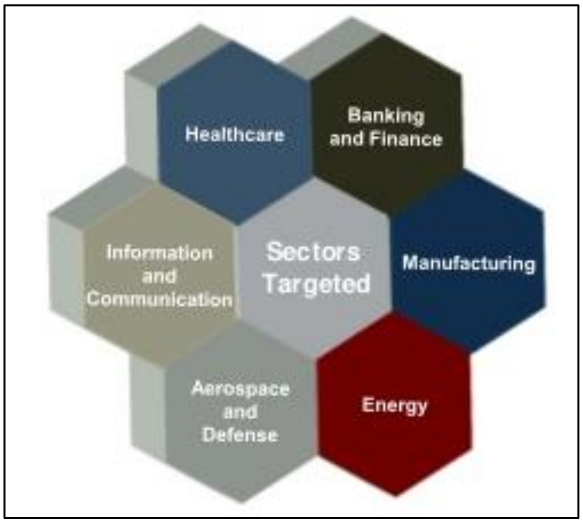


Figure 1.13 Critical Sectors Targeted by Cybersecurity
Source: Cybersecurity Innovations [39]

1.3.1 Cybersecurity Worldwide Forecast

The worldwide panorama of cybersecurity is mainly focused in a group of countries that have an established budget for this sector. Worldwide spending on information security was expected to reach $90 billion by 2017 [40], nonetheless most of the countries still do not have a budget for this sector. The following list show the spending of the leading countries in Cybersecurity by 2017.

Country	Units
US	14 billion
UK	800 million
Singapore	2.4 billion
Australia	530 million
Japan	6 billion
Germany	2014 million

Table 1.2 Cybersecurity Budget per Country by 2017
Source: Own elaboration based on [48], [1], [49], [50], [51], [52]

Even though there is a lot of money spending in cybersecurity, one problem that affect the usage of it is the lack of standards in defining, tracking and reporting incidents. Various organizations have reported various incidences as [3]:

- “Electronic attacks”, Australian Computer Crime and Security Survey (ACC)
- “Virus encounters” and “virus disasters”, International Computery Security Association (ICSA)
- “Total number of electronic crimes or network, system, or data intrusions” (CSI/FBI)
- “Security incidents” “accidental security incidents” International Specialized Book Services (ISBS)
- “Any form of security breach” (Deloitte)

In 2014, the National Institute of Standards and Technology (NIST) developed a complete framework of cybersecurity trying to solve the problem of standardization. This Cybersecurity Framework provided a *“prioritized, flexible, repeatable, performance-based, and cost-effective approach”* to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. They lead the development of the Cybersecurity Framework by [41]:

- Identifying security standards and guidelines applicable across sectors of critical infrastructure
- Providing a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Helping owners and operators of critical infrastructure to identify, assess, and manage cyber risk
- Enabling technical innovation and account for organizational differences
- Providing guidance that is technology neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services
- Including guidance for measuring the performance of implementing the Cybersecurity Framework
- Identifying areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations

In that way they will include a set of standards, methodologies, procedures, processes that align policy, business and technological approaches to address cyber risks. This framework is based in Request for Information (RFI) [41], which is shown in **Figure 1.14**, in order to collect, categorize and analyze cyber risks.

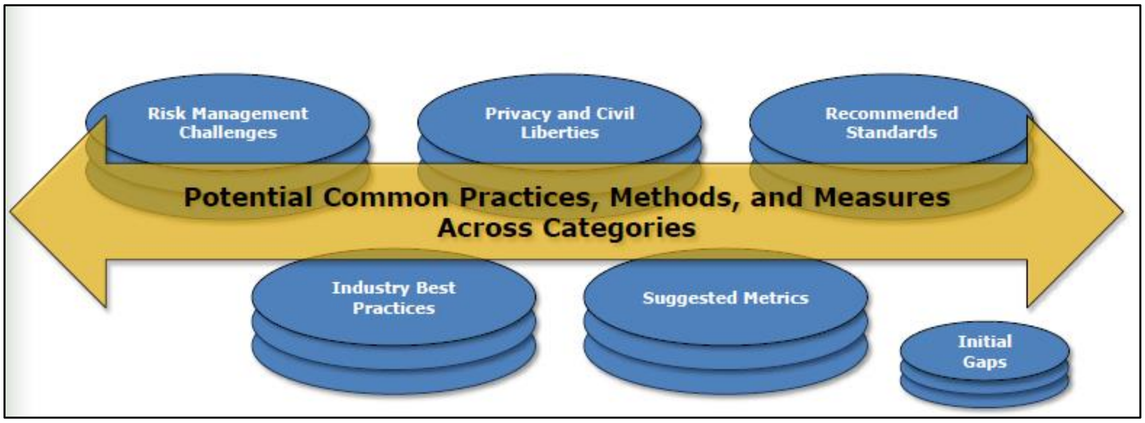

Risk Management Challenges
Privacy and Civil Liberties
Recommended Standards
Potential Common Practices, Methods, and Measures Across Categories
Industry Best Practices
Suggested Metrics
Initial Gaps

Figure 1.14 RFI Methodology
Source: Directive (EU) 2016/1148 of the European Parliament and of the Council [42].

1.3.2 Cybersecurity and Energy Sector

The constant growing of digitalization in almost every industry process gives an alert in the potential issues that can occur in the sector due to cyber-attacks. In December 2015, the European Parliament and the Council made an agreement on the Commission’s proposed measures for security of network and information systems (NIST Directive) [42].

The Commission under the lead of DG Energy is preparing a strategy on cyber security for the whole energy sector in order to reinforce and complement the implementation of Directive on security of Network and Information Systems (NIS) at energy sector level [43]. The analysis approach of this work is shown in **Figure 1.15**.

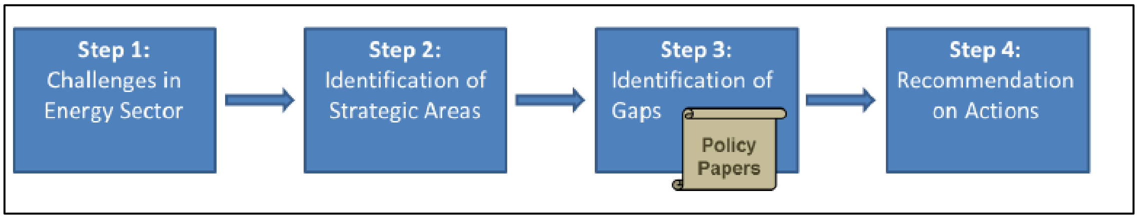

Step 1: Challenges in Energy Sector
Step 2: Identification of Strategic Areas
Step 3: Identification of Gaps
Policy Papers
Step 4: Recommendation on Actions

Figure 1.15 Overview of analysis approach
Source: Directive (EU)2016/1148 of the European Parliament and of the Council [42].

Researchers have discovered a massive new Botnet growing up a cyber-storm that could cause several issues on the internet and digitalization process. The Botnet is evolving by introducing a malware into the IP of smart devices, indeed they can be controlled remotely [44]. This is a potential issue that can generate problems in the industrial process and the energy sector (smart grid, EVs, etc.) and is being expanding for the past years, as it can be seen in **Figure 1.16**.

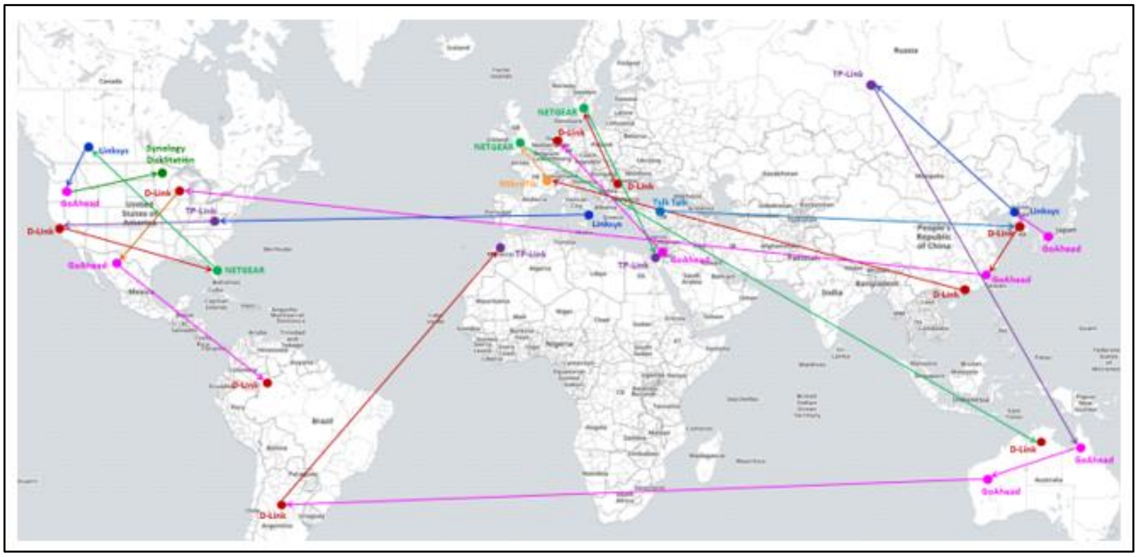


Figure 1.16 Expansion of Botnet
Source: A New IoT Botnet Storm is Coming [44].

1.4 Vehicle Communications

Nowadays vehicles have a big amount of electrical, pneumatic and mechanical components. Communication is needed between these components in order to have a proper vehicle performance [45]. For instance, when a car brakes the brake pedal has to be connected with the rear lights.

Multiplexing is the method for transferring data among distributed electronic modules via serial data bus, most of the following communication protocols are based on this method [45]. In **Figure 1.17** there is a benchmarking of the different technologies that are being used in car manufacturing. Data rate is the velocity of bits per second in the “Y” axis and the “X” axis is the cost per node. Further, in the document it will be explained the applications of each protocol according to the car needs.

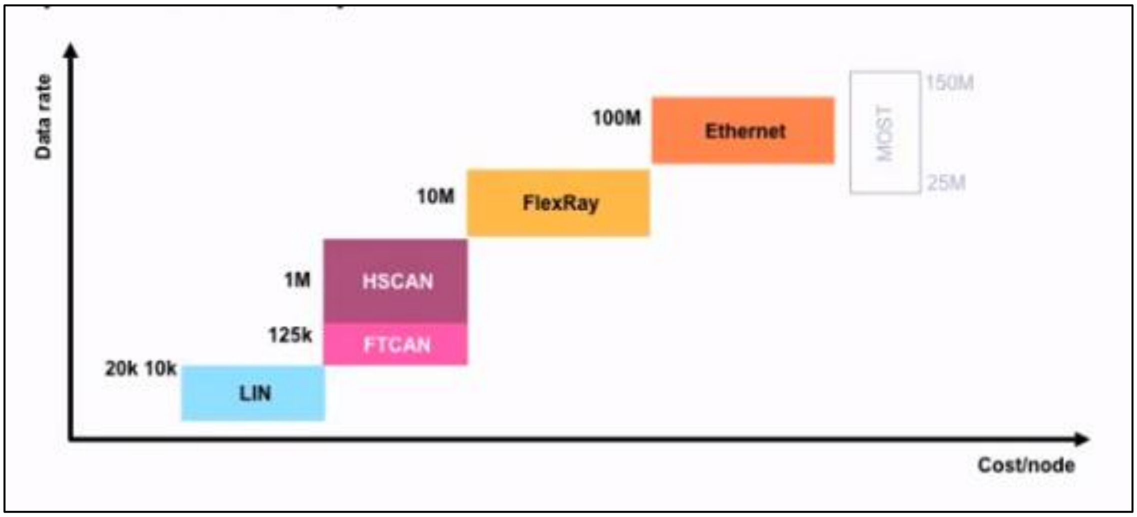


Figure 1.17 Characteristics of Vehicle Communications
Source: Introduction In-Vehicle-Networking [46].

1.4.1 Controlled Area Network (CAN)

Connect all the electronic components of vehicles is a complex duty, mainly because of the number of cables and the need of make them connected (point to point). The CAN Bus protocol, which was proposed in 1982 by Bosch, solved this issue by using a single cable that goes over the vehicle [47]. **Figure 1.18** shows how CAN Bus works, there are devices that are connected in one cable and then these devices are dominated by two 120 Ohms resistors. They are connected in two signals (CAN-low and CAN-high).

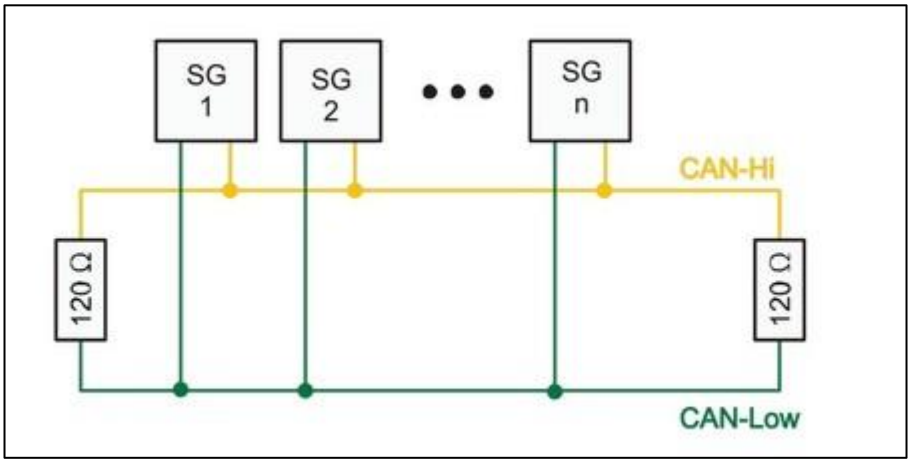


Figure 1.18 Bus CAN Simplified Diagram
Source: CAN and CAN FD bus decoding [48].

Regarding the high and low CAN are differential signals (**Figure 1.19**), the CAN high goes up to 2.5 volts and CAN low below 2.5V, both differentials gives a dominant signal which is the 0 signal, meanwhile the recessive signal is represented as 1, and it only goes in the nominal voltage 2.5 volts. The full protocol is shown in **Figure 1.20**, and it works in base of the high and low CAN, the overall process is explained in the following steps [49].

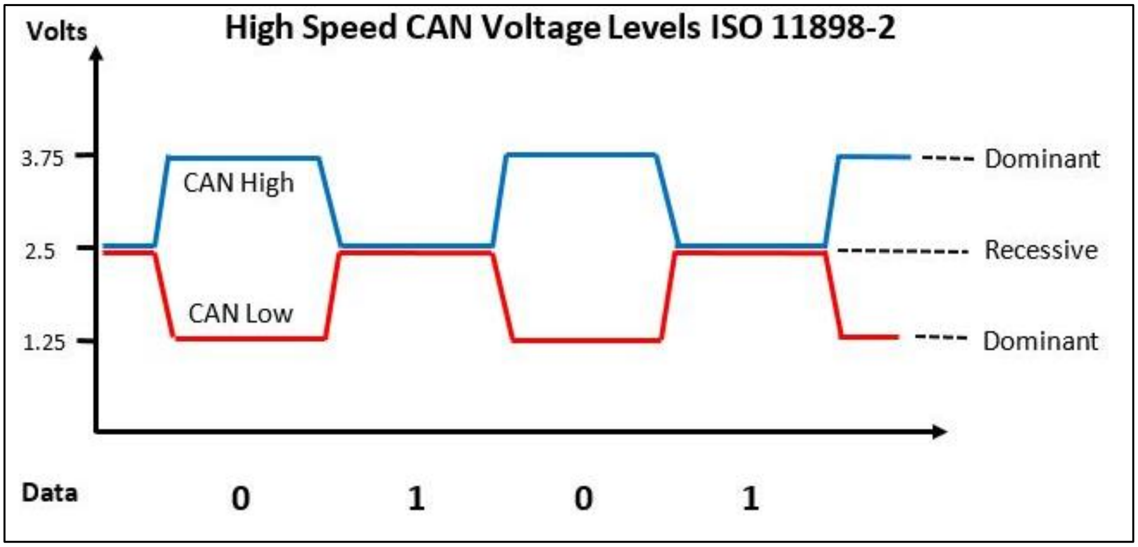


Figure 1.19 High and Low CAN voltage
Source: CAN and CAN FD bus decoding [49].

The complete protocol is explained in the following list and in **Figure 1.20** shows the correct order of the sequence [50].

1. SOF: The Start of Frame it announces to ECU (Electronic Control Unit) that a message is coming
2. Arbitration field: Indicate message Priority
3. RTR: Remote Transmission request allows ECUs to request messages from other ECUs
4. Control: Informs the length of the data 0 to 8 bytes
5. Data field: contains the actual data value which need to be convert to be readable and ready for analysis
6. CRC: The cyclic redundancy check, checks data integrity
7. Acknowledge: indicates if the CRC process is ok
8. EOF: Marks the end of the message

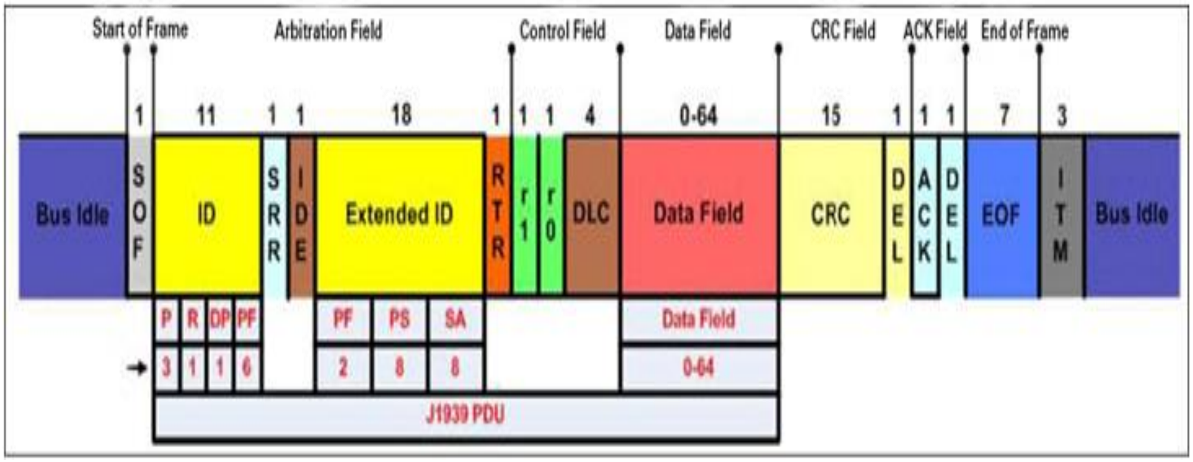


Figure 1.20 Complete CAN Communication Protocol
Source: Creating a CAN Bus Communication Platform Based on the SAE J1939 Protocol and NI PXI [51].

1.4.2 Connectivity Issues

Smart cars have many systems which connect them with the outside world and the inside car. For instance, a modern Jeep car has a system which integrates the WiFi, cellular and Bluetooth and the CAN bus.

This condition in the system was discovered by Charlie Miller and Chris Valasek, two experts in cybersecurity. They found the way to access to the CAN protocol remotely taking advantage of this condition, besides during the experience they just controlled the windshield, horn and air-conditioning system; however, they could have taken control of the brakes and even stop the engine [52].

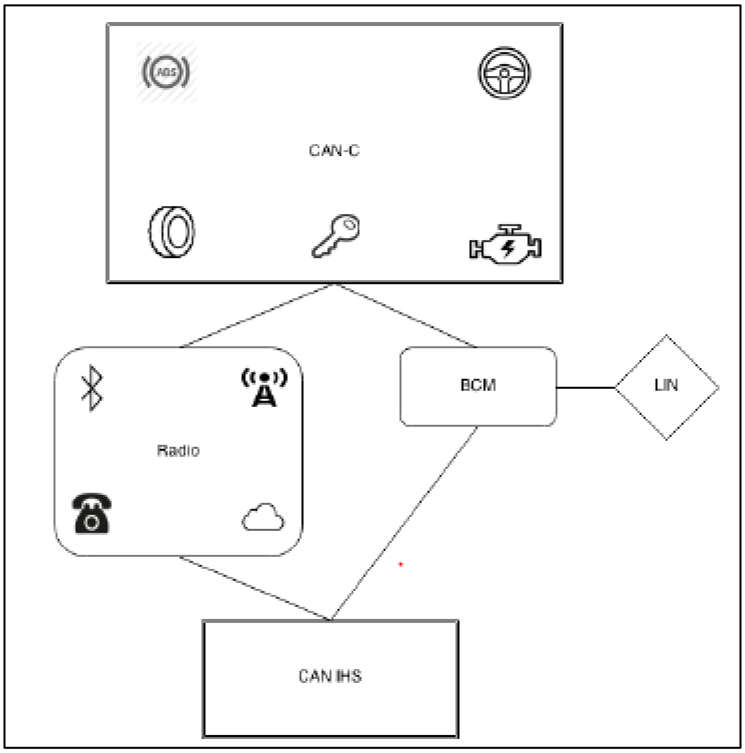
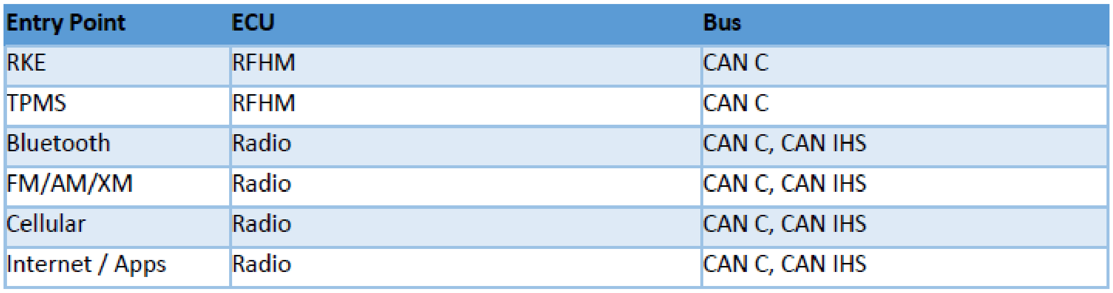


Figure 1.21 Jeep Cherokee Architecture Diagram
Source: Remote Exploitation of an Unaltered Passenger Vehicle [52].

