Team 16 - Cybersecurity Considerations for Rolls-Royce

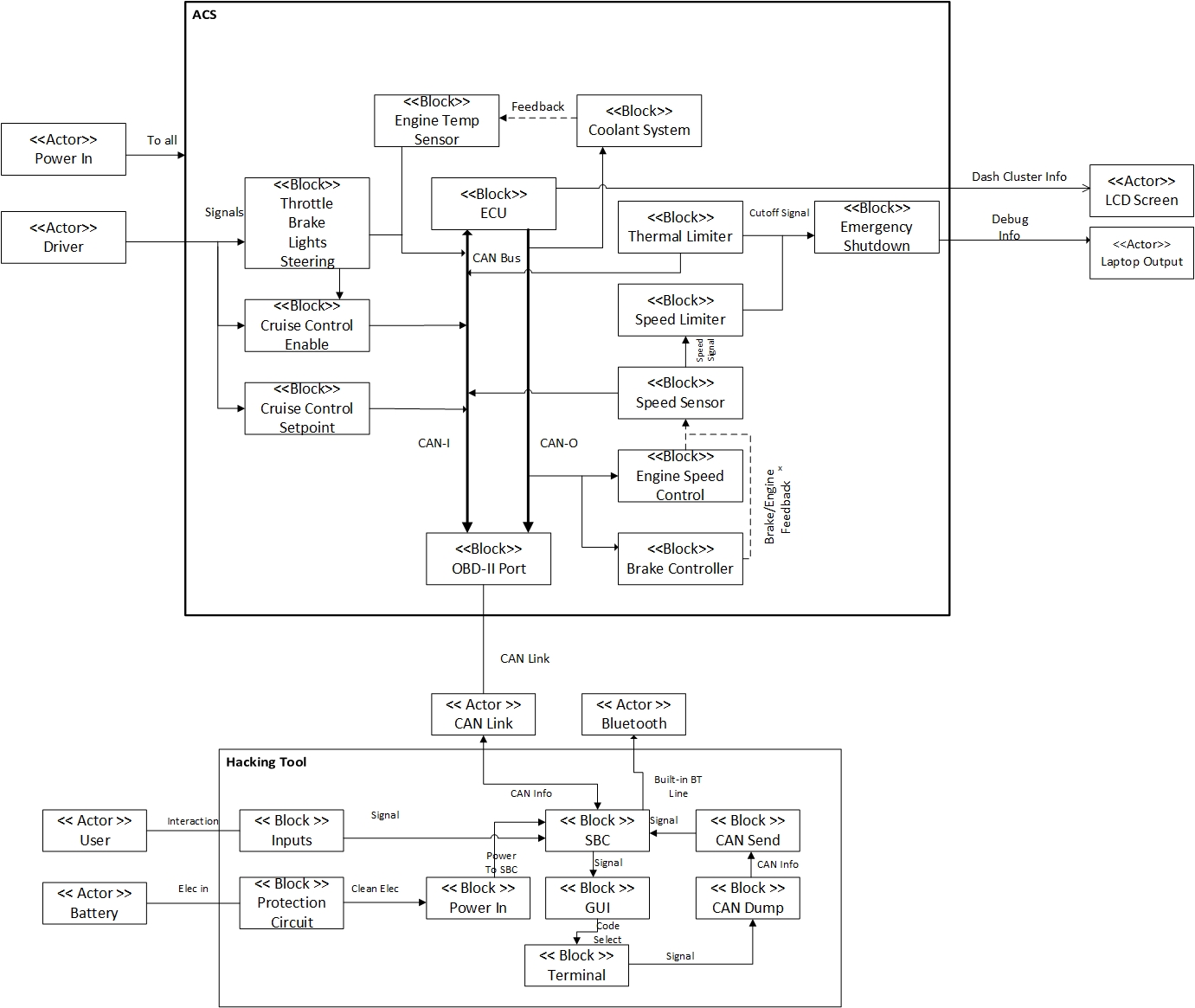
Assignment: System Decomposition and Requirements