Technically speaking, the hackers first run a code in the system by connecting their laptops to the network, then inject false CAN messages affecting the physical systems of the vehicle. **Figure 1.21** shows two CANs network, the high speed (HIS) which is directly connected with the WiFi, cellphone and the CAN-C that is connected with the engine, start on switch, etc. Miller entered first in the radio and after running the code the CAN C (Primary Bus) and HIS, were he took control of every potential entry point [52]. **Table 1.3** shows the entry points to attacks.



Entry Point	ECU	Bus
RKE	RFHM	CAN C
TPMS	RFHM	CAN C
Bluetooth	Radio	CAN C, CAN IHS
FM/AM/XM	Radio	CAN C, CAN IHS
Cellular	Radio	CAN C, CAN IHS
Internet / Apps	Radio	CAN C, CAN IHS

Table 1.3 Potential Entry Points for an Attacker
Source: Remote Exploitation of an Unaltered Passenger Vehicle [52].

As a result of the Jeep problem and the increasing of cybercrime, many manufacturers are interested in give a higher protection to their vehicles. Part of this research consists in evaluate the actual security systems and try to propose a new one to protect car against cyber-attacks [53].

It is interesting how does protection protocols work, and most of experts work and represent the issue as a military field, the attacker side is the "red team" and the defender side is the blue team. Then you need to infer the next step, the red team will start attacking to the highest risk areas that are likely to have the best chance to success, on the other hand if you belong to the blue team you will look to your risk outline and correct each threat with countermeasure [53].

Threat	Intercepts and injects commands from the cellular network
Risk	High
Attack technique	Intercept serial communications over HSI
Countermeasure	All commands sent over cellular are cryptographically signed

Table 1.4 Intercepting HSI Commands
Source: The car hackers hand book [53].

1.4.3 Local Interconnect Network (LIN)

Local Interconnect Network is a low cost multiplexed network protocol, which complement CAN unit. Due to CAN have become a prohibitive network, simple devices like the windows system, car seats, door locks are controlled by LIN [54].

LIN is a sub-bus system based on the same principle of CAN but to reduce costs. Components are driven without crystal or ceramic resonators. The master is the CAN bus and it is connected to a LIN bus network, after them there are the slaves that are the components of the LIN system, the diagram is showed in **Figure 1.22**.

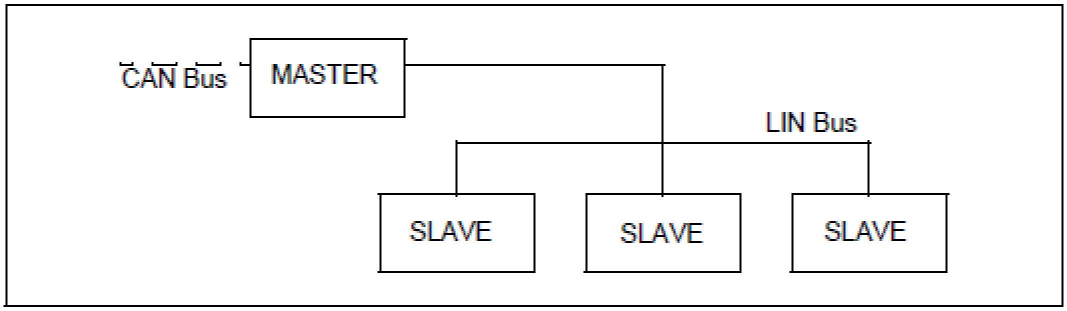


Figure 1.22 Lin Network Overview
Source: Microcontroller Division Applications [54].

1.4.4 Media Oriented Systems Transport (MOST)

Media Oriented Systems Transport (MOST) is a standard bus protocol which focused in controlling the multimedia in vehicles, the main difference from other networks is the use of optical fiber which is used because the big data is processed in all the vehicle. A MOST network must have masters for different functions, the masters can be contained in the same device. The user gives some functions to the network service, then the data is processed and finally the automated process is done by a physical interface, as it can be seen in **Figure 1.23** [55].

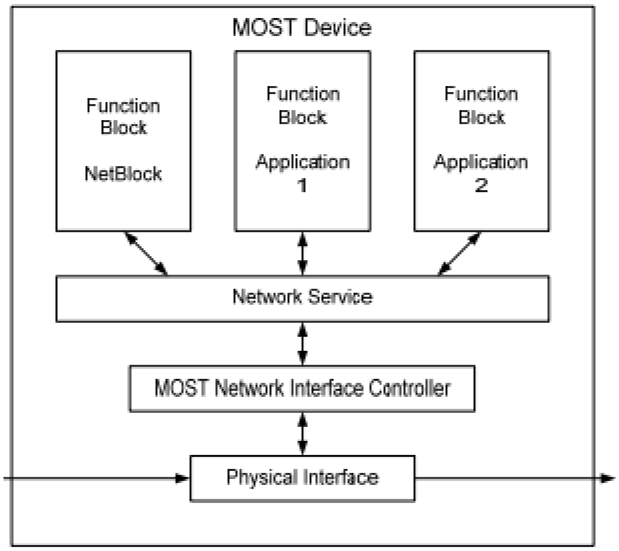

MOST Device
Function Block NetBlock
Function Block Application 1
Function Block Application 2
Network Service
MOST Network Interface Controller
Physical Interface

Figure 1.23 Model of MOST device
Source: MOST Specification [56].

CHAPTER II
METHODOLOGY

In this chapter it is explained how experiments were made for the collection and analysis of data. Experiments were executed in the INSET Electrical Vehicle Laboratory at Purdue University in the Polytechnic Department. The car tested was an electric go-kart that was used in the spring semester of 2014 for The Grand Prix race at Purdue University. Basically, the car was constructed with a motor controller, a DC battery, a Battery Management (BMS) system and other sensors that are later explained.

The methodology consisted in the development of four parts, which will be fully explained in this chapter: **Car arrangement, data collection, threat detection and mitigation, decoding and reverse engineering**. With these four steps it was possible to do all the experiments and get valuable data.

Finally, at the end of this chapter it will be explained all the needed procedures to diagnostic the car performance under distinct circumstances that can appear. In that sense, in the following paragraphs there will be explained each part of the proposed methodology.

2.1 Car Arrangement

The constructed vehicle can be classified as a BEV [17] by definition, since it is only powered by a battery and no other energy source. The main components of the vehicle and their characteristics are described in **Table 2.1**.

Components	Characteristics
Curtis AC Motor Controller 1236-5401	This controller is the main part of the vehicle or the “Brain”, because it operates almost all the processes required by the car. Most of the connections involve the Curtis controller.
Battery Management System	The battery management system is in charge of controlling under-voltage and protect the battery against short-circuits.
Manual Steering	A regular manual steering to change the car direction, which is no longer used for experimentation.
Manual Brake	Hydraulic brake which works with oil and reduces the car acceleration. It does not have any connection with the controller.
48 V DC battery	Battery of multiple cells of 48V and a capacity of 2Ah
Switch x 3	One switch to turn on the BMS, one to short the contactor and other to change reverse and forward movement in the car.
Speed Controller 840 programmer	A programmer which displays all the programming settings that can be done.
AC-9 Brushless AC Motor 1236 SE-5621	AC motor that operates at 36-60V. It can draw up to 650A producing up to 27 HP and 70 ft-lbs of torque.

Table 2.1 Test Bed of the Vehicle
Source: Own Elaboration

The car was originally designed to simulate driving cycles, however, for the purposes of this research, some artifacts as the dynamometer were not used. The arrangement of the vehicle was focused only on collecting data from all the possible ports that send relevant information like the CAN Bus messages. On the other hand, all the needed data from the race was already collected by the previous lab worker. It is important to highlight that this vehicle does not represent a real vehicle setup due to the lack of sensors and networks.

The Curtis Controller and the Battery Management System are the main sources of data and the only ones available in the car. The general scheme of the network system is shown in **Figure 2.6**, where all the components converge, but two interfaces are needed to collect data.

The car arrangement was designed to follow the type of sensors the CURTIS 1236 and the BMS can support. For instance, it was possible to put a battery indicator because at least the BMS software and hardware could send signals to it; in the other hand, it would have been useless to put a pressure monitor because the components were not designed for processing that kind data. In other terms, the components determine how much data can be gotten from the vehicle.

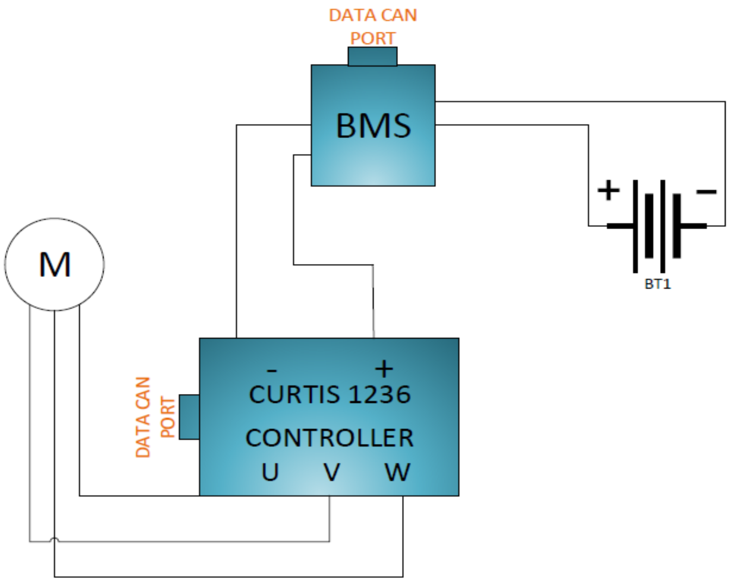


Figure 2.1 Available data ports scheme
Source: Own Elaboration

In January 2018, the vehicle was not working properly, consequently it was necessary to make some modifications. As stated in **Table 2.1**, the main controller of the car is the CURTIS 1236 controller. This component was not shorting the contactors, then no energy was being delivered from the batteries to the controller. In order to fix the problem, there were executed the following steps.

- Ask the previous laboratory worker about all the modifications that were made in the car, before early 2018.
- See the Diagnostic and troubleshooting table in the CURTIS Controller manual (Appendix 1).
- Examine the possible causes and the conditions required to repair the car.
- Fix the problem and test the car, considering the new changes made in the car.

- Write down all the observations and recommendations about the possible causes and best practices for future changes.
- If none of these measures worked, the advisor or manufacturer was able to help with the issue.

Other issues about the vehicle were found during the experimentation and repairing process. The BMS and the manual steering were part of this, but as it was listed in the last paragraph, the procedure to determine the solution of the problem was basically following those steps.

2.2 Data Collection

It was fundamental to detect all the open ports of the vehicle. It was an exercise of checking for data and control sources, for example the CAN BUS system of the Battery Management System for collecting data from batteries; the CAN BUS system of the controller; and the Vehicle Control Language (VCL) of the car. In addition, the controller had a Curtis 1311 programmer to set basic functions like the RPM or current limits.

For the purposes of this research, the data was collected from Purdue Grand Prix and the experiments were made in the INSET lab. The data collected for this research follow the below process:

- After repairing the car, it was necessary to look for all the possible communications that can be done in the car: CAN BUS for the BMS and the Curtis Controller, and the VCL just for the controller.
- Record data in tables. Classify the data between main data and secondary data by its relevance, were the main data was related to specific can messages and parameters that influence in the engine functioning.

2.2.1 Data collection from the Battery Management System

The software used to collect data from the Battery Management System (BMS) was designed by Enerdel[2]. The purpose of this component was getting real time data from the cells during all the car functioning; the voltage, current, temperature and other parameters were needed to analyze fully how the battery systems reacted to different performance scenarios.

It was crucial to focus in the security of the components; therefore, some contactors were put on the BMS to make them work safely. **Figure 2.2** *Battery Monitoring System* shows the distribution of the components, for example, the white cylindrical parts highlighted in the red circle are the contactors of both lines of the circuit. The yellow circle is the board, the input is the DC wire that comes from the battery and the output is DC current without any disturbance; therefore, it is safe to energize the Curtis 1236.

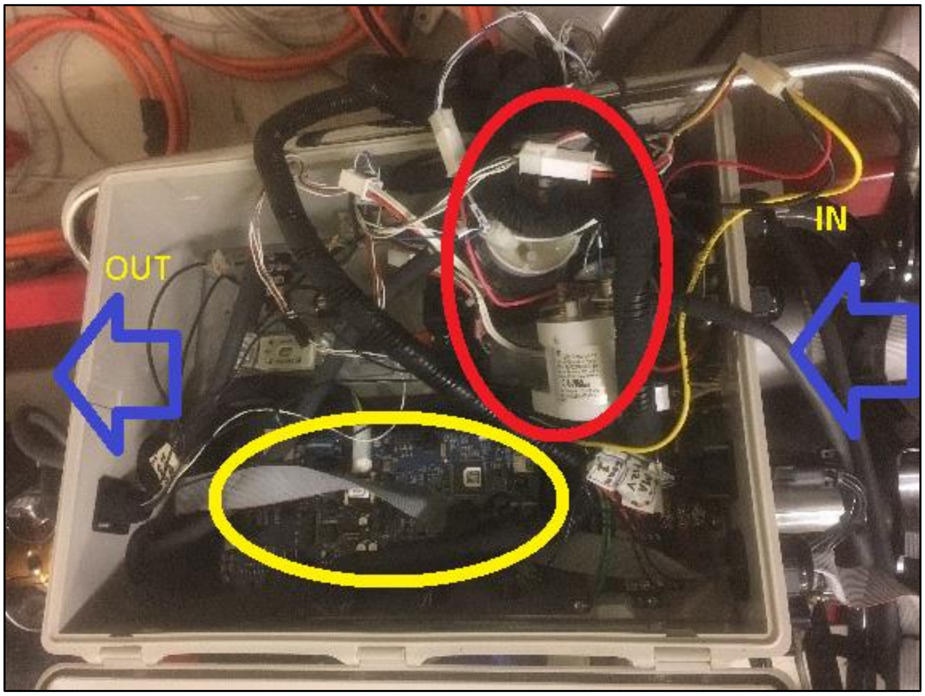


Figure 2.2 Battery Monitoring System
Source: Enerdel Inc [57].

[2] EnerDel, Inc is a designer and manufacturer of lithium-ion energy storage and battery systems.

This system used a USB-to-CAN adaptor that received real time data from the battery. This data was stored in an excel chart showing the parameters mentioned above, every time frame. The packets were CAN Bus messages, which were received and processed by the Curtis Controller.

The receiver used in the BMS was the software CommTool, while the controller did not have a determined software, which did not allow the researcher to penetrate easily the BMS.

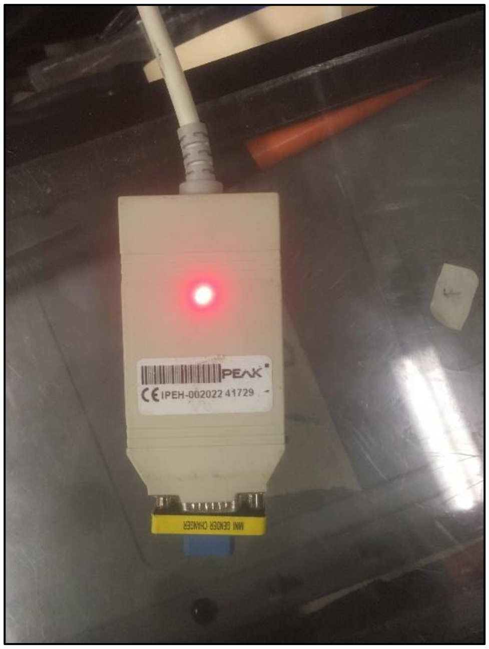
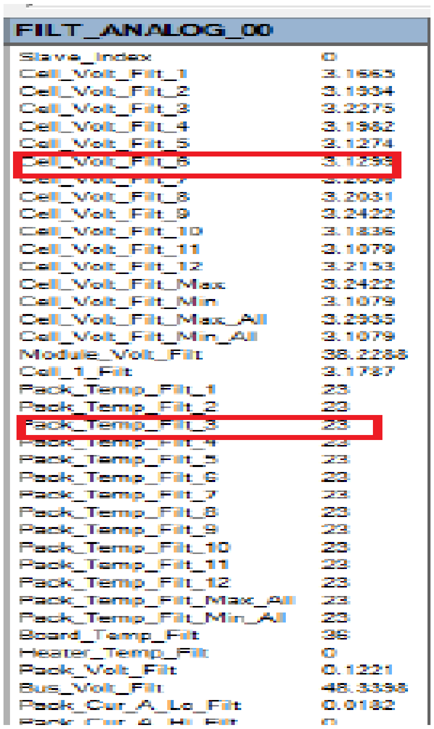


Figure 2.3 Interface CAN BUS for the BMS

The BMS had a safety roll protecting the battery from overvoltage and failures that can occur during the race or experimentation, it uses two contactors in order to protect the batteries, which are expensive. **Figure 2.4** below shows different parameters that can be obtained such as voltage, temperature of every cell, state of charge, state of health, among other items. All needed for this process was the CAN BUS for the BMS, a computer with the Commtool software and the BMS.



FILT_ANALOG_00	
Slave_Index	0
Cell_Volt_Filt_1	3.1663
Cell_Volt_Filt_2	3.1934
Cell_Volt_Filt_3	3.2275
Cell_Volt_Filt_4	3.1982
Cell_Volt_Filt_5	3.1274
Cell_Volt_Filt_6	3.1233
Cell_Volt_Filt_7	[illegible]
Cell_Volt_Filt_8	3.2031
Cell_Volt_Filt_9	3.2422
Cell_Volt_Filt_10	3.1836
Cell_Volt_Filt_11	3.1079
Cell_Volt_Filt_12	3.2153
Cell_Volt_Filt_Max	3.2422
Cell_Volt_Filt_Min	3.1079
Cell_Volt_Filt_Max_All	3.2935
Cell_Volt_Filt_Min_All	3.1079
Module_Volt_Filt	38.2288
Cell_1_Filt	3.1787
Pack_Temp_Filt_1	23
Pack_Temp_Filt_2	23
Pack_Temp_Filt_3	23
Pack_Temp_Filt_4	23
Pack_Temp_Filt_5	23
Pack_Temp_Filt_6	23
Pack_Temp_Filt_7	23
Pack_Temp_Filt_8	23
Pack_Temp_Filt_9	23
Pack_Temp_Filt_10	23
Pack_Temp_Filt_11	23
Pack_Temp_Filt_12	23
Pack_Temp_Filt_Max_All	23
Pack_Temp_Filt_Min_All	23
Board_Temp_Filt	36
Heater_Temp_Filt	0
Pack_Volt_Filt	0.1221
Bus_Volt_Filt	48.3398
Pack_Cur_A_Lo_Filt	0.0182
Pack_Cur_A_Hi_Filt	0

Figure 2.4 Comm Tool Software to read BMS value, voltage and temperature of one cell selected
Source: Enerdel

Figure 2.5 shows an example of the discharging process of the Battery during a race made in the Grand Prix Race, the frequency of data collection can vary depending on the accuracy of the experiment and the amount of data that the software can support.