# Executive Summary

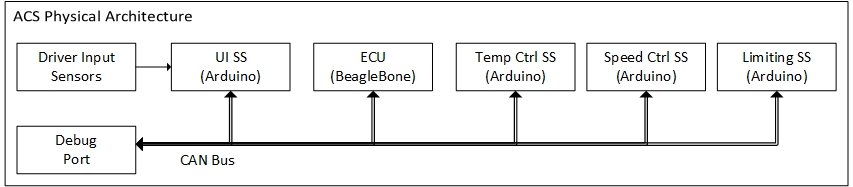
Cars have had more technological advancements done to them in the last 15 years than all the years before since they began being mass produced. This mass growth in the car industry is not an isolated event. Across all industries, we are creating new technologies faster than we are able to master the old technologies. Even industries that have been notorious for being slow to adapting to new technologies are now changing quicker than ever before, including the automotive industry. The implementation of these new technologies is having a positive impact on people’s daily lives. Cars are becoming more fuel efficient and environmentally safe, from a manufacturing standpoint as well as an emissions standpoint. Cars are also getting new features that have increased the safety of the driver of the car as well as anyone else around.. This includes during collisions and also with features such as lane departure detection, better headlights, distance locking cruise control, and other similar features. However, all of these technologies are being implemented without thinking about the repercussions. With new technologies comes new ways for dangerous people to be able to hack in these connected devices. It goes without saying that there a huge safety concern if someone were to be able to hack into a vehicle, especially if it were moving. This is where our project comes into focus.

We are tasked with designing a control system that is an adequate analogy for a modern control system in today’s cars. For our project, this comes in the form of a CAN bus system comprised up of arduino minis and a beaglebone black. A CAN bus network was created because that is the industry standard for the communication used internally in almost every vehicle on the market. Our network is broken up into multiple nodes, with each arduino handling different aspects of a vehicle’s internal network, such as speedometer, temperature sensors, and breaking. The beaglebone black will be used to act as the vehicle’s ECU, which does the interpolation of the information being sent on the CAN bus. Then once our system is designed, we must think of different ways to hack into the system and compromise the signals being sent and received. Once again, this will be done with a different beaglebone black. We will connect our beaglebone black directly to our CAN bus network and perform different attacks such as DDOS attack and man-on-the-middle attack. Once we have identified multiple security risks, we then need to devise and document cheap and effective ways to harden the system from these attacks. We will be constructing a duplicate version of the system that is our CAN bus, the arduinos and beaglebone black aforementioned. Once this network has been duplicated and has been tested to confirm that it is running the same way as the original network, we will harden it against the malicious attacks mentioned above. The creation of a second system is done for demonstration purposes so we have a way of showing our clients what hacks can be performed on a standard, unprotected CAN bus and then show what a hardened CAN bus network looks like and how well it stands up to the same hacks as the other system.