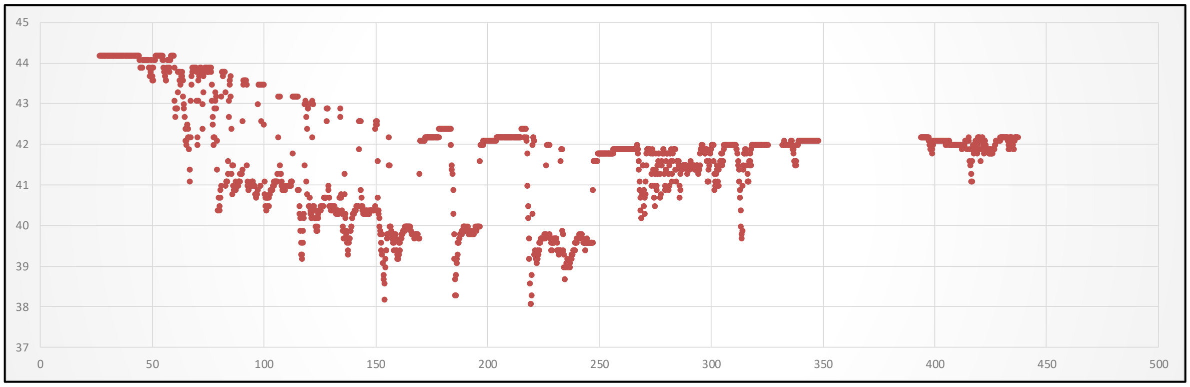


Figure 2.5 . Example of data Collected from Commtool-Battery discharging process.

2.2.2 Data collected from the Curtis Controller

There are two options when collecting data from the Curtis 1236 (**Figure 2.6**): Using the Curtis 1311 programmer (see **Figure 2.7)** directly and using the dashboard (see **Figure 2.8**), which was created in a previous research to obtain the main characteristics of the vehicle.

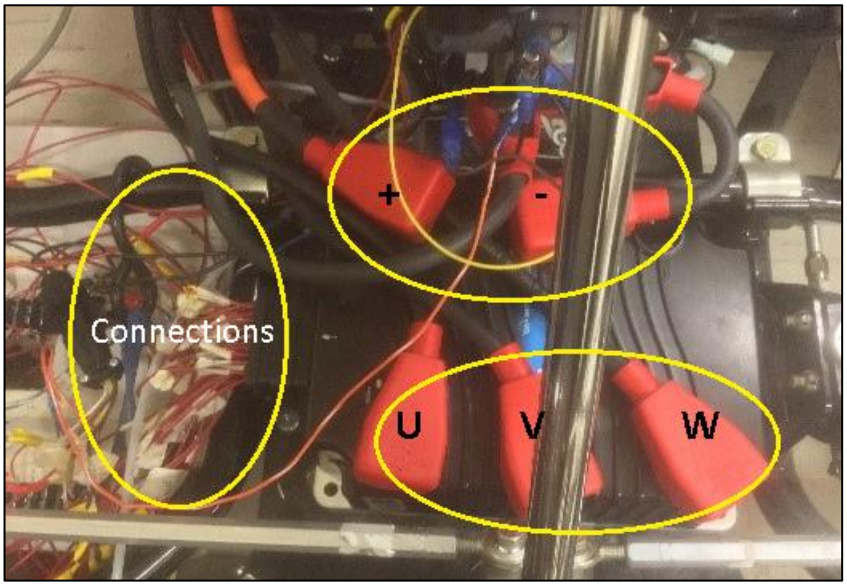


Figure 2.6 Curtis Controller Connections
Source: Curtis Instruments [58].

While it is true that it is easier to diagnostic the programmer, it is no recommended to collect data from this device because this is just a diagnosis tool. It is more suitable to use the dashboard to collect several amounts of data packets, which are exported easily by using excel or other spreadsheet software. The CAN messages were sent to the dashboard as well, however, the problem was that there were few CAN message in the car because of the lack of sensors.

At the end, for changing settings it was used the 1311 and for data collection, the dashboard. The CURTIS 1311 was used because it was simpler to manipulate. To access to the CAN network, the user only has to program the CANopen interlock with the status 5, which means operational state.

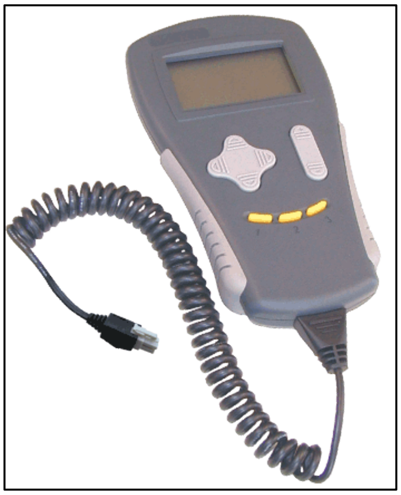
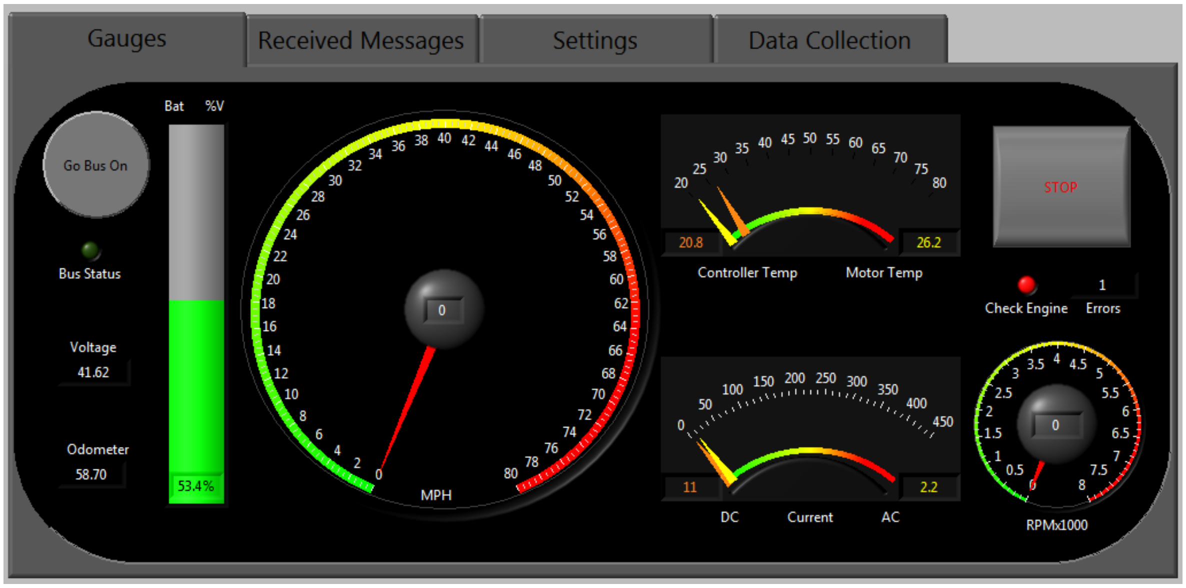


Figure 2.7 CURTIS 1311 Programmer
Curtis Instruments [58].



Voltage 41.62

Odometer 58.70

Controller Temp 20.8

Motor Temp 26.2

Errors 1

DC 11

AC 2.2

Figure 2.8 Dashboard
Source: An empirical approach to driving cycles [59].

A CAN-to-USB interface (**Figure 2.9)** was needed to transfer data from the Curtis to the computer. The receiver software used was the Kvaser CAN King (see **Figure 2.10**), a free software that records CAN messages. In fact, any software that supports CAN messages is useful, but in this case it was used the Kvaser CAN King because it is a free software.

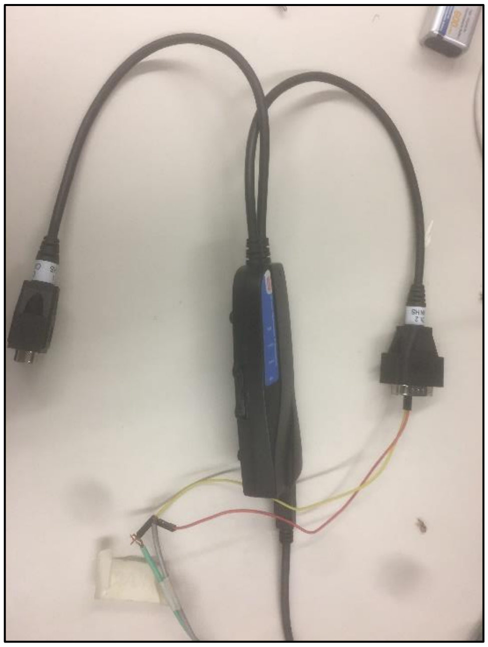
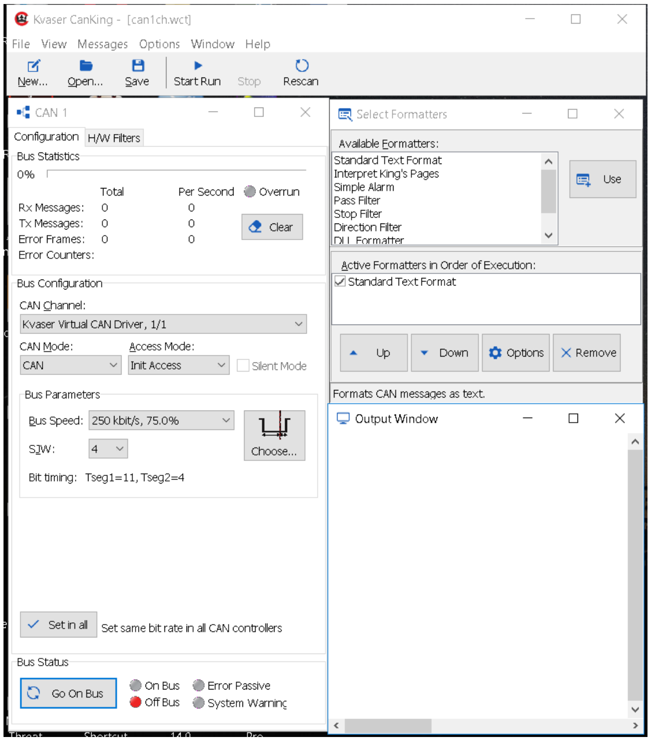


Figure 2.9 Kvaser Interface for the Curtis Controller
Curtis Instruments [58].

The Kvaser interface has two can ports that record data in real time. The reason it has two ports is because some vehicles possess more than one automotive network, like LIN, MOST or more than one CAN. For this research, just one port was needed.

Apart from this specific device, some configurations were required for the Kvaser software and the CURTIS 1236 to coincide the parameters. For instance, the rate of transferred messages (Bauds) is critical to match both the transmitter and the receiver, **Figure 2.10** shows all options that can be done.


Kvaser CanKing - [can1ch.wct]
File View Messages Options Window Help
New... Open... Save Start Run Stop Rescan
CAN 1
Configuration H/W Filters
Bus Statistics
Overrun
Clear
Bus Configuration
Bus Parameters
Choose...
Set in all
Set same bit rate in all CAN controllers
Bus Status
Go On Bus
On Bus
Off Bus
Error Passive
System Warning
Select Formatters
Use
Up Down Options Remove
Formats CAN messages as text.
Output Window

Bus Statistics 0%

	Total	Per Second
Rx Messages:	0	0
Tx Messages:	0	0
Error Frames:	0	0
Error Counters:		

CAN Channel: Kvaser Virtual CAN Driver, 1/1

CAN Mode: CAN

Access Mode: Init Access

☐ Silent Mode

Bus Speed: 250 kbit/s, 75.0%

SJW: 4

Bit timing: Tseg1=11, Tseg2=4

Available Formatters:

Standard Text Format
Interpret King's Pages
Simple Alarm
Pass Filter
Stop Filter
Direction Filter
DLL Formatter

Active Formatters in Order of Execution:

☑ Standard Text Format

Figure 2.10 Interface Kvaser-Canking Software
Source: CanKing [60].

The simplest way to manipulate the CURTIS 1236 parameters is by using the CURTIS 1311. This tool allows the user to control many settings like RPM threshold, current, voltage, kp, kd and ki controlling. All the available settings that can be changed are in the appendix. If this tool is not available, the other way to send messages to the controller is by using the Vehicle Control Language (VCL), which is the pseudocode in which the manufacturer based all the programming. In other terms, this control allows to tune the vehicle for the wanted purpose. The Curtis 1311 was used continuously to manipulate parameters such as RPM, threshold limits of voltage and current, speed modes and so on.

The previous researcher built a dashboard in LABVIEW for the vehicle in order to get easily the most critical performance parameters. **Figure 2.8** showed the setup of the dashboard. Data was received in CAN Bus messages (raw data) and then processed in charts to finally get data to be analyzed. The use of this tool simplifies data collection significantly because there is no need to repeat the race. This data was used to analyze the vehicle in steady conditions. In addition, other tests were done in the lab to corroborate the validity of data.

Due to the versatility of LABVIEW in the design process, more than one parameter can be measured during the experiments. **Figure 2.11** shows the different parameters that were gotten from the dashboard: Miles per hour (MPH), voltage, motor temperature, controller temperature, among others.

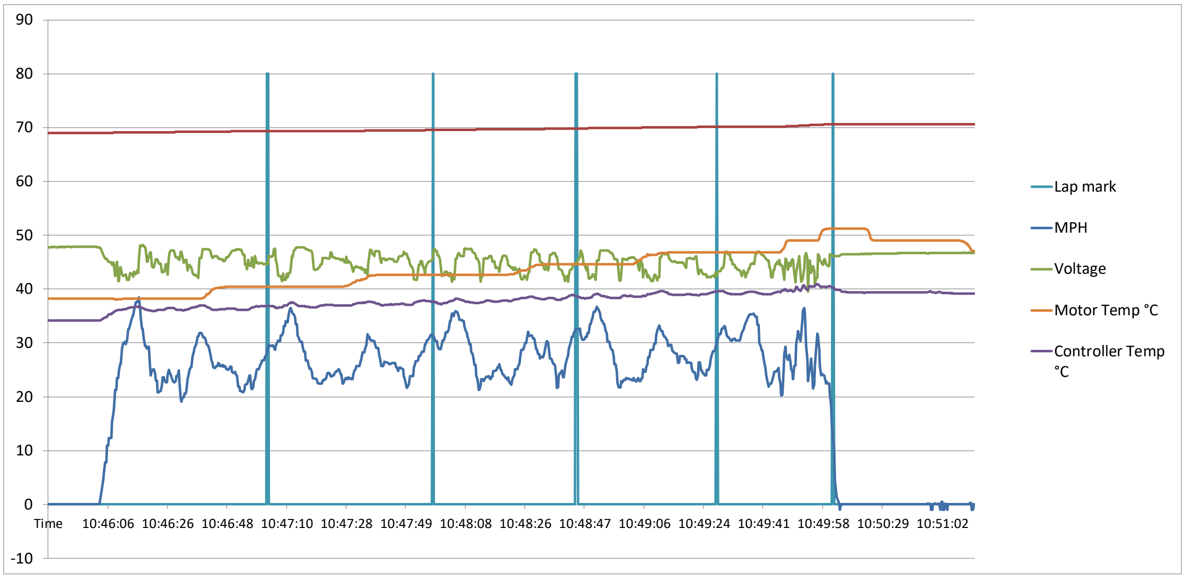


Figure 2.11 Example of data from the dashboard.
Source: Own elaboration using Commtool.

2.3 Threat Detection and Mitigation

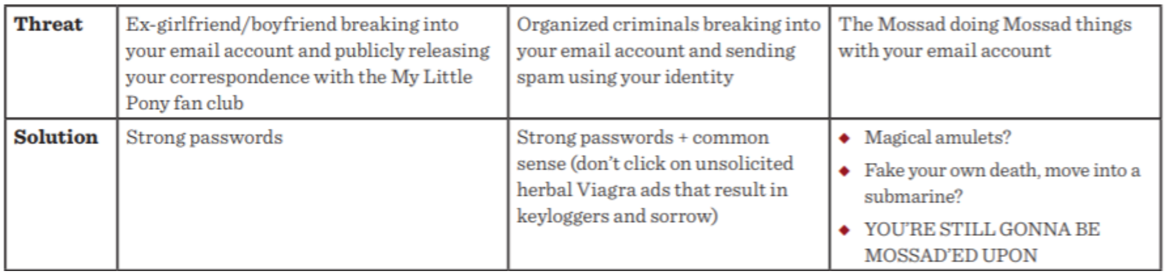
First of all, we need to define the experiments to prove the veracity of the hypothesis, which is that the car is vulnerable. In that sense, the first part consisted in testing the car vulnerability to performance attacks or failures.

For this kind of security studies, a threat model is a practical technique in the information security sector. It indicates the threat and possible mitigations to address them. Doing the threat model requires a complete analysis of the object studied, in this case the vehicle. According to Adam Shostack, a threat modeling expert, there are four basic questions to proceed with the model [61]:

1. What are we working on?
2. What can go wrong?

3. What are we going to do about it?
4. Did we do a good job?

Due to the limitations of this research, the last question was omitted because there was not any test to prove if the mitigations were good enough. In the analysis and results section, all of the rest questions will be answered. The format of the diagram is shown in **Table 2.2**.



Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Table 2.2 Threat Model Format
Source: This World of Ours [62].

Since the vehicle performance was desirable to be evaluated, electrical and mechanical tests and calculations were needed. The vehicle responses were analyzed at different paths and time frames for each parameter, and recorded during the race and the experiments made in the lab. For instance, **Figure 2.12** shows the three parameters evaluated: Revolutions per minute, number of laps and amperage. In addition, there are other factors that are influenced by the motor current like the motor efficiency, load factor, slip and so on. **Table 2.3** shows the correlations that were used to recognize the vehicle behavior in normal or steady conditions.

Title	Equation	Description
Real Power	$P_{in} = 3\, V_{ph} I_{ph} cos\theta$	Real electrical resistance power consumption in circuit
Motor Efficiency	$\eta = \frac{0.7457\ \times hp \times Load}{P_{in}}$	General Efficiency of the motor
Slip	$Slip\ = \frac{(n_s - n)}{n_s} \times 100$	This is an indicator that shows how motor is affected by different loads and forces operating in the rotor.

Table 2.3 Analyzed Equations

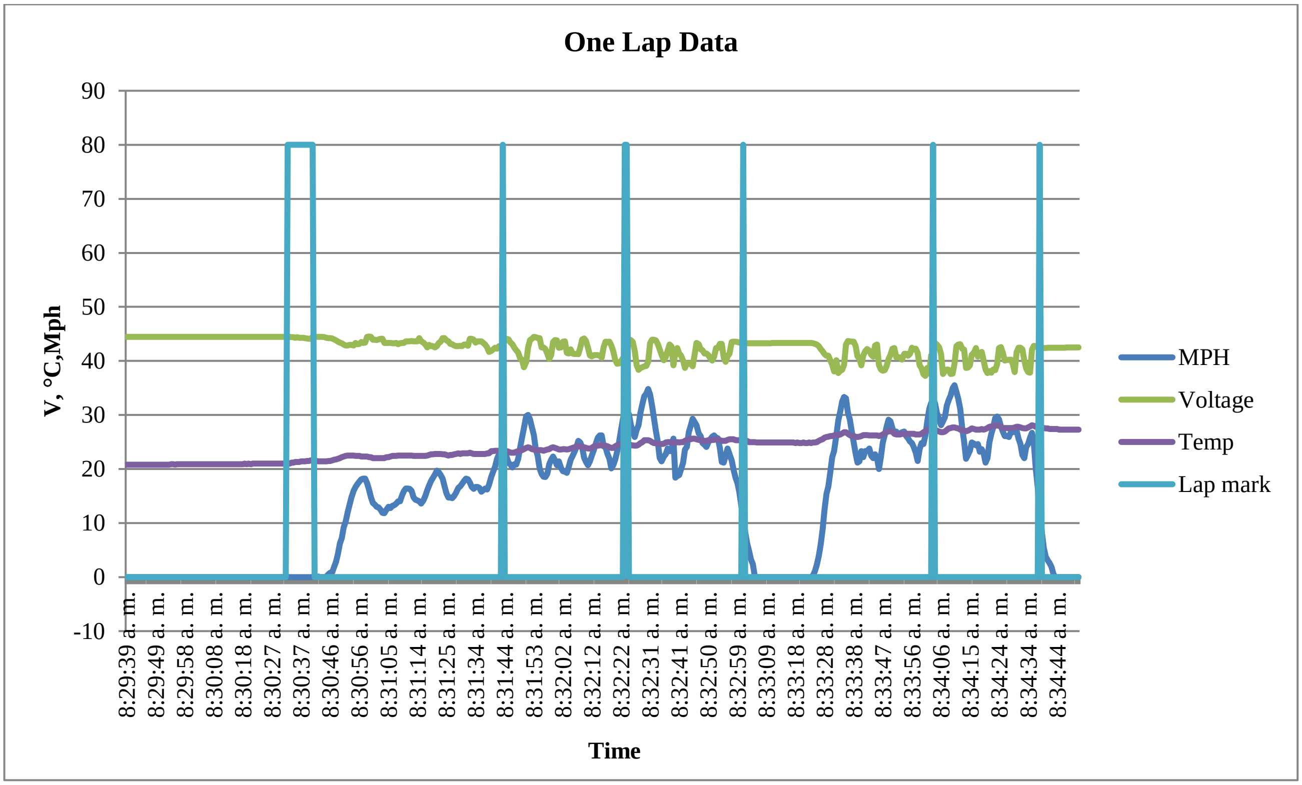


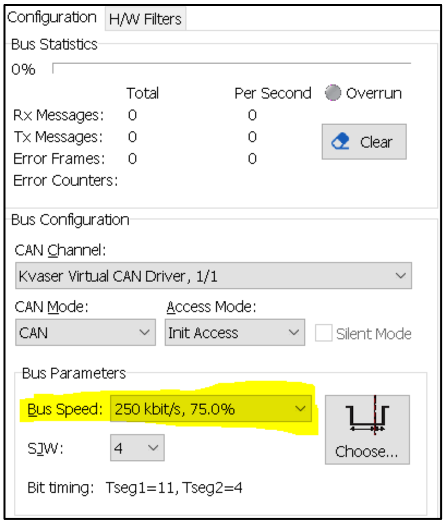
Figure 2.12 Example of data analyzed

Then, when penetration was demonstrated there had to be other theoretical tests to finally analyze the vehicle performance when is penetrated. Once some failures or threats were detected with the last penetration test, the countermeasures needed to follow stablished thresholds of the components. For example, if the motor current limit was 50A, the countermeasure had to block the changes on that specific parameter, otherwise, the motor can break because of high load.

2.4 Decoding and Reverse Engineering

In order to Penetrate the electric vehicle, it was used reverse engineering to access its first layer of cybersecurity. For doing that, it was required to access to the CAN Bus network without authorization of the manufacturer. The output of this experiment was decoding all the possible messages from the vehicle by using reverse engineering. In addition, the testing of this experiment was delimited only by the CURTIS controller, because the main vehicle operations are made by this device. The following steps were made to do this process:

- Observe the Curtis wiring diagram showed in the appendix section in ¡Error! No se encuentra el origen de la referencia. to locate the CAN bus connections and other relevant ports.
- Once located those terminals, it was needed to unlock the CAN connections. There are two ways to do the unlocking process, by using the Curtis 1311 programmer or programming the Vehicle Control Language.
- After that, some settings of the CAN software interface had to be changed, in this case, with the CANking software. For doing that, it was needed to change the bauds rate of the Curtis controller to coincide with the CANking rate (see **Figure 2.13**).
- Once all the last steps were completed, it was started the reverse engineering process and the data packets were transferred from the Curtis to the PC.



Bus Statistics

0%

	Total	Per Second
Rx Messages:	0	0
Tx Messages:	0	0
Error Frames:	0	0
Error Counters:		

Bus Configuration

CAN Channel: Kvaser Virtual CAN Driver, 1/1

CAN Mode: CAN

Access Mode: Init Access

□ Silent Mode

Bus Parameters

Bus Speed: 250 kbit/s, 75.0%

SJW: 4

Bit timing: Tseg1=11, Tseg2=4

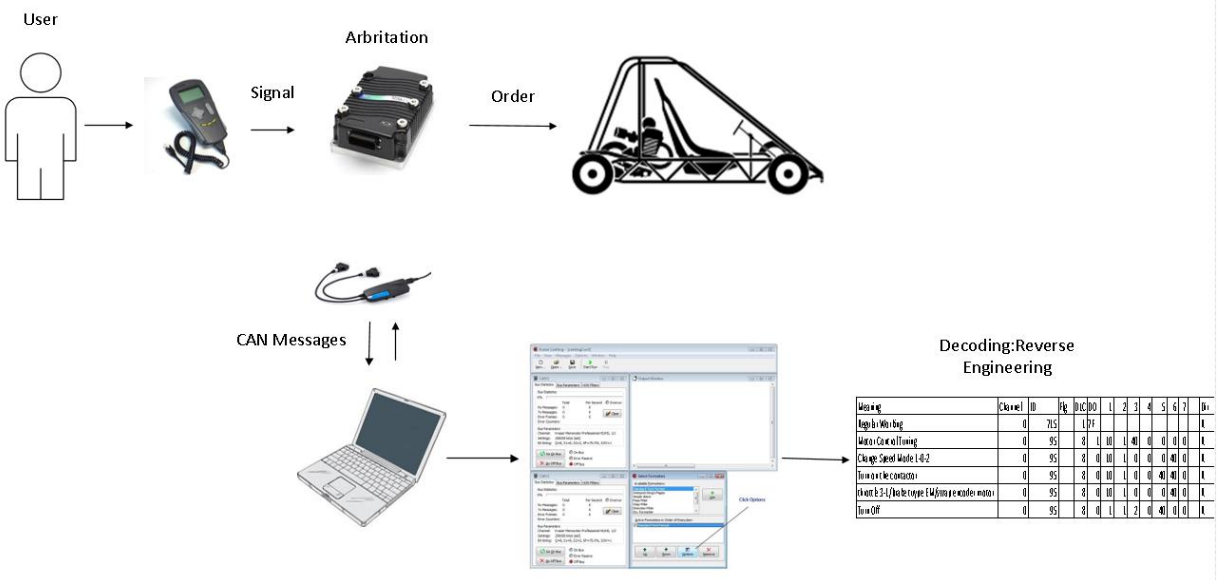
Figure 2.13. Configuration of the speed rate of CANking
Source: Own elaboration

The decoding and reverse engineering process follow the methodology posted in **Figure 2.14.** The user takes control of the changes that are made in the vehicle with the

CURTIS 1311, this practice is straightforward and common. It is used to program the vehicle according to the needs of the road, golf car, go-kart race, cargo vehicle and so on.

CAN messages are sent from the programmer to the Curtis, the problem remains in the impossibility to read the can messages in the programmer. Therefore, was needed to look for alternatives methods to read these messages. In the data collection section, it was stated that the Kvaser ports is a useful tool to read messages then this method is the chosen one.

In the following diagram, it is specified the two output lines in the CURTIS 1236, the orders and the CAN message values. Reading those values is a not a simple task, it requires to receive the data packet in the software Can King and then it is needed to do reverse engineering to understand those messages. For example, when pressing the throttle, the software receives a messages, after that it is necessary to press do the same action multiple times to make sure that the code is the right one. Finally, when all possible messages are decoded those are tabulated.



Meaning	Chanel	ID	Flg	DLC	D0	1	2	3	4	5	6	7		Di
Regular Working	0	715		1	7F									R
Motor Control Tuning	0	95		8	1	10	1	40	0	0	0	0		R
Change Speed Mode 1-0-2	0	95		8	0	10	1	0	0	0	40	0		R
Turn on the contactor	0	95		8	0	10	1	0	0	40	40	0		R
change 3-1/brake type EM/swap encoder motor	0	95		8	0	10	1	0	0	0	40	0		R
Turn Off	0	95		8	0	1	1	2	0	40	0	0		R

Figure 2.14 Decoding and reverse Engineering Process

CHAPTER III

RESULTS

This chapter presents all the results and analysis from the experiments made for this research. Data was collected from the Grand prix race and the experiments were made in the INSET laboratory.

3.1 Analysis of the Vehicle in Steady Conditions

During the race, the vehicle worked in normal conditions, which means that all the components were working properly. All the parameters were measured in one lap; and the analysis was just for that time frame

Figure 3.1 shows how Revolutions Per Minute (RPM), Amperage (Amps) and the laps changed over time during one cycle. In fact, the different type of paths in the race track affect how the internal components work (see **Figure 3.1**).

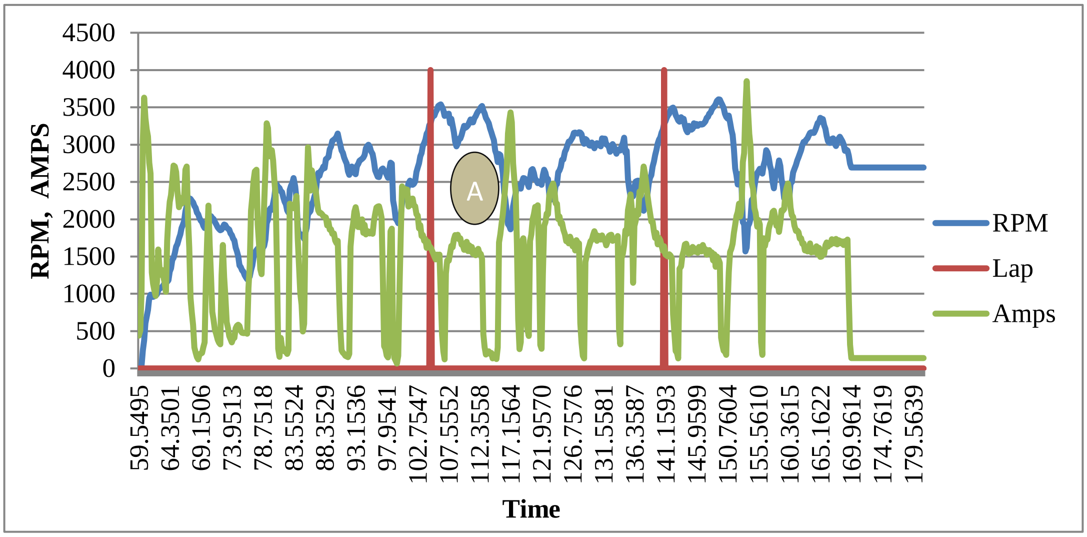


Figure 3.1 Data collected from one lap of the vehicle in the Purdue Grand Prix race

For example, in the straight line of the track from point 3 to 4, amperage has a regular and expected linear behavior. This can be demonstrated just by looking **Figure 3.1**, where the circle A is that straight path. The parameter that impacts more in the power of the vehicle is the motor current or amperage, which is considered an independent variable. Dependable variables would be real power and torque, that are important values to understand the motor behavior under diverse load conditions.

In **Figure 3.2**, there are seven numbers pointed that show those mentioned kind of paths. As it can be seen those paths force to change the speed and brake of the vehicle, so the throttle is manipulated several times in this driving cycle.

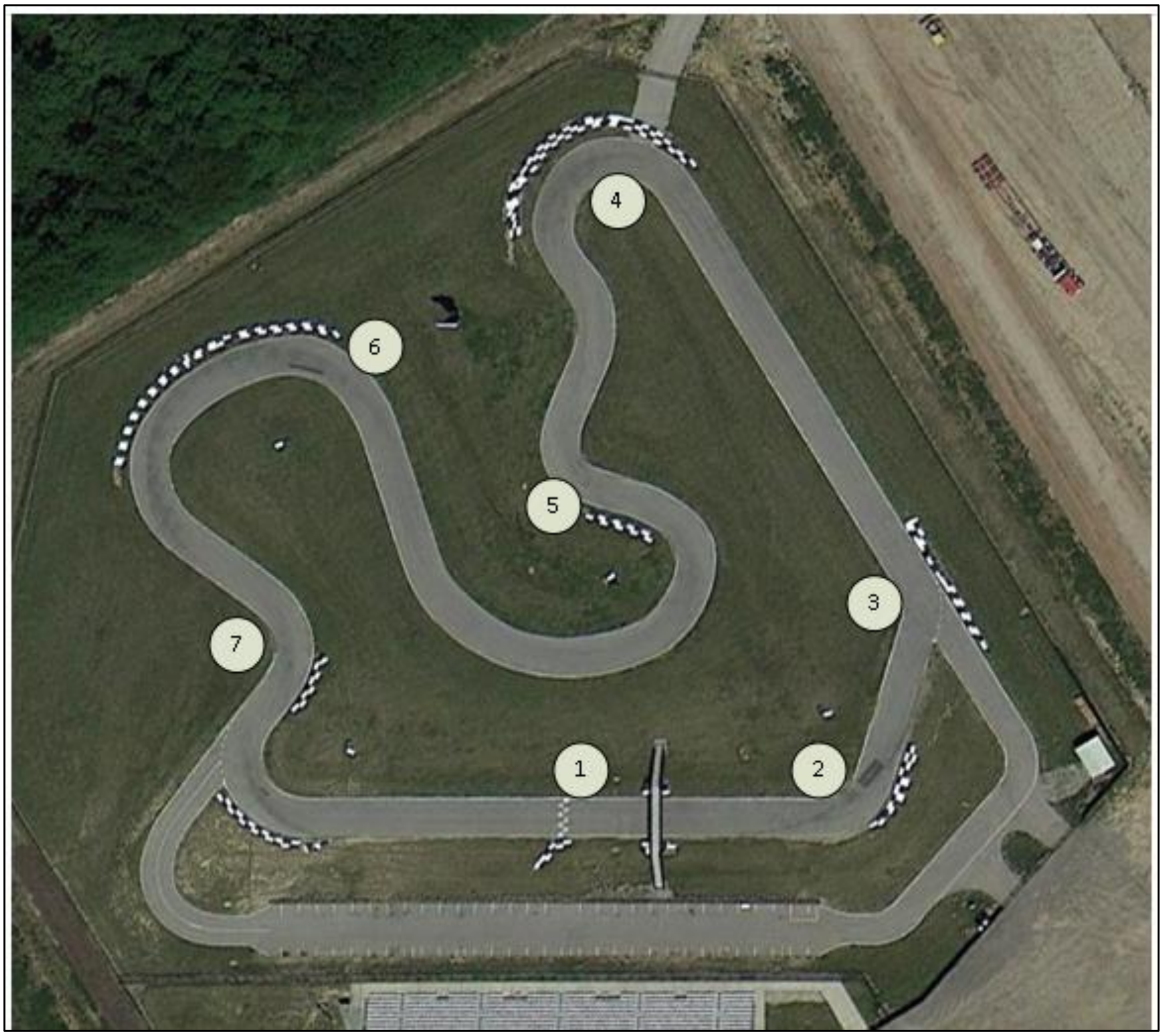


Figure 3.2 Grand Prix Race Circuit Paths divided per number

The correlation between real power and current is defined by **Equation 1**, where currents affect directly the output power. As it was stated in the literature review, in most of the cases, an induction motor presents this phenomenon when different loads are applied in one-time lapse, one lap for example.

$$P_{in} = 3\, V_{ph} I_{ph} cos\theta \qquad (1)$$

To demonstrate how this correlation is affected in one period of time, **Figure 3.3** shows how the real power changes over the same time lapse of **Figure 3.1**. It is important to mention that voltage, and the power factor are regularly constant values under different loads, therefore it is not necessary to analyze fully both parameters.

$$y = 14874e^{-0.012x}\ ; R^2 = 0.1166\ (2)$$

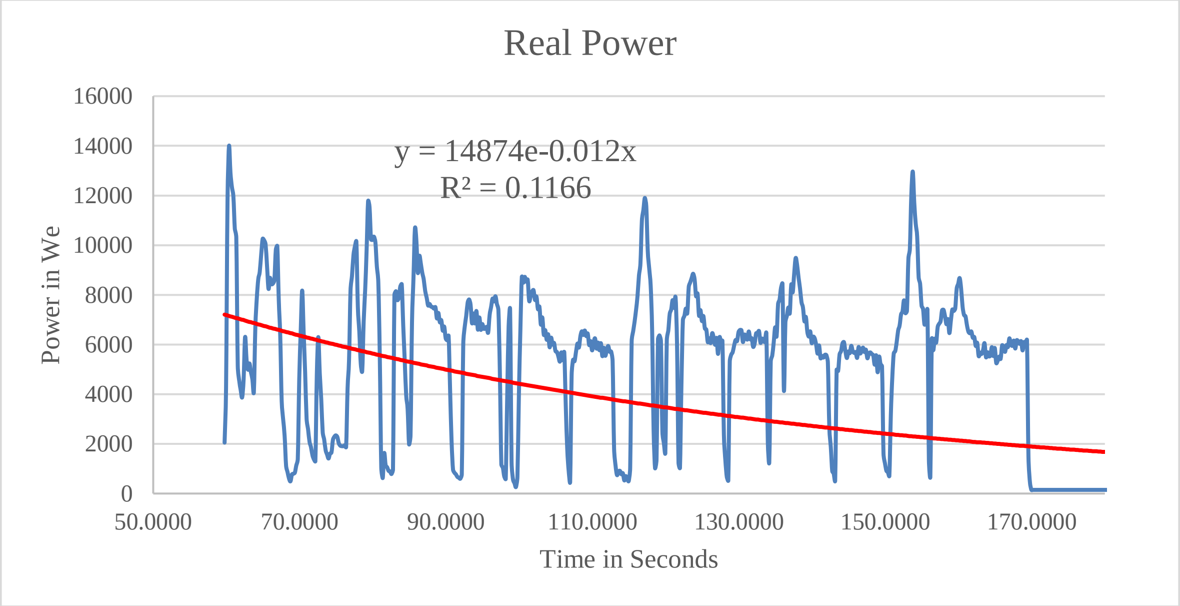


Figure 3.3 Real Power Variability in one lap

At the beginning of the engine experiments, there was a high torque because the vehicle needs considerable amount of energy to get out from inertia. During all the lap, power keeps changing in normal rates, nonetheless, the predictability of the values are very weak.

This can be seen in **Figure 3.3**, where the exponential regression does not fit in the real power curve. In fact, the Pearson correlation value R is weak, which means that there is not a strong correlation between time and power. This happens because of the different kind of paths in the circuit, for this reason the average values need to be analyzed per section to represent valid data.

Even though the predictability of the parameters is not valid to analyze from a performance and cybersecurity point of view, the range values of the manufacturer contribute to protect the engine and predict values that runs between those limits. The range of the vehicle parameters are delimited by the values obtained experimentally in the race, which are shown in the previous graph. Consequently, any value that exceeds that threshold will be considered a disturbance.

There are diverse data inputs or parameters that can be analyzed, nonetheless, it is more practical to determine which parameters are the most important. In that way, it is easier to analyze the parameters that affect the car performance the most.

For this data selection, there were used two criteria. The first one was to use the threat model, which is explained in the mitigation and protection section, because it allows selecting the riskiest process easily; and the second one was to use not uniform data according to its standard deviation. The data selected is shown in **Table 3.1**, corresponding to miles per hour (mph), voltage, RPM, and current; all of them affect the car performance and have a high degree of variability during the experiment that may generate **noise in data**.

	Average	Standard Error	Lower Threshold	Upper Limit	Standard Deviation	Lower Threshold	Upper Limit
Current (A)	159.7709	3.21383	153.47179	166.07003	75.37111	157.8109	307.498276
Voltage (V)	40.3485	0.07911	40.19341	40.50353	1.85532	38.3885	43.984906
Mph	26.5295	0.29523	25.95080	27.10811	6.92378	24.5695	40.1000634
RPM	2580.1855	28.55213	2524.22327	2636.14764	669.60691	2578.2255	3892.615

Table 3.1. Statistic Values to prove hypothesis

The p value allows proving a hypothesis of what would happen to the vehicle performance if some values change. During the test the car had an average current of 159 A, the next question was what would happen if the controller exceeds 350A, which is the threshold of the motor.

It was found, according to the statistic test, significant evidence that there will be no overcurrent flow in the motor if the controller is set between 0 and 3500 RPM (which is the RPM threshold during the experiment) and rpm range p=0.0003, if p is much smaller than 0.05, then the hypothesis is false.

The p value is too little in comparison to the alpha value. A low p (p=0.0003) value is common when there is a large sample size like this case, indeed there is data dispersed mainly because the vehicle is moving in many directions, zig zag or curves. In **Figure 3.4**, the current of the motor varies drastically from 50 A to 350A, this data actually affects the diagnostic of the car, because it highly dispersed creating big ranges.

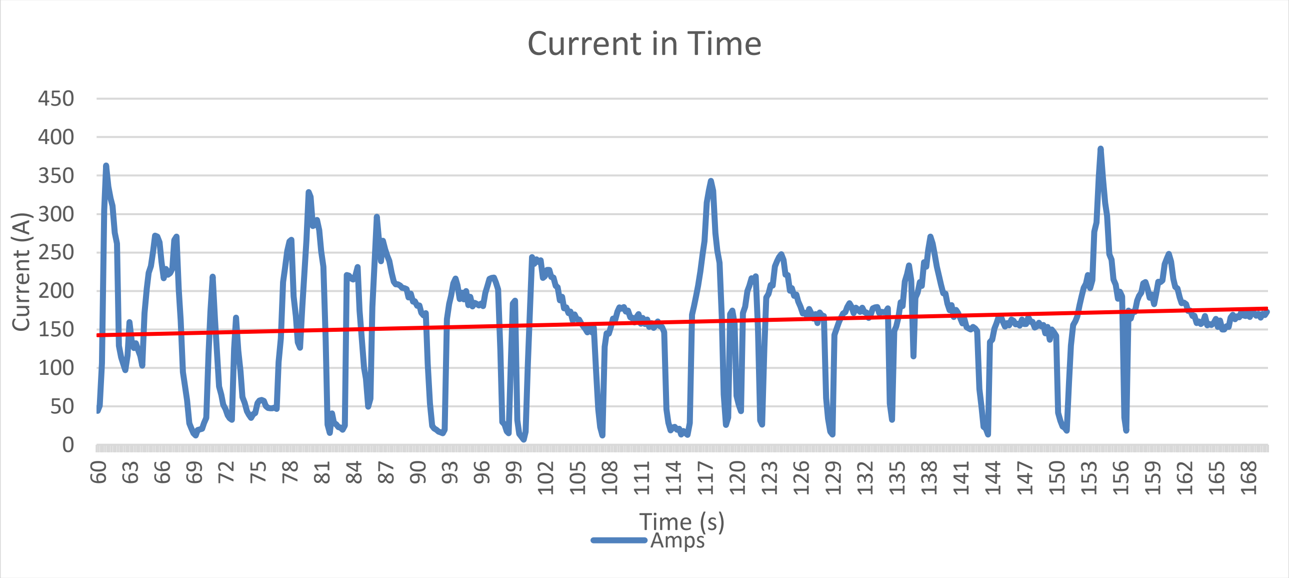


Figure 3.4 Current in Time

As it can be seen in **Figure 3.4**, the current average is 159 A, which was not useful for diagnostic and for reading values due to the high degree of variability. Nevertheless, those values are still data and they had to be analyzed and interpreted using SPS Software.