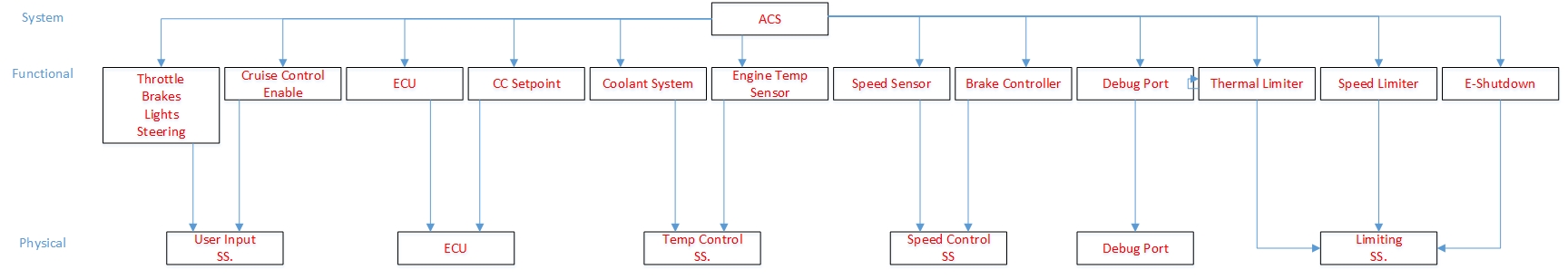
# Decomposition and Physical Synthesis



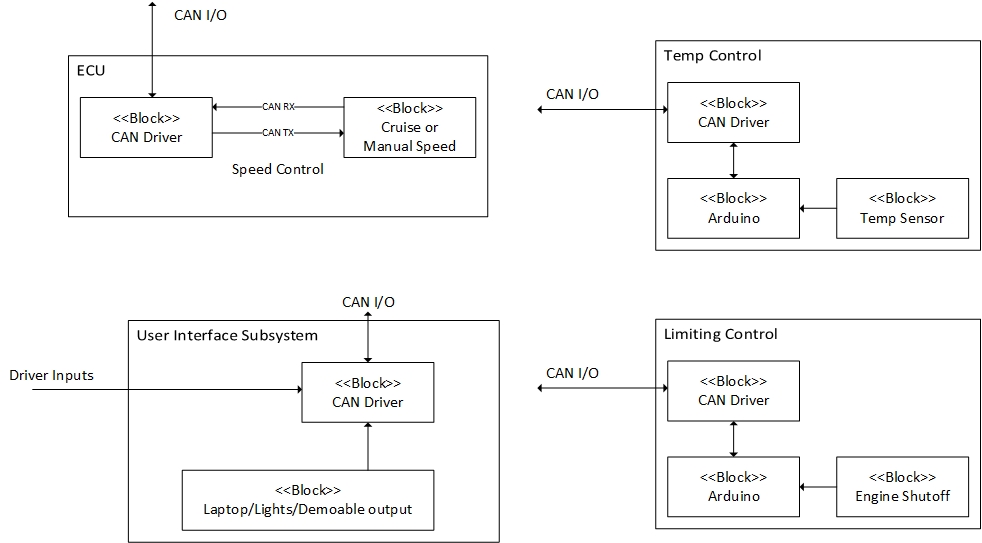
**Figure 1** - Functional Architecture of the ACS and Hacking Tool.



**Figure 2:** An illustration of the functional and physical architectures.



**Figure 3:** ORG chart that shows a mapping of functional behaviors to physical subsystems and further decomposition of those physical subsystems.

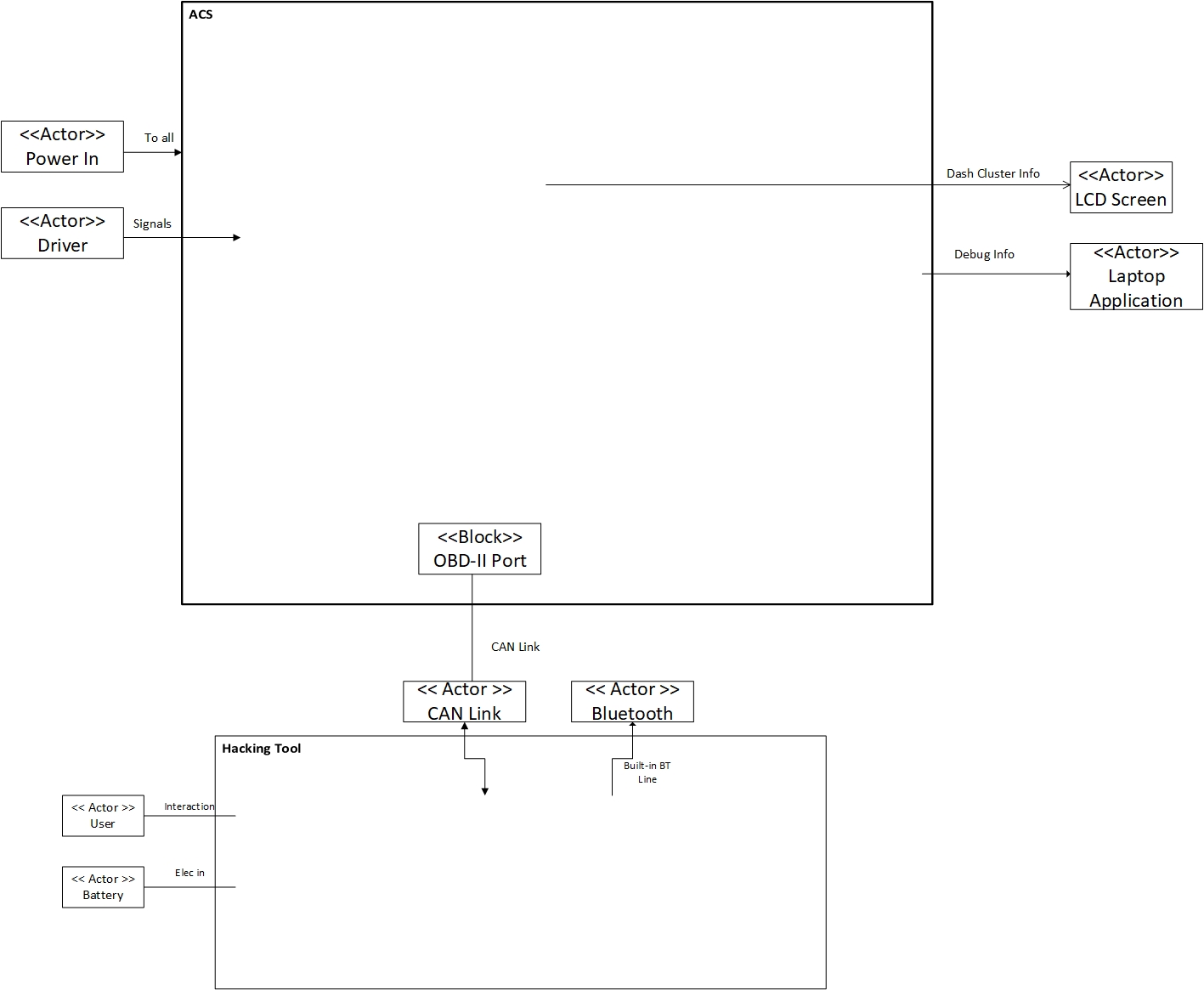


**Figure 4:** An illustration of decomposition of the ECU, UI, Temp Control, and Limiting Control Subsystems

The Analogous Car System, or ACS, is a control system comprised of a discrete set of nodes communicating over a common bus, seen in figure 2. Each node is physically very similar, with an Arduino mini microcontroller (or beaglebone black in the case of the ECU) connected to a CAN transceiver and a set of sensors and outputs. This sensor or output connection along with its supporting code is what then makes each node unique - making the temperature control system read and report engine temperature, the speed control subsystem monitor and control the ‘speed of the car’, etc. The breakdown of these I/Os can be seen in figure 4.

This modular architecture mimics that of the general architecture of a modern car’s control system, and allows us to develop and perform theoretical attacks that would affect a real car control system. The architecture then allows us to attempt to harden against these same attacks in a manner that could also be applied back to a modern car (with some developmental work).

# Black-Box Technical Requirements

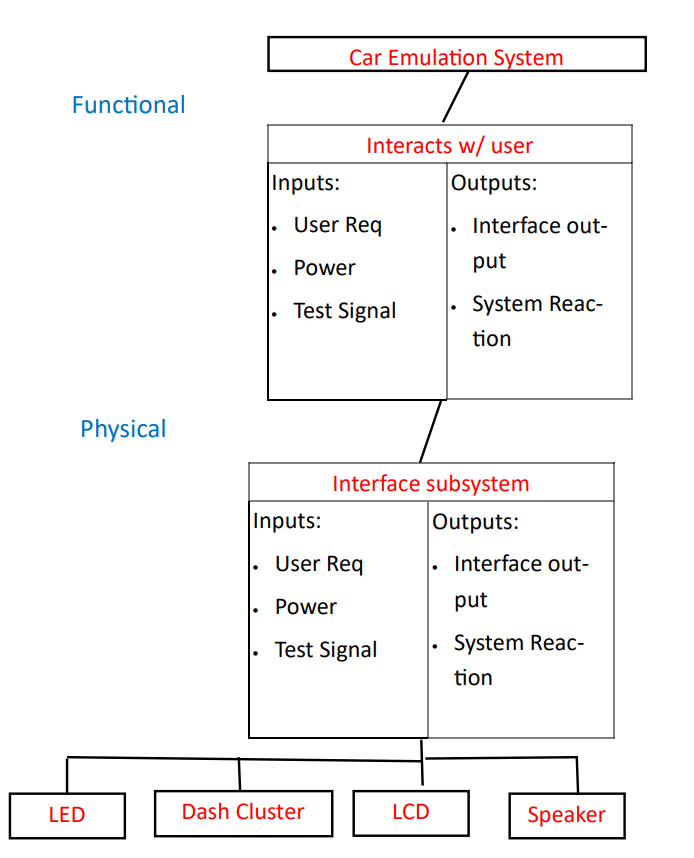


**Figure 5:** A subset of the functional architecture that shows only the actors and the system involved in the Interaction.