Table 3.1 shows the Standard Deviation (SD), Standard Error (SE) and its proper Upper and Lower limits. As it can be seen, the range of the SD is larger while the range for the SE is shorter. The explanation for the standard error is that there were taken 550 data points and the average value was 159.7 A, this means anytime the data can be taken again either N=550 or N=1000 about the same population (it means running the car under 3500 RPM), the mean range will be between 153.4 and 166.0 A.

On the other hand, the limit of the SD tells that if you choose any data point of the sample, the current should be between the range of 157.8 and 307 A. In general terms, standard error permits knowing the error anytime the sample is changed, while the standard deviation shows the range of the actual sample. What can be discussed in this part is the value that is important to analyze in the electric engine:

1. The analysis needs to be considered only under full load conditions, this value is showed in the motor label, other values create variability.
2. If some specific time frame needs to be analyzed, the values to considered are the straightest pattern. In other words, the path of the track.

The battery is fully charged when the race starts and it decreases gradually during all the lap time frame, varying voltage from 44V which is the full charge state to 38V. The battery pack is Lithium-Ion battery, which is composed of 12 cell of 3.8V each one. The recommended ranges for this kind of battery is 3.8 to 3V per cell, therefore 36 V would be the lowest limit for the entire battery pack, in this case the BMS and the Curtis is programmed to not work under 38V for safety reasons.

Knowing this information, the user would not have any problem related to the battery and the BMS if the person has a visual telematics device like a dashboard or even the CURTIS 1311. Nevertheless, the BMS and the CURTIS are vulnerable devices that are easy to access by the public, in fact both of them have a CAN port access which can be penetrated just by doing a reverse engineering process and finally the intruder can change the range values.

The discharging process of the battery can be identified by looking at the voltage behavior during one-time frame. In Figure 3.5 is showed how voltage is varying in time at different path of the race. Normally the battery is fully charged between 3 or 4 hours, meanwhile the discharging process can take less than half an hour using the vehicle under full load conditions like in the race. There were taken 68 points for each second of the race that is why some points look repeated in fact this is actually useful to look how some cells values can affect the average voltage of the battery which goes from 38 to 44 volts. Approximately every range of 1-15 seconds voltage varies (increase and decrease) which is an indicator of rapid and sudden changes while driving. As a consequence, the read average voltage does not show really what is the real charge state of the battery until it is keeps a constant speed or it is stopped.

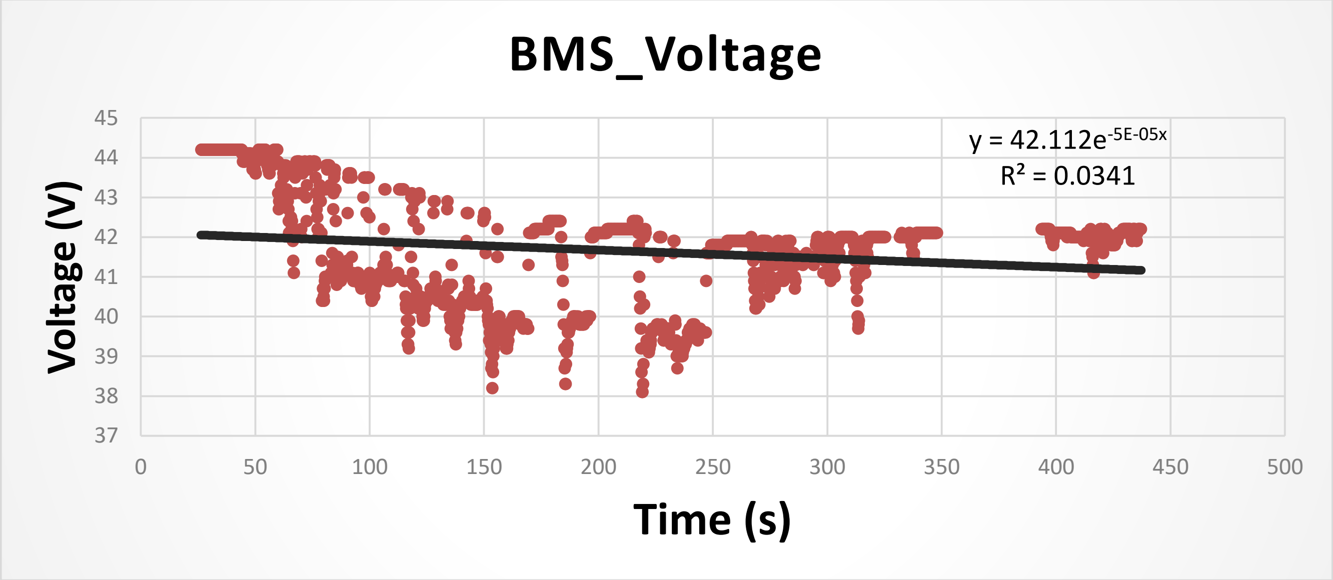


Figure 3.5 Discharging Process of the battery

3.2 Decoding and Reverse Engineering

The CURTIS 1236 works as an electronic control unit in the studied vehicle. In the previous chapter it was specified the procedure used to access to the vehicle CAN Bus network and how it was made the decoding. In this section, the analysis goes deep on the meaning of each data packet and why there are few messages in comparison to an actual vehicle.

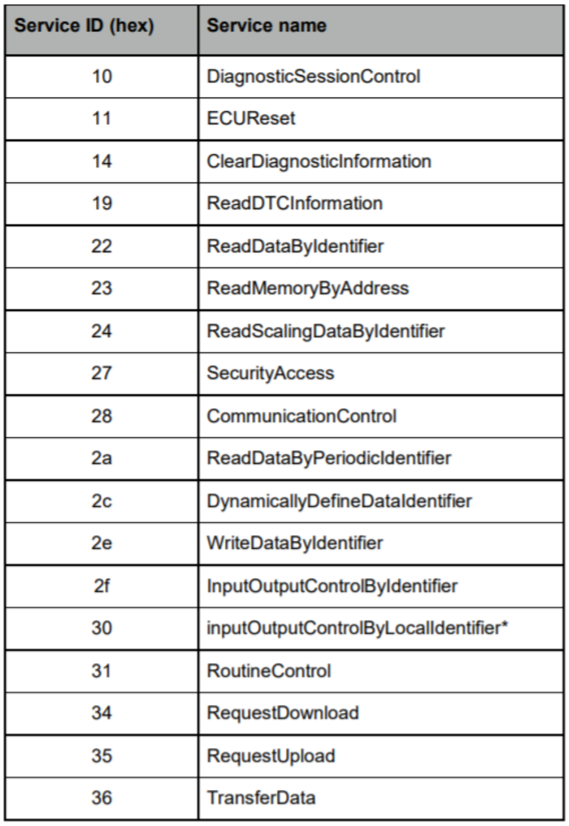
Accessing to the controller is not an easy task, the methodology section describes the steps to understand and decode CAN messages. **Table 3.2** shows the amount of messages that were decoded from the CURTIS 1236 during various test made in the INSET lab.

Meaning	Channel	ID	Flg	DLC	DO	1	2	3	4	5	6	7		Dir
Regular Working	0	715		1	7F									R
Motor Control Tuning	0	95		8	1	10	1	40	0	0	0	0		R
Change Speed Mode 1-0-2	0	95		8	0	10	1	0	0	0	40	0		R
Turn on the contactor	0	95		8	0	10	1	0	0	40	40	0		R
throttle 3-1/brake type EM/swap encoder motor	0	95		8	0	10	1	0	0	0	40	0		R
Turn Off	0	95		8	0	1	1	2	0	40	0	0		R

Table 3.2 Data packets recorded in experimentations.

There are 6 different messages that the software CAN King receive when some manipulations are made in the vehicle, only one message can be seen in the platform in one-time frame. In addition, the CAN protocol is configured to do just one action when the vehicle needs it. This process is called arbitration and the protocol selects according to the ID which process is more relevant. For example, in **Table 3.2**, the ID of regular working is high, which means this is not a message to priories if some disturbance occurs in the vehicle; on the other hand, when the user access to the Curtis programming and switch the speed mode, all the additional functions of the car are frozen until the speed mode is changed.

The CAN packets uses the ISO-TP, an international standard for sending data packets over a CAN bus network. Below it is a list of service IDs for the ISO 14229, each one has a particular format and the arbitration is made by using the lowest ID. **Table 3.3** shows the hexadecimals values of the ID while in **Table 3.2**, IDs are in decimal values.



Service ID (hex)	Service name
10	DiagnosticSessionControl
11	ECUReset
14	ClearDiagnosticInformation
19	ReadDTCInformation
22	ReadDataByIdentifier
23	ReadMemoryByAddress
24	ReadScalingDataByIdentifier
27	SecurityAccess
28	CommunicationControl
2a	ReadDataByPeriodicIdentifier
2c	DynamicallyDefineDataIdentifier
2e	WriteDataByIdentifier
2f	InputOutputControlByIdentifier
30	inputOutputControlByLocalIdentifier*
31	RoutineControl
34	RequestDownload
35	RequestUpload
36	TransferData

Table 3.3 IDs for ISO 14229

There are two types of IDs in the results which are 95 and 715, these numbers are in a decimal base. Therefore, both have to be converted to hexadecimal base, being 2cb and 5f respectively. The meaning of both values are interpreted in **Table 3.3**.

On the other hand, the DLC box means the length of the message, which is the number of bytes in the message. The first packet possesses 1 byte while the others 8. The meaning of each one will depend on the manufacturer interpretation, even though it is possible to know the meaning of the number of bytes by asking the manufacturer manual; the reverse engineering process requires to predict this value. In that way, the laboratory tests indicated that the on state of the car send same messages after 5 minutes' tests. The 1 byte DLC showed that when the car is working normally, no action needs to be done in the vehicle.

3.3 Mitigation and Protection

The kart prototype has two high risks, which are the control of the VCL and the CAN BUS communication, once accessed to these systems, it is easy to control any parameter of the car such as voltage, current, control motor settings like the kp, ki, kd, rpm limit and so forth. Using the VCL allows the user to change the different thresholds of the car. For example, the relation of current and power in a three phase induction motor is crucial, **Equation 1** shows the direct relation between the two parameters (without considering voltage because it keeps the same mostly). For example, the induction motor has 18 HP of max power and 350 A of max current. Exceeding current reduces the lifespan of materials and the energy supply of the motor and could eventually blow the fuse.

Curtis Messages

The CURTIS 1311 permits the user to change different parameters to tune the engine for different purposes. For example, if this car is used for a golf field, the speed should be steady; on the other hand, if the car is used for a race, parameters such as the PID values or the maximum speed should be modified. These changes are not made manually by using potentiometers or any mechanical source, this actually needs to be modified by using a controller which sends CAN messages. The 1311 controller send messages and the Curtis process these messages in a closed loop, as shown in **Figure 3.6** below.

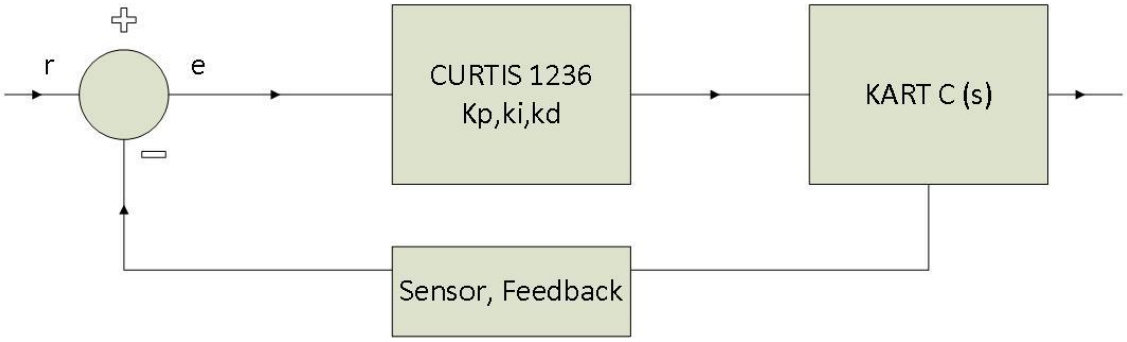


Figure 3.6 Control Loop of the system

The programmer has a display which shows the kind of programming of the car, however, this was created for the user to simplify the operation. In **Figure 3.7** it can be seen the display of the programmer.

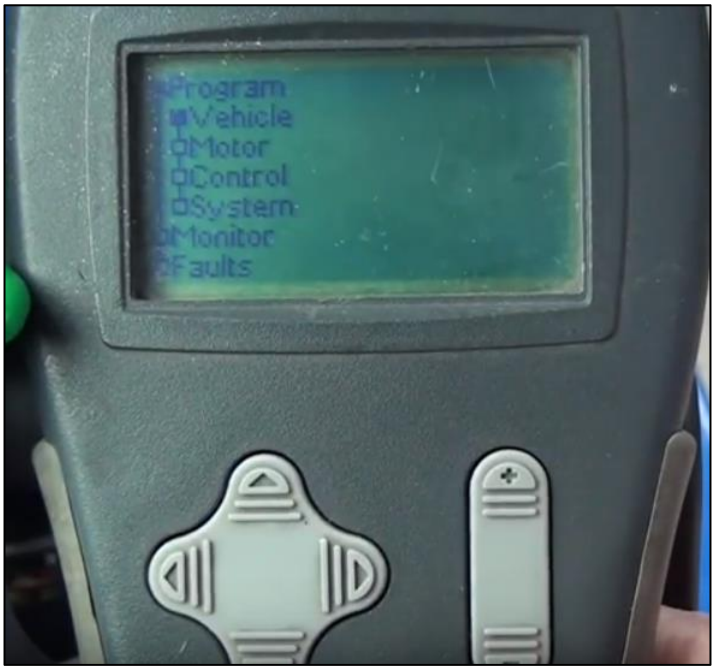
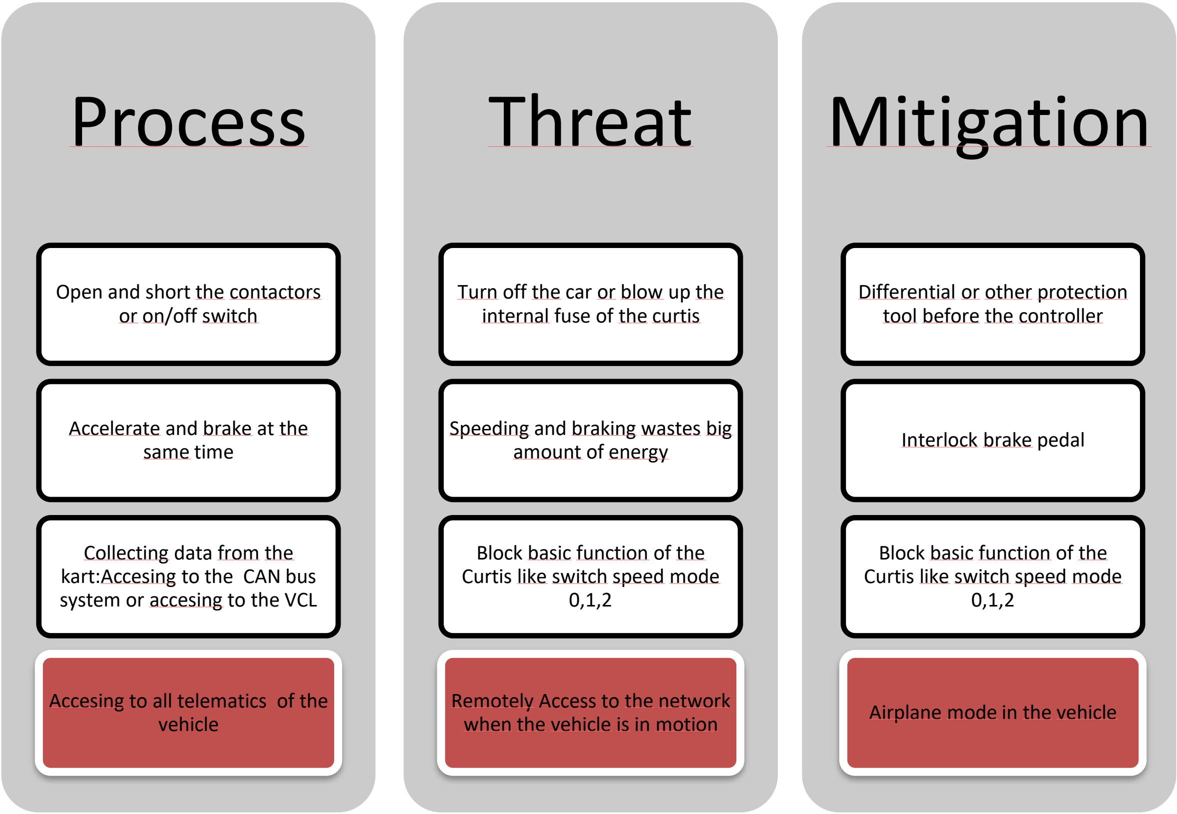


Figure 3.7 CURTIS 1311 Displayer

The displayer send CAN messages to the Curtis, however, this process can be repeated with a CAN bus interface like the Kvaser, once knowing what are the messages. All of this process can be seen in **Figure 3.7**.

There is a proposed hypothesis about the car security, which has vulnerabilities and potential cyber threats. In order to have a general overview of the car vulnerabilities, a threat model is a common practice to recognize easily a range of different risks, as showed in **Figure 3.8** below, the model is divided by process threat and possible mitigation or solution that may be applied; the colors represent the level of danger, where yellow is the less risky and red the most dangerous. Since this vehicle has a lack of sensors and process there are only four process. In general terms the following experiments need to prove the veracity of the presented hypothesis.



Process	Threat	Mitigation
Open and short the contactors or on/off switch	Turn off the car or blow up the internal fuse of the curtis	Differential or other protection tool before the controller
Accelerate and brake at the same time	Speeding and braking wastes big amount of energy	Interlock brake pedal
Collecting data from the kart:Accesing to the CAN bus system or accesing to the VCL	Block basic function of the Curtis like switch speed mode 0,1,2	Block basic function of the Curtis like switch speed mode 0,1,2
Accesing to all telematics of the vehicle	Remotely Access to the network when the vehicle is in motion	Airplane mode in the vehicle

Figure 3.8 Threat Model of the Vehicle

In regular vehicles either electrical o engine combustion, there is always temperature variations, therefore motor or battery temperature always fluctuates in a regular range. When a cyberattack occurs, it is less likely to attack directly temperature fluctuations of components, for this reason this is considered a low level risk.

There are also the mechanical and energy problems which are important due to the energy consumption and durability of the car ride, however, this does not represent a cyber-threat per se. Indeed, it is something that can be solved by using high tech components (Li-ion batteries or Advanced BMS).

On the other hand, the threat becomes riskier when communications are involved. In the car under study, there are two communications gateways: the CAN and the VCL, both of them are equally useful for reading and changing any car performance settings. Moreover, once accessed to the VCL system, any threshold or parameter can be modified for performance purposes. For instance, when using the throttle configuration, the normal voltage threshold is 5.24 V, VCL allows the change of this threshold to any kind of voltage, which can cause and overvoltage producing rapid motor response in the car. The possible vulnerable changes that can be made are listed below:

- Throttle: This is used in two ways as a name for the drive throttle and as a generic term covering both drive throttle and the brake throttle [58]
- Max RPM
- Max Current

Controlling communications is the highest risk in the threat model during the operation process. Apart from determining the threat, the mitigation or possible solutions to this problem, there are also other risks such as the acceleration in various sequence times by breaking and accelerating, which is not a network problem, however, it wastes big amount of energy. The threat model guaranties prevention of possible attacks, it was executed only for the real kart, with the intention of knowing which variables to manipulate.

3.4 Unsteady Condition

The unsteady condition is the operation of the vehicle out of the limits that were presented by the manufacturer. This condition can affect drastically the vehicle performance, provoking deconfigurations in the controller of the vehicle or reducing the life expectancy of the equipment, such as the battery bank which has a life expectancy of 5 to 8 years [63].

Table 3.4 shows the parameter limits of both operation modes, the steady and unsteady conditions. It is worth mentioning that these are not nominal values or plate values, since the vehicle is present for one specific mode of operation, where the threshold values vary. Essentially the vehicle is modified to reach maximum speed ranges because of the needs of the Purdue grand prix race, other configuration is needed for a cargo vehicle which needs more torque and less speed.

Parameter	Steady Limit	Unsteady Condition
Motor Current	350A	<350
RPM	3600	<3600
Motor Voltage	48V	<48 or >40
Battery Voltage	48-40	<48 or >40

Table 3.4 Steady and Unsteady conditions of the Vehicle

Even though these values can change during the vehicle operation, where the driver can perceive the conditions and turn off the engine; there are other ways to send messages to the indicators, SCADA or dashboard of the vehicle that cheat the driver. Therefore, this part of the results will focus only on the physical ranges of the vehicle.

3.4.1 Performance Response

Once penetration is executed in the vehicle network, several packet messages can be sent to the controller and alter the parameters of the vehicle. Since it can be found easily the threshold of the equipment just by looking for the plate values; there is one likely scenario of attack. The attacker changes the limits of current and voltage depending of the intentions which is unpredictable.

For this performance response under unsteady conditions, the threshold of the current has been changed from 0 to 50 amps randomly. Varying the current affects, the real power as well, and in fact the variability and dispersion of the data will increase too.

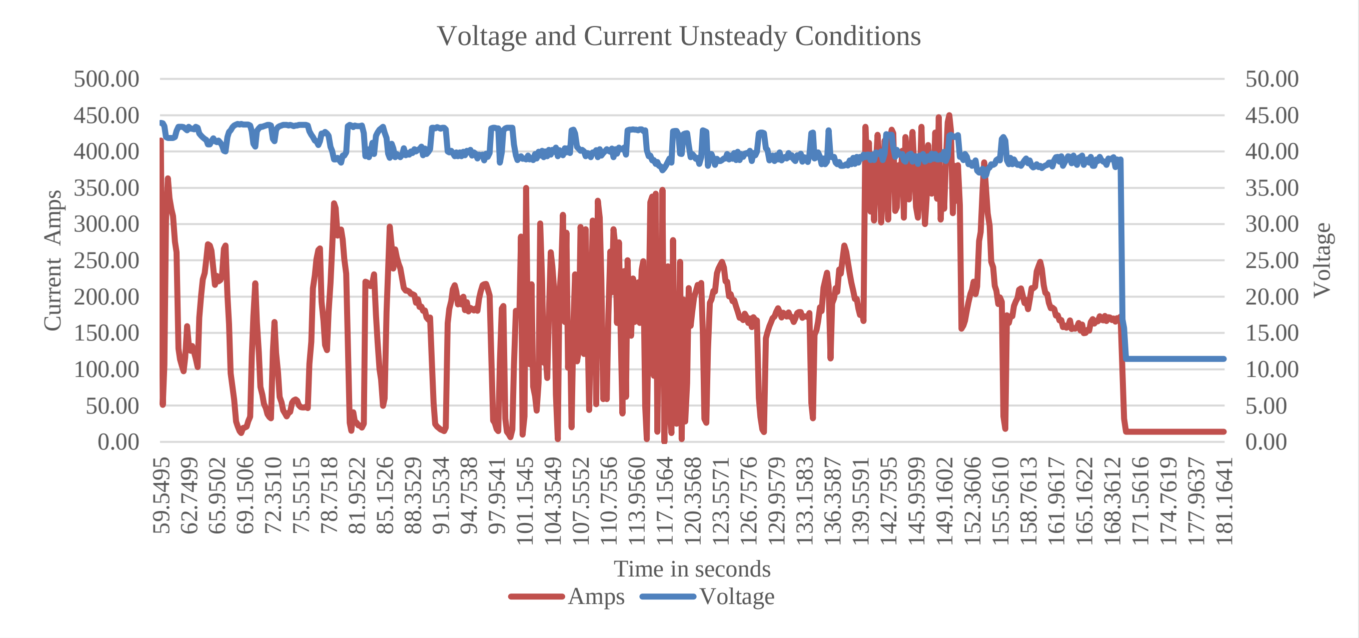


Figure 3.9. Voltage and Current Unsteady Condition in Motor

The suitable range values to alter is between 100 to 120 and 137 to 151 seconds since it has more unsteady curves during the race. As it can be seen in **Figure 3.9**, current keeps a regular or at least controlled growing until 100 seconds, where a random function is inserted in the mentioned two intervals. It is important to note that voltage keeps the same during this test because it is an independent variable of current. The effects of this high degree of variability is analogous to what happens to the real power and revolutions per minute in the motor.

In **Figure 3.10**, real power has drastic fluctuations in the second 100 which has the same variability of current since they are directly proportional; on the other hand RPM reaches 4000 values which reduces the torque values of the car causing more speed but less strength. It is important to emphasize that this RPM peak is not even closer to the nominal 10000 RPM limit of the motor plate, but as it was mentioned, full load conditions change once the vehicle is preset.

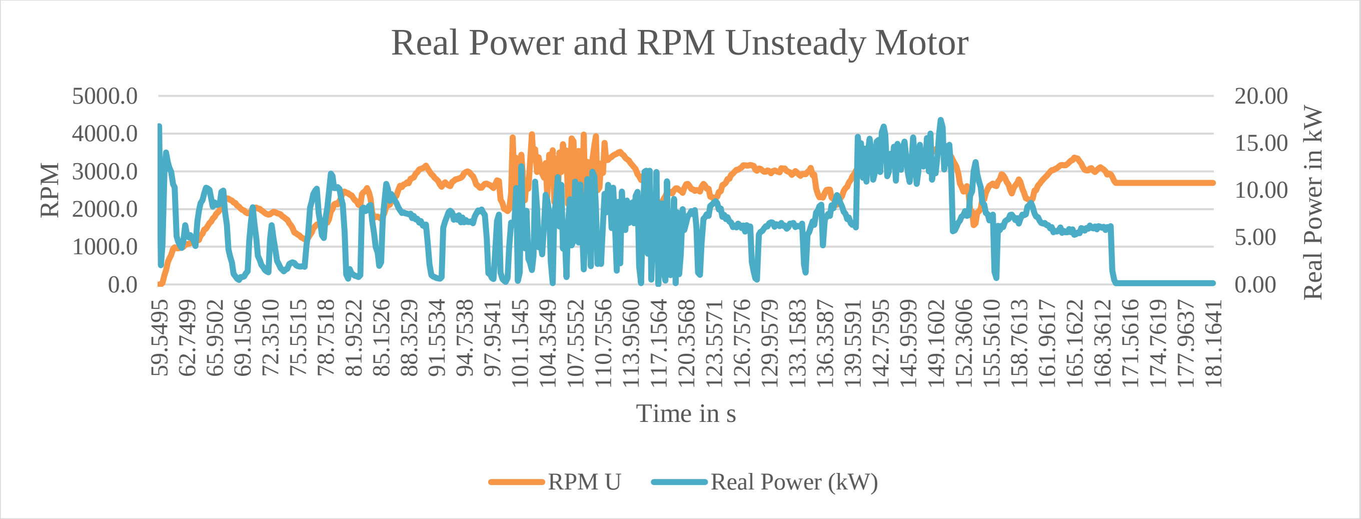


Figure 3.10 Real Power and RPM Unsteady Motor Conditions

The Battery Managements System can be penetrated separately apart from the Curtis controller because it has its own CAN bus network, then its limits can be changed too. In fact, the effects on the BMS will reach the controller during the discharging and charging process, there are sudden changes in the 193 second until the 257, which finally is observed in **Figure 3.11**. This disturbance has an effect on the torque which affect the final efficiency of the motor.

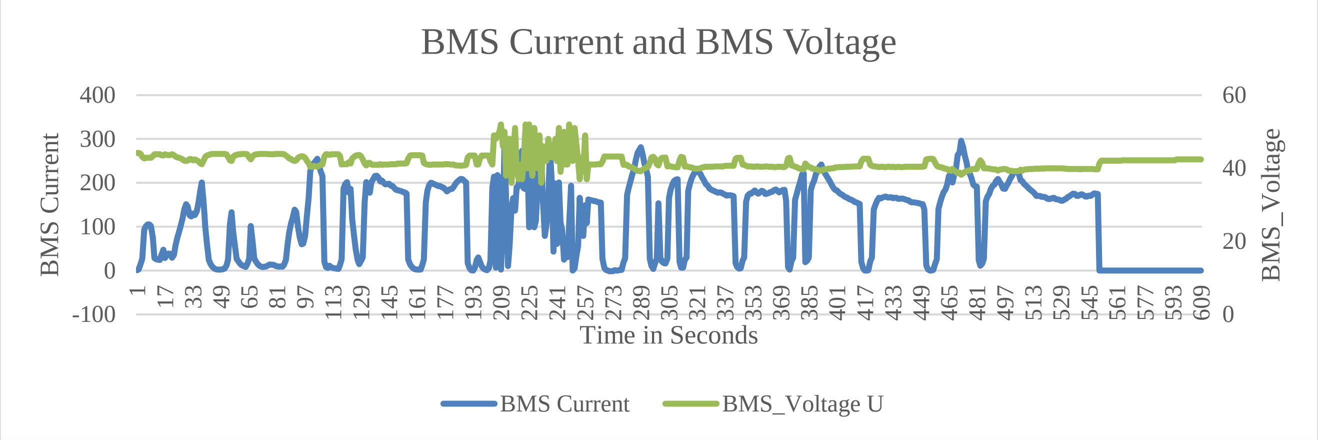


Figure 3.11. BMS Current and BMS voltage Unsteady Conditions

The final indicator that shows the losses of the motor is its efficiency. In the following chart, it is showed how much varies this parameter under different RPM and load conditions. One of the main thing to highlight is that during the race most of the points are located at lower real power values between 1-6kWThis actually makes the motor reduce the efficiency, being 177 of 600 seconds under 60% of efficiency those were gotten in normal conditions (see Figure 3.12 and **Figure 3.13**).

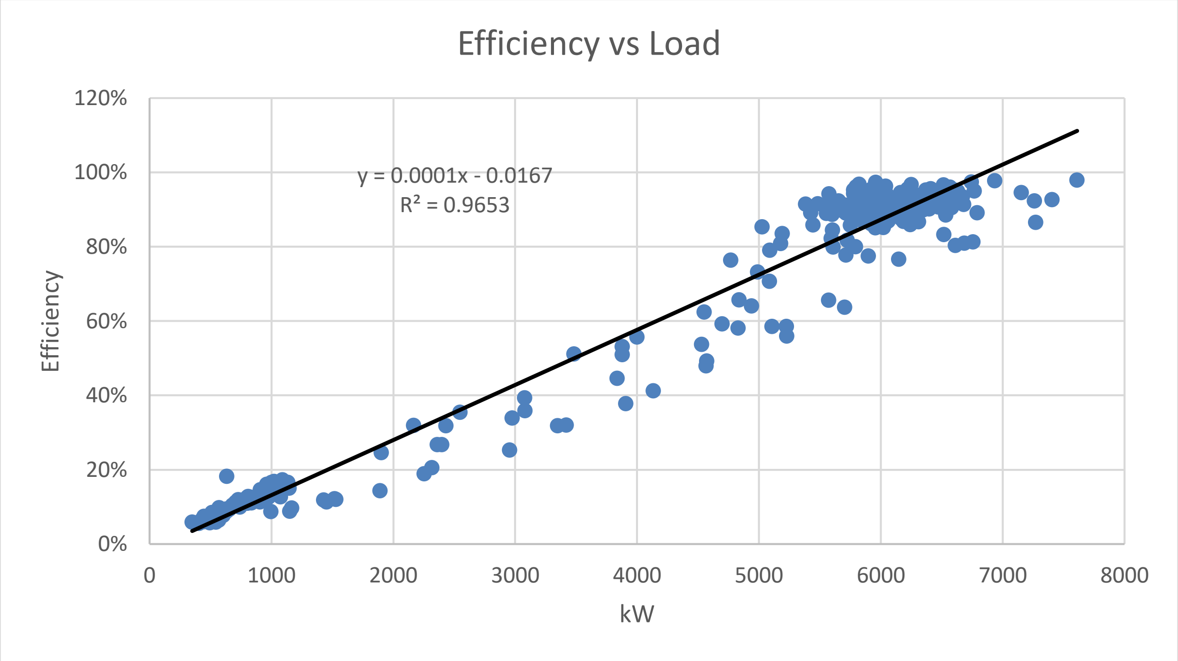


Figure 3.12 Efficiency vs Load in Normal conditions

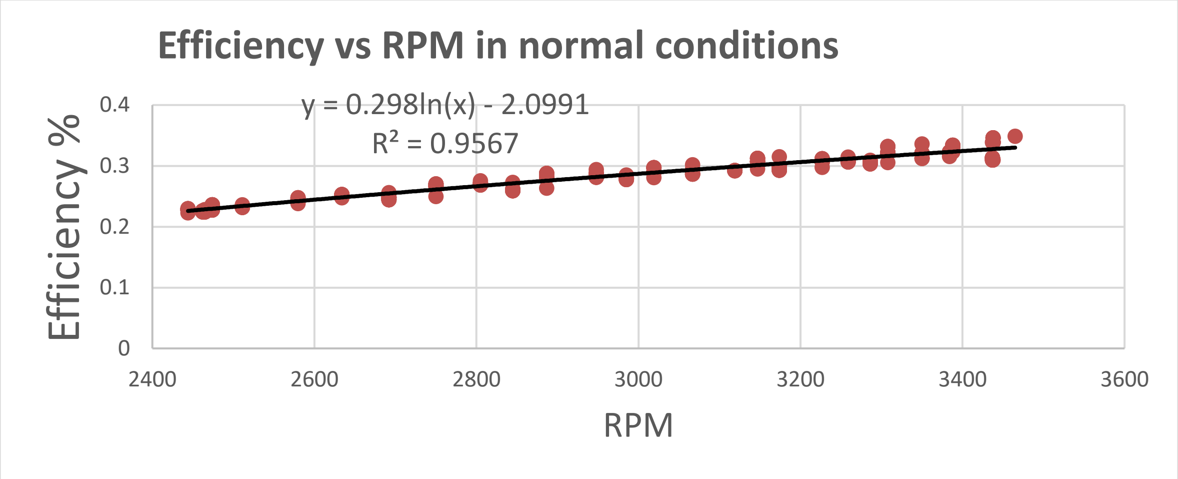


Figure 3.13 Efficiency vs Load behavior under normal conditions

The other test consisted in varying the frequency of the motor simulating a VFD(Variable Frequency Drive), a device that is normally used to improve efficiency but in this case it will be used to reduce efficiency in the vehicle, in Figure 3.14 is showed the same chart as the normal conditions chart, but changing the frequency of the motor between 60 and 80 hz, provoked an average efficiency of 24% in comparison to 28% of the normal conditions. In fact, the correlation factor is reduced drastically in the simulated penetration, which highly dispersed data. In other terms a simple change in frequency can affect drastically the energy consumption in the vehicle.

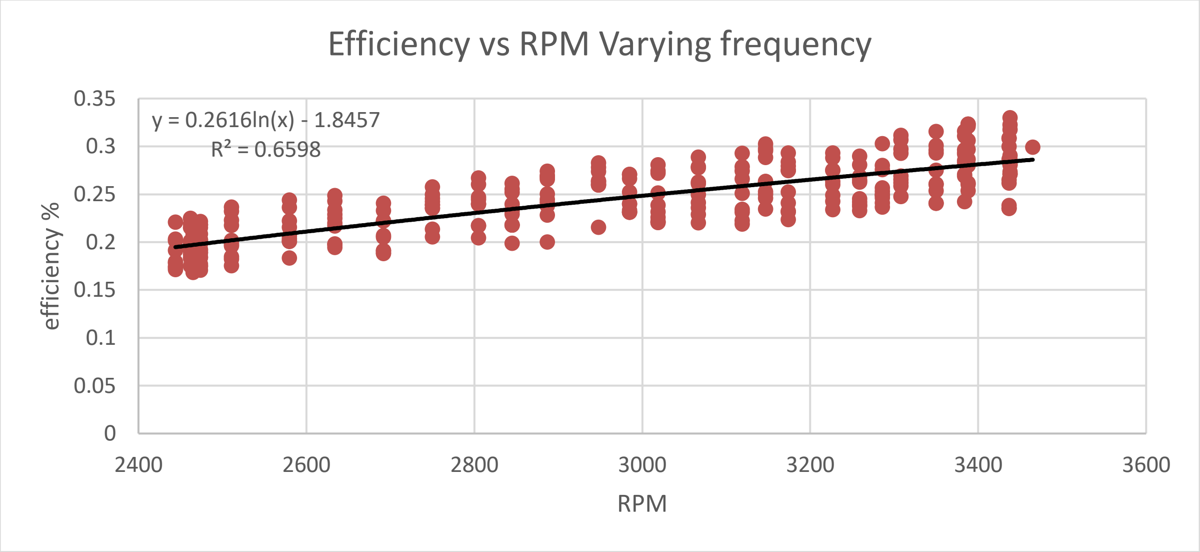


Figure 3.14. Efficiency altered by varying frequency

4 CHAPTER IV SUMMARY AND RECOMMENDATIONS

This research was done in collaboration of two universities: UTEC in Lima Peru, and Purdue University in Indiana USA. The theoretical part of this research took place at UTEC installations; meanwhile the experimental part was made in the Polytechnic faculty of the CNIT department in the Integrated Smart Energy Technology Lab at Purdue University. The tests were done with the assistance of researchers of the INSET lab and with the previous investigation made by Andrew Larson about driving cycles. The lab had an already constructed vehicle which had to be repaired, when that was done, the decoding and reverse engineering was possible.

The research proposed a general analysis about the physical effects that a cybersecurity penetration may cause in an electric vehicle. There were three separated sections in this work: Vehicle analysis in steady and unsteady conditions, decoding and reverse engineering, and finally, mitigation and protection.

Experiments employed different instrumentation and software (Commtool, Kvaser, SPS) to process data, meanwhile there was already recorded data in a previous research work that was used to analyze the vehicle in steady conditions.

The studied vehicle was used for a go-kart race which highly limited the scope of this cybersecurity study due to the lack of sensors and networks that a regular modern vehicle has. However, for the specific purposes of this research only the CAN bus network, the electric engine and the battery are useful to resemble the present-day EVs; which couples one of the objectives that was analyzing only the performance response of the car.

The different tests done in steady and unsteady conditions indicated that this vehicle is highly vulnerable to penetration attacks by decoding controller messages and changing the limits of the main parameters like current and voltage threshold, which were changed up to 100A extra of the full load. The problem with that growth was the deterioration of the motor and the variability of data.

Reverse engineering is a useful methodology to decode easily the CAN messages that the controller is receiving, once that data is processed the false messages can be sent with a meaning. Many messages were recorded during the tests, nonetheless, most of the messages were repetitive, then it was necessary to tabulate them manually.

The messages came in 8 bits packet with and ID. The ID is the prioritization number which can tell us what is the most critical messages, lower numbers have higher priority in the bus, therefore as an attacker you will pick a low number for critical systems like the engine components and equipment, which can be broken. This process can be imitated in almost any modern vehicle with a bus network, it is just needed the correct software and tools to decode the messages and pick up the critical numbers. When frequency was changed from 60Hz to 80Hz, vehicle efficiency was decreased by 4%. The tool that changed this variable was a Variable Frequency Driver (VFD), therefore what can be concluded about this experiment is that a tool that is commonly used to improve efficiency can diminish it as well. In comparison to an internal combustion engine, an electric motor always need a controller to operate and even other devices to improve the performance. Therefore, the electric motor has more ports to access, which represent a higher risk.

For the mitigation and protection part, it was necessary to observe the vehicle as a machine that has output and inputs interactions between other machines and people; once detected these points, a threat model is a good practice to recognize the main vulnerabilities and risk of the vehicle. Thus, the mitigation actions are prioritized according to the needs of the vehicle.

The main risk in the vehicle was the total penetration of the Curtis Controller, controlling the threshold of current and RPM can cause components wear and even block all functions. In addition, unlike the oil fueled vehicles, the EVs possess electric motors which represent higher risks, since controlling this type of engine depends more of the controller, like a VFD (Variable Frequency Drive). Generally speaking, the electric motor is more manageable than combustion motors.

Even though of the scope of this research, the facts indicate that the electric vehicle market is growing and vehicle manufacturers will have to face a conversion fuel to electric.

At the same time, many things are more connected than ever, which is something to pay attention carefully and not disassociate its potential threats.

Recommendations and future work

The limitations and weaknesses of this research were showing up when the tests were made. The tools that were used can be considered superficial analysis of a real test bed, for more accuracy other communication networks and sensors could have been used.

Future works can be oriented in other communication levels such the LIN, MOST or ETHERNET, which focus on other vehicle functions.

Another important fact to consider is that the manipulation of the electric motor can highly reduce the efficiency of the electric vehicle. Unlike the combustion engines when more load is applied, the efficiency goes up, in the case of electric vehicles, it will depend of two variables: Torque and current.