**Table 1: Illustration of Black-Box Technical Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I/Os** | **ID** | **Requirement** | **Feature(s)** | **Verified By** |
| [Power] To all | ACS-1 | The ACS shall accept a [Power] to all systems at a [Wall Voltage of 120VRMS] and [5VDC, 1 Amp] is supplied to all subsystems. | Maintainable  Safety | Instrument Test |
| [Driver] Signals | ACS-2 | The ACS shall take input signals (Steering, Lighting, Brakes, Throttle, Cruise Control) from a [Driver] user and use these to adjust outputs of the system (Coolant System, Speed Limiter, Engine Speed Control, Brake Control, and Emergency Shutdown System). | Safety  Security | Demonstration  Instrument Test |
| [OBD-II] Can Link | ACS-3 | The ACS shall have an On-Board Diagnostic port for easily debugging problems | Maintainable  Cots | Demonstration |
| DEMO Outputs | ASC-4 | The ACS shall give DEMO Outputs for [showing user input, ECU output, and CAN bus information] | Safety  Security | Demonstration |
| [User] Interaction | HKT-1 | The Hacking tool shall take inputs from a [Hacker] user and use these to select what type of hack they would like to perform to [show a demonstrable attack] | Security | Demonstration  Instrument Test  Code Test |
| [Battery] Elec in | HKT-2 | The Hacking tool shall accept a [Battery] Electrical Power in at [5VDC, 1Amp] so that it may be portable. | Security  Manufacturability  Safety | Instrument Test |
| CAN Link | HKT-3 | The Hacking tool shall have an exposed CAN link so that it may be [connected to the OBD-II port] or [spliced onto the CAN bus] if said port is missing. | Security | Demonstration |
| Bluetooth | HKT-4 | The Hacking tool shall use bluetooth to [send/receive data] from the CAN bus as well as be used for [probable attack vectors]. | Security | Demonstration  Code Test |

# Validating the Physical Architecture



**Figure 5:** Tracing the I/Os through the physical subsystem.

# Decision Matrix

After we successfully perform malicious attacks on the analogous car system we designed, we have to harden the system to show that these attacks can be prevented. The Decision Matrix below was used so we could come up with a decision on if it was best to keep the hardened car system separate from the original systems, or just have the two together. As you can see below, we decided to go with having two separate system. One of the positives from this decision that is not demonstrated from the Decision Matrix is that by having two systems that are nearly identical means that we have backup parts if one of the systems goes down. This also means that recreating the Hardened system should go relatively smoothly since it is the same system until it gets hardened.

**Table 2: Decision Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Weight** | **15%** | **40%** | **20%** | **25%** | **100%** |
| **Option** | **Price ($)** | **Simplicity for Demonstration Purposes** | **Transportation & Setup** | **Design Complexity** | **Total Score** |
| Two Separate Analogous Car Systems (Hardened and Original) | 1 | 3 | 2 | 3 | 2.5 |
| One Analogous Car System (Ability to have ‘hardened’ portion turned off) | 3 | 2 | 3 | 1 | 2.1 |

Each weight given to the different categories were assigned largely based on which of these categories were most useful for us to be able to effectively present our findings to our clients. For instance, the simplicity for demonstration purposes category had the most weight because we do not want to have to spend a lot of presentation time just to describe to the audience what they are looking at. The design needs to be intuitive so our presentation can focus on educating our audience on the aspects of our system that is most important to them, the cybersecurity. The next category that we deemed most important was the design complexity. We thought this because we want to make sure that the information we are presenting to our clients is extensive enough so we are actually exposing them to information that they should not be familiar with already. Keeping with the theme of valuing aspects which make our project easier to present, we valued the transportation and setup of our system to be the third most valuable category in the decision matrix. Since our entire project is an education tool, it should be easy to take down, transport, and set back up relatively easily. We value this because this will allow our presentation to go smoothly and not have to spend a lot of time beforehand making sure that everything is setup and working before we present. This also goes hand in hand with our simplicity for demonstration purposes category. If the physical design of our system is simple, then we should be able to package it in a way that allows for simple transportation and setup. The last category that we had to consider, as with any engineering project, was the price of the system. We valued this least important because we knew that no matter which design decision we decided to go with that we would be well under our budget. Though we still have to make a conscious effort to be frugal with what we are given.