For future investigations, it is recommended to ask the manufacturer the real meaning of the CAN messages to corroborate the decoding and reverse engineering results, finally there is still uncertainty about the general deconfigurations of the CURTIS controller because not only threshold values can be changed, there are other more parameters that can be changed.

5 REFERENCES

[1] D. Hodge, Information, Place, and Cyberspace: Issues in Accessibility, Springer, 2000.

[2] I. T. Union, "ITU," 2016. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. [Accessed 28 August 2018].

[3] B. Gammons, "6 Must-Know Cybersecurity Statistics for 2017 | Barkly Blog," January 2017. [Online]. Available: https://blog.barkly.com/cyber-security-statistics-2017. [Accessed 26 September 2017].

[4] A. Bindra, "Securing the Power Grid," *Cybersecurity for the power grid and connected power electronics,* vol. 4, no. 3, pp. 20-27, 2017.

[5] J. Brandon, "Read This Before You Buy a Car With 'Autonomous' Technology," August 2016. [Online]. Available: https://www.inc.com/john-brandon/tesla-mercedes-google-read-this-before-you-buy-a-car-with-autonomous-technology.html. [Accessed 28 September 2017].

[6] A. Aditya, A. Hahn and Manimaran, "Cyber-physical security of Wide-Area Monitoring Protection and control in a smart grid enviroment," *Journal of Advanced Research,* vol. 5, pp. 481-489, 2014.

[7] NXP Semiconductors, "Introduction In-Vehicle-Networking," 30 August 2011. [Online]. Available: https://www.youtube.com/watch?v=DeQb8Q6hEkA. [Accessed 21 September 2017].

[8] A. Greenberg, "Hacher Remotely Kill a Jeep on the Highway— with me in it," Wired, 21 7 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed 17 9 14].

[9] BBC, "FBI warns on risks of car hacking," BBC, 18 3 2016. [Online]. Available: http://www.bbc.com/news/technology-35841571. [Accessed 14 9 2017].

[10] Newsroom, "Smart Electric Vehicle Charging Will Necessitate Greater Utility Investment in Cyber Security Systems," 2011. [Online]. Available: http://www.navigantresearch.com/newsroom/smart-electric-vehicle-charging-will-necessitate-greater-utility-investment-in-cyber-security-systems. [Accessed 21 September 2017].

[11] F. Lambert, "Elon Musk says preventing a ‘fleet-wide hack’ is Tesla’s top security priority," 17 July 2017. [Online]. Available: https://electrek.co/2017/07/17/tesla-fleet-hack-elon-musk/. [Accessed 22 September 2017].

[12] J. M. Amend, "GM’s Top Cyber Cop Ratchets Up Product Security," 21 July 2016. [Online]. Available: http://wardsauto.com/technology/gm-s-top-cyber-cop-ratchets-product-security. [Accessed 22 September 2017].

[13] K. Zetter, "AN EASY WAY FOR HACKERS TO REMOTELY BURN INDUSTRIAL MOTORS," Wired, Jan 2016. [Online]. Available: https://www.wired.com/2016/01/an-easy-way-for-hackers-to-remotely-burn-industrial-motors/. [Accessed Nov 2017].

[14] K. Chau, Electric Vehicles Machines and Drives: Desing Analysis and Application., Wiley, 2015.

[15] IFP Energies Nouvelles, "Development of electric vehicle: where," Lyon, 2017.

[16] International Energy Agency , "Global Electric Vehicle Outlook," *Electric vehicle initiative,* pp. 5-7, 2017.

[17] M. Weiss, M. Patel, M. Junginger, A. Perujo, P. Bonnel and G. Grootvel, "On the electrification of road transport Learning rates and price forecasts for hybrid electric cars and battery electric vehicles," *Energy Policy,* vol. 48, pp. 374-393, 2012.

[18] REN 21, "Renewables 2018 Global Status Report," 2018.

[19] World Economic Forum, "The Future of Electricity New Technologies Transforming the Grid Edge," 2017.

[20] Mckinsey & Company, "Electric vehicles in Europe:gearing up for a new phase?," 2014.

[21] European Alternative Fuels Observatory, "Top 5," Junio 2017. [Online]. Available: http://www.eafo.eu/top-5. [Accessed 10 10 2017].

[22] T. Penny, "U.K. Joins France, Says Goodbye to Fossil-Fuel Cars by 2040," Bloomberg, 26 July 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-07-25/u-k-to-ban-diesel-and-petrol-cars-from-2040-daily-telegraph. [Accessed 20 10 2017].

[23] M. Sharma and M. Kulkarni, "Trends and Challenges in Electric Vehicles," *International Journal of Innovative Research in Science,,* vol. 5, no. 5, p. 8592, 2016.

[24] T. C. Aiqiang Pan, "Electric Vehicle Development in China and its Power Quality Challenges for distribution grid," *CIRED workshop ,* no. 0160, p. 1, 2016.

[25] M. Tarpenning, "The 21 st Century Electric Car," pp. 1-10, 2006.

[26] Y.Xiao and M.Nemec, "Regenarative Breaking of Series-Wound Brushed DC Electric Motors for Electric Vehicles," in *2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, Singapore, 2012.

[27] Y. Fan, C. Tan, S. Chen and M. Chen, "Design and Analysis of a New Interior Permanent Magnet Motor for EVs," in *2016 IEEE 8th International Power Electronics and Motion Control Conference (IPEMC-ECCE Asia)*, Nanjing, 2016.

[28] A. Wang and Y. Jia, "Comparison of Five Topologies for an Interior Permanent-Magnet Machine for a Hybrid Electric," in *IEEE TRANSACTIONS ON MAGNETICS, VOL. 47, NO. 10, OCTOBER 2011*, 2011.

[29] The Tesla Motors Team, "Dual Motor Model S and Autopilot," 10 Oct 2014. [Online]. Available: https://www.tesla.com/blog/dual-motor-model-s-and-autopilot?redirect=no. [Accessed 24 10 2017].

[30] J. Kim, C.-J. Yu, M. Khammuang, J. Lui, A. Almujahid and T. Daim, "Forecasting Battery Electric Vehicles," *2017 IEEE Technology & Engineering Management Conference (TEMSCON),* pp. 1-8, 2017.

[31] B. Sarlioglu, C. T. Morris, D. Han and S. Li, "Benchmarking of Electric and Hybrid Vehicle Electric Machines, Power Electronics, and Batteries," *Wisconsin Electric Machines and Power Electronics Consortium (WEMPEC),* pp. 519-526, 2017.

[32] J. Hanania, B. Heffernan, J. Jenden, R. Leeson, T. Mah, J. Martin, K. Stenhouse and J. Donev, "Energy density," Energy Education, 2009. [Online]. Available: http://energyeducation.ca/encyclopedia/Energy_density#cite_note-r1-2. [Accessed 24 Oct 2017].

[33] Technology review, "The price of batteries," 2016. [Online]. Available: http://www.technologyreview.com/sites/default/files/legacy/jan11_featu. [Accessed 24 10 2017].

[34] R. Martin, "Why We Still Don't Have Better Batteries," MIT Technology Review, 29 August 2016. [Online]. Available: https://www.technologyreview.com/s/602245/why-we-still-dont-have-better-batteries/. [Accessed 24 Oct 2017].

[35] Wordpress, "¡PERÚ: HALLAN RESERVAS DE LITIO EN MACUSANI!," 2016. [Online]. Available: https://sintramin.wordpress.com/2016/06/06/peru-hallan-reservas-litio-en-macusani/. [Accessed 13 Nov 2017].

[36] W. Wilcke and H. Cheol, "Lithium Ion Batteries," *Spectrum,* p. 62, 2016.

[37] N. Jabbour, E. Tsioumas and N. K. a. C. Mademlis, "Improved Monitoring and Battery Equalizer Control Scheme for Electric Vehicle Applications," pp. 380-386, 2017.

[38] Rossouw von Solms, Johan van Niekerk, "From information security to cyber security," *computer & security 38,* 2013.

[39] D. G. Thakurta, "Cybersecurity Innovations," Frost and Sullivan, 2014.

[40] R. Muresan, *Cyber security spending to reach $90 billion in 2017,* 2017.

[41] NIST, "Cybersecurity Framework Development Overview," in *NIST's Role in Implementing Executive Order 13636*, 2013.

[42] " Directive (EU)2016/1148 of the European Parliament and of the Council," 2016.

[43] EECSP, "Cyber Security in the Energy Sector Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector," 2017.

[44] Research Checkpoint , "A New IoT Botnet Storm is Coming," 19 Oct 2017. [Online]. Available: https://research.checkpoint.com/new-iot-botnet-storm-coming/. [Accessed 13 Nov 2017].

[45] M. GIORGOS, "Introduction to In-Vehicle Networking: Generic Protocols," 2007.

[46] NXP Semiconductors, "Introduction In-Vehicle-Networking," 2011.

[47] M. P. Kristian Ismaila Aam Muharama, "Design of CAN bus for research applications purpose hybrid electric vehicle using ARM microcontroller," *2nd International Conference on Sustainable Energy Engineering and Application, ICSEEA 2014,* pp. 288-296, 2014.

[48] L. Camaron, "CAN Bus: la forma de transmitir información en el automóvil," 23 January 2013. [Online]. Available: https://www.motorpasion.com/coches-hibridos-alternativos/can-bus-como-gestionar-toda-la-electronica-del-automovil. [Accessed 13 October 2017].

[49] PICO Technology, "CAN and CAN FD bus decoding," [Online]. Available: https://www.picotech.com/library/oscilloscopes/can-bus-serial-protocol-decoding. [Accessed 05 Nov 2017].

[50] National Instruments, "Controller Area Network (CAN) Tutorial".

[51] Dongfeng Motor Corporation , "Creating a CAN Bus Communication Platform Based on the SAE J1939 Protocol and NI PXI," National Instruments, [Online]. Available: http://sine.ni.com/cs/app/doc/p/id/cs-14643#. [Accessed 14 Nov 2017].

[52] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," 2015.

[53] C. Smith, "The car hackers hand book," 2016.

[54] Microcontroller Division Applications, *Local Internet Network.*

[55] Most Cooperation, *Media Oriented System.*

[56] MOST, *MOST Specification,* Germany, 2006.

[57] "Enerdel Inc," [Online]. Available: https://curtisinstruments.com.

[58] "Curtis Instruments Inc," [Online]. Available: https://curtisinstruments.com.

[59] A. Larson, "An empirical approach of driving cycles," Purdue, West Lafayette, 2014.

[60] Kvaser, "Kvaser's CanKing - Free Bus Monitor Softwar," 2018. [Online]. Available: https://www.kvaser.com/canking/.

[61] A. Shostack, "Threat Modeling Why, What and How?," 03 July 2018. [Online]. Available: https://misti.com/infosec-insider/threat-modeling-what-why-and-how. [Accessed 11 September 2018].

[62] J. Mickens, "Usenix," January 2014. [Online]. Available: https://www.usenix.org/system/files/1401_08-12_mickens.pdf. [Accessed 11 September 2018].

[63] U. Vehicles, "Electric Vehicle Battery: Materials, Cost, Lifespan," [Online]. Available: https://www.ucsusa.org/clean-vehicles/electric-vehicles/electric-cars-battery-life-materials-cost#.W9TIGbuZ1PY]or the motors that can be severely affected by the driving conditions

and the breaking behavior [https://core.ac.uk/download/pdf/82196196.pdf . [Accessed 29 October 2018].

[64] PEDRO GAMIO, Manual processing xxx, Perth: Yale, 2016.

[65] Avast, "Ransomware," [Online]. Available: https://www.avast.com/es-es/c-ransomware. [Accessed 28 September 2017].

[66] J. Larminie and J. Lawrie, Electric Vehicle Technology Explaines, Wiley, 2012.

[67] D. Zhaoyang, "Smart Grid Cyber Security," 2014.

[68] A. C. e. al., "Cyber–Physical Device Authentication for the," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,* vol. 32, no. 7, Julio 2014.

[69] S. Morash, "Vehicle To Grid: Plugging In the Electric Vehicle," 2013.

[70] IEEE, "IEEE CYBER SECURITY FOR THE SMART GRID," IEEE, 2014.

[71] Kaushiva and C. Hawk, "Cybersecurity and the Smarter Grid," *The Electricity Journal,* vol. 27, pp. 84-92, 2014.

[72] L. Bitencourt, B. Borba, R. Maciel, M. Fortes and V. Ferreira, "Optimal EV Charging and Discharging Control Considering Dynamic Pricing," *PowerTech, 2017 IEEE Manchester,* p. 6, 2017.

[73] CSS Electronics, "OBD2 Explained - A Simple Intro," 2017.

[74] K. Mucevski, "OBD-II Connector and Fault Codes Explained," Linked In, 22 11 2015. [Online]. Available: https://www.linkedin.com/pulse/obd-ii-connector-fault-codes-explained-kiril-mucevski. [Accessed 24 11 2017].

6 APPENDICES

6.1APPENDIX 1: CURTIS 1238 TROUBLESHOOTING CHART

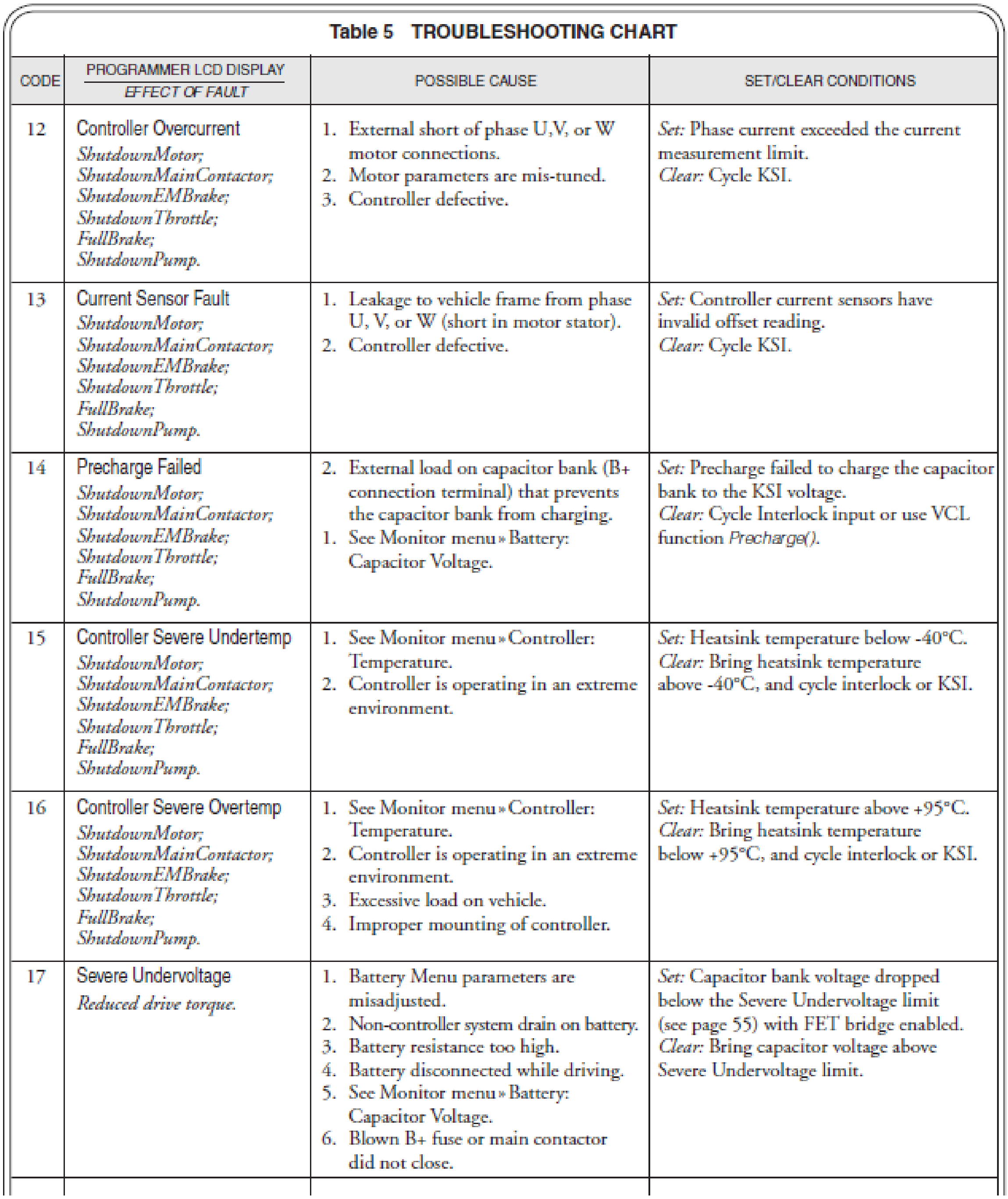


Table 5 TROUBLESHOOTING CHART

CODE	PROGRAMMER LCD DISPLAY *EFFECT OF FAULT*	POSSIBLE CAUSE	SET/CLEAR CONDITIONS

12	Controller Overcurrent
	ShutdownMotor;
	ShutdownMainContactor;
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake;
	ShutdownPump.
		1. External short of phase U,V, or W motor connections.
		2. Motor parameters are mis-tuned.
		3. Controller defective.
			Set: Phase current exceeded the current measurement limit.
			Clear: Cycle KSI.

13	Current Sensor Fault
	ShutdownMotor;
	ShutdownMainContactor;
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake;
	ShutdownPump.
		1. Leakage to vehicle frame from phase U, V, or W (short in motor stator).
		2. Controller defective.
			Set: Controller current sensors have invalid offset reading.
			Clear: Cycle KSI.

14	Precharge Failed
	ShutdownMotor;
	ShutdownMainContactor;
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake;
	ShutdownPump.
		2. External load on capacitor bank (B+ connection terminal) that prevents the capacitor bank from charging.
		1. See Monitor menu » Battery: Capacitor Voltage.
			Set: Precharge failed to charge the capacitor bank to the KSI voltage.
			Clear: Cycle Interlock input or use VCL function Precharge().

15	Controller Severe Undertemp
	ShutdownMotor;
	ShutdownMainContactor;
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake;
	ShutdownPump.
		1. See Monitor menu » Controller: Temperature.
		2. Controller is operating in an extreme environment.
			Set: Heatsink temperature below -40°C.
			Clear: Bring heatsink temperature above -40°C, and cycle interlock or KSI.

16	Controller Severe Overtemp
	ShutdownMotor;
	ShutdownMainContactor;
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake;
	ShutdownPump.
		1. See Monitor menu » Controller: Temperature.
		2. Controller is operating in an extreme environment.
		3. Excessive load on vehicle.
		4. Improper mounting of controller.
			Set: Heatsink temperature above +95°C.
			Clear: Bring heatsink temperature below +95°C, and cycle interlock or KSI.

17	Severe Undervoltage *Reduced drive torque.*	1. Battery Menu parameters are misadjusted. 2. Non-controller system drain on battery. 3. Battery resistance too high. 4. Battery disconnected while driving. 5. See Monitor menu » Battery: Capacitor Voltage. 6. Blown B+ fuse or main contactor did not close.	*Set:* Capacitor bank voltage dropped below the Severe Undervoltage limit (see page 55) with FET bridge enabled. *Clear:* Bring capacitor voltage above Severe Undervoltage limit.

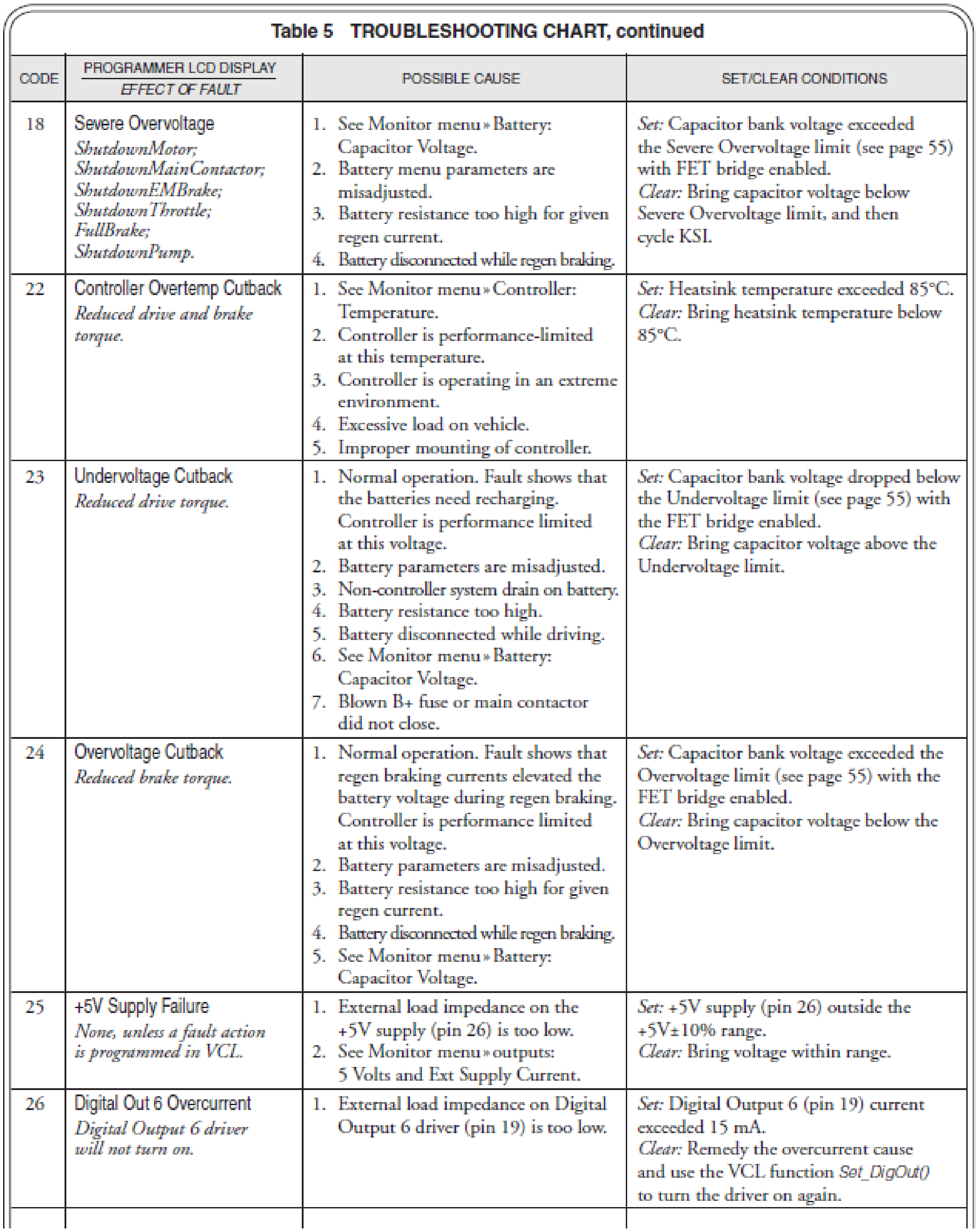


Table 5 TROUBLESHOOTING CHART, continued

CODE	PROGRAMMER LCD DISPLAY *EFFECT OF FAULT*	POSSIBLE CAUSE	SET/CLEAR CONDITIONS

18	Severe Overvoltage
	ShutdownMotor;
	ShutdownMainContactor;
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake;
	ShutdownPump.
		1. See Monitor menu » Battery: Capacitor Voltage.
		2. Battery menu parameters are misadjusted.
		3. Battery resistance too high for given regen current.
		4. Battery disconnected while regen braking.
			Set: Capacitor bank voltage exceeded the Severe Overvoltage limit (see page 55) with FET bridge enabled.
			Clear: Bring capacitor voltage below Severe Overvoltage limit, and then cycle KSI.

22	Controller Overtemp Cutback *Reduced drive and brake torque.*	1. See Monitor menu » Controller: Temperature. 2. Controller is performance-limited at this temperature. 3. Controller is operating in an extreme environment. 4. Excessive load on vehicle. 5. Improper mounting of controller.	*Set:* Heatsink temperature exceeded 85°C. *Clear:* Bring heatsink temperature below 85°C.
23	Undervoltage Cutback *Reduced drive torque.*	1. Normal operation. Fault shows that the batteries need recharging. Controller is performance limited at this voltage. 2. Battery parameters are misadjusted. 3. Non-controller system drain on battery. 4. Battery resistance too high. 5. Battery disconnected while driving. 6. See Monitor menu » Battery: Capacitor Voltage. 7. Blown B+ fuse or main contactor did not close.	*Set:* Capacitor bank voltage dropped below the Undervoltage limit (see page 55) with the FET bridge enabled. *Clear:* Bring capacitor voltage above the Undervoltage limit.
24	Overvoltage Cutback *Reduced brake torque.*	1. Normal operation. Fault shows that regen braking currents elevated the battery voltage during regen braking. Controller is performance limited at this voltage. 2. Battery parameters are misadjusted. 3. Battery resistance too high for given regen current. 4. Battery disconnected while regen braking. 5. See Monitor menu » Battery: Capacitor Voltage.	*Set:* Capacitor bank voltage exceeded the Overvoltage limit (see page 55) with the FET bridge enabled. *Clear:* Bring capacitor voltage below the Overvoltage limit.
25	+5V Supply Failure *None, unless a fault action is programmed in VCL.*	1. External load impedance on the +5V supply (pin 26) is too low. 2. See Monitor menu » outputs: 5 Volts and Ext Supply Current.	*Set:* +5V supply (pin 26) outside the +5V±10% range. *Clear:* Bring voltage within range.
26	Digital Out 6 Overcurrent *Digital Output 6 driver will not turn on.*	1. External load impedance on Digital Output 6 driver (pin 19) is too low.	*Set:* Digital Output 6 (pin 19) current exceeded 15 mA. *Clear:* Remedy the overcurrent cause and use the VCL function *Set_DigOut()* to turn the driver on again.

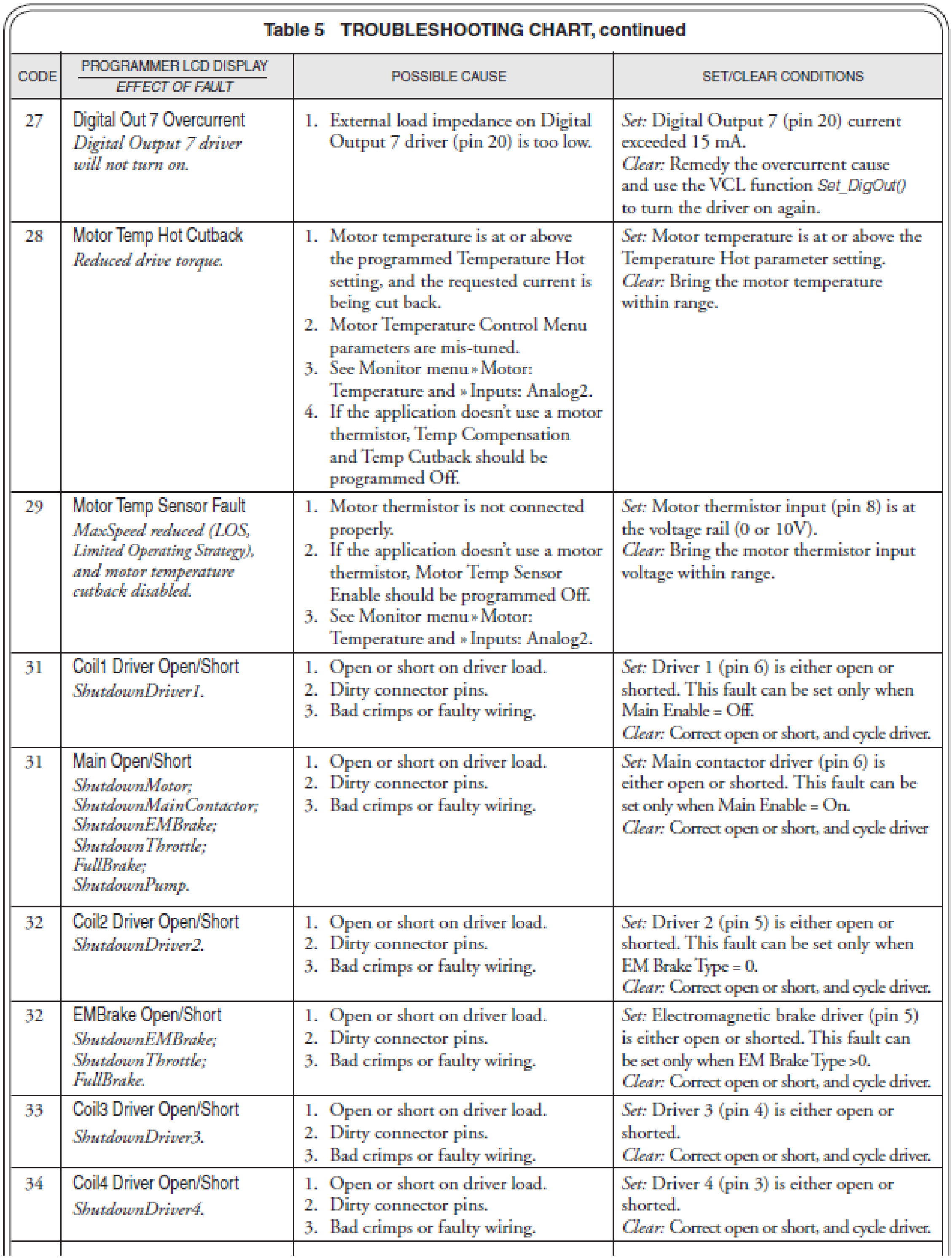


Table 5 TROUBLESHOOTING CHART, continued

CODE	PROGRAMMER LCD DISPLAY *EFFECT OF FAULT*	POSSIBLE CAUSE	SET/CLEAR CONDITIONS
27	Digital Out 7 Overcurrent *Digital Output 7 driver will not turn on.*	1. External load impedance on Digital Output 7 driver (pin 20) is too low.	*Set:* Digital Output 7 (pin 20) current exceeded 15 mA. *Clear:* Remedy the overcurrent cause and use the VCL function *Set_DigOut()* to turn the driver on again.
28	Motor Temp Hot Cutback *Reduced drive torque.*	1. Motor temperature is at or above the programmed Temperature Hot setting, and the requested current is being cut back. 2. Motor Temperature Control Menu parameters are mis-tuned. 3. See Monitor menu » Motor: Temperature and » Inputs: Analog2. 4. If the application doesn't use a motor thermistor, Temp Compensation and Temp Cutback should be programmed Off.	*Set:* Motor temperature is at or above the Temperature Hot parameter setting. *Clear:* Bring the motor temperature within range.
29	Motor Temp Sensor Fault *MaxSpeed reduced (LOS, Limited Operating Strategy), and motor temperature cutback disabled.*	1. Motor thermistor is not connected properly. 2. If the application doesn't use a motor thermistor, Motor Temp Sensor Enable should be programmed Off. 3. See Monitor menu » Motor: Temperature and » Inputs: Analog2.	*Set:* Motor thermistor input (pin 8) is at the voltage rail (0 or 10V). *Clear:* Bring the motor thermistor input voltage within range.
31	Coil1 Driver Open/Short *ShutdownDriver1.*	1. Open or short on driver load. 2. Dirty connector pins. 3. Bad crimps or faulty wiring.	*Set:* Driver 1 (pin 6) is either open or shorted. This fault can be set only when Main Enable = Off. *Clear:* Correct open or short, and cycle driver.

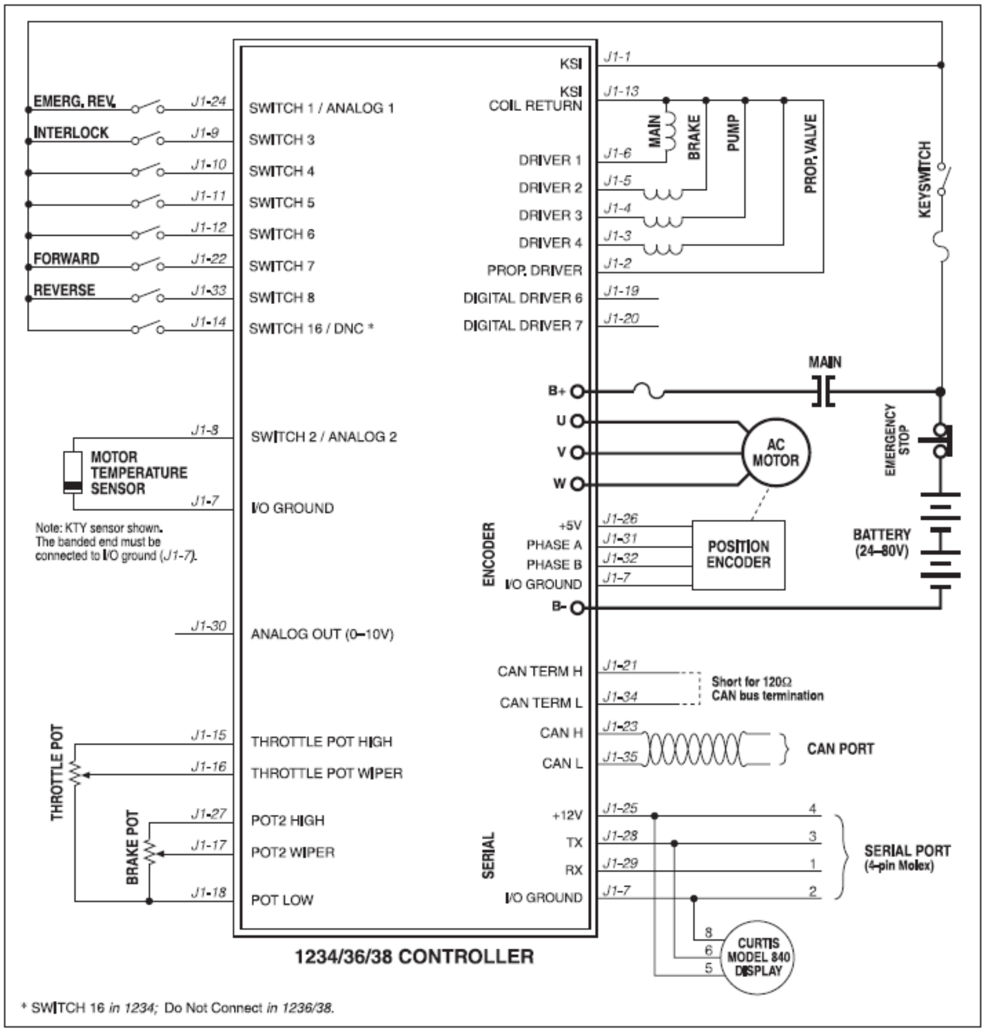
31	Main Open/Short
	ShutdownMotor;
	ShutdownMainContactor;
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake;
	ShutdownPump.
		1. Open or short on driver load.
		2. Dirty connector pins.
		3. Bad crimps or faulty wiring.
			Set: Main contactor driver (pin 6) is either open or shorted. This fault can be set only when Main Enable = On.
			Clear: Correct open or short, and cycle driver

32	Coil2 Driver Open/Short *ShutdownDriver2.*	1. Open or short on driver load. 2. Dirty connector pins. 3. Bad crimps or faulty wiring.	*Set:* Driver 2 (pin 5) is either open or shorted. This fault can be set only when EM Brake Type = 0. *Clear:* Correct open or short, and cycle driver.

32	EMBrake Open/Short
	ShutdownEMBrake;
	ShutdownThrottle;
	FullBrake.
		1. Open or short on driver load.
		2. Dirty connector pins.
		3. Bad crimps or faulty wiring.
			Set: Electromagnetic brake driver (pin 5) is either open or shorted. This fault can be set only when EM Brake Type >0.
			Clear: Correct open or short, and cycle driver.

33	Coil3 Driver Open/Short *ShutdownDriver3.*	1. Open or short on driver load. 2. Dirty connector pins. 3. Bad crimps or faulty wiring.	*Set:* Driver 3 (pin 4) is either open or shorted. *Clear:* Correct open or short, and cycle driver.
34	Coil4 Driver Open/Short *ShutdownDriver4.*	1. Open or short on driver load. 2. Dirty connector pins. 3. Bad crimps or faulty wiring.	*Set:* Driver 4 (pin 3) is either open or shorted. *Clear:* Correct open or short, and cycle driver.

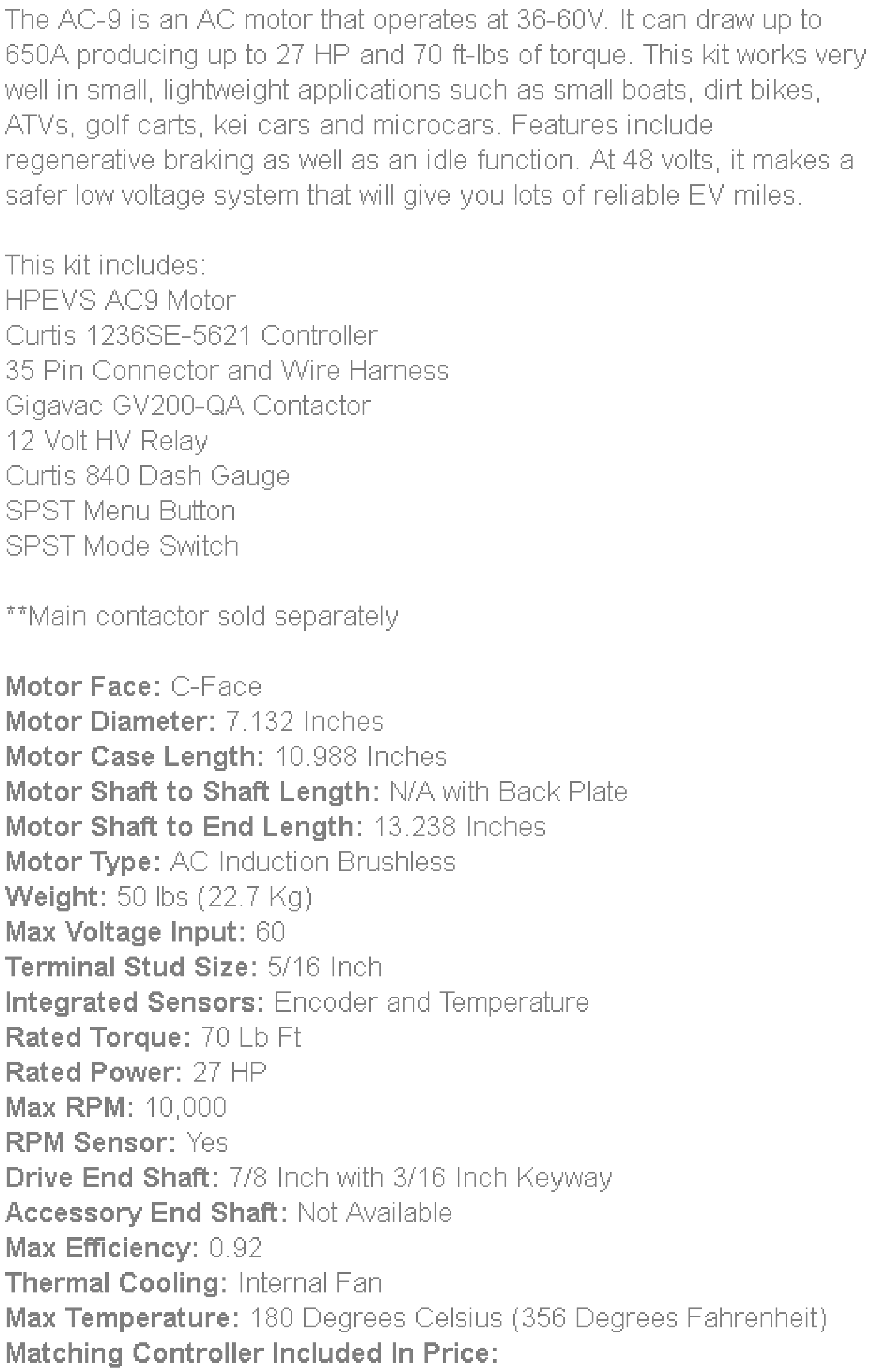
6.2APPENDIX 2: CURTIS 1238 WIRE DIAGRAM



Note: KTY sensor shown. The banded end must be connected to I/O ground (*J1-7*).

* SWITCH 16 *in 1234;* Do Not Connect *in 1236/38.*

6.3APPENDIX 3: MOTOR DATASHEET



The AC-9 is an AC motor that operates at 36-60V. It can draw up to 650A producing up to 27 HP and 70 ft-lbs of torque. This kit works very well in small, lightweight applications such as small boats, dirt bikes, ATVs, golf carts, kei cars and microcars. Features include regenerative braking as well as an idle function. At 48 volts, it makes a safer low voltage system that will give you lots of reliable EV miles.

This kit includes:
HPEVS AC9 Motor
Curtis 1236SE-5621 Controller
35 Pin Connector and Wire Harness
Gigavac GV200-QA Contactor
12 Volt HV Relay
Curtis 840 Dash Gauge
SPST Menu Button
SPST Mode Switch

**Main contactor sold separately

Motor Face: C-Face
Motor Diameter: 7.132 Inches
Motor Case Length: 10.988 Inches
Motor Shaft to Shaft Length: N/A with Back Plate
Motor Shaft to End Length: 13.238 Inches
Motor Type: AC Induction Brushless
Weight: 50 lbs (22.7 Kg)
Max Voltage Input: 60
Terminal Stud Size: 5/16 Inch
Integrated Sensors: Encoder and Temperature
Rated Torque: 70 Lb Ft
Rated Power: 27 HP
Max RPM: 10,000
RPM Sensor: Yes
Drive End Shaft: 7/8 Inch with 3/16 Inch Keyway
Accessory End Shaft: Not Available
Max Efficiency: 0.92
Thermal Cooling: Internal Fan
Max Temperature: 180 Degrees Celsius (356 Degrees Fahrenheit)
Matching Controller Included In Price: