1 Introduction to the Student CyberTruck Experience

1.1 Trucking as a Critical Infrastructure

Transporting material by truck is a critical aspect of modern life. The Transportation Systems Sector has been declared a critical infrastructure sector by the Department of Homeland Security (DHS) [?]. Therefore, protecting trucks, trailers, vans, buses and the logistic engines supporting these vehicles is of the utmost importance for our way of life.

In the mid 1990s, the technology used on heavy vehicle transitioned from mechanical controls to digital controls. For many years, these digital controls and embedded systems were isolated from the rest of the world unless accessed by a technician. This is known as an air gap. However, the trucking industry realized process improvements through remote monitoring of the vehicles and their status. Technologies like over-the-air updates have become part of the truck and its supporting systems. This broke down the air gap defense and trucks may be connected to the Internet by way of a cellular modem. With the truck network connected to an outside network, there is a possibility for a vulnerability to be exploited and an attacker to remotely execute code on the truck. This is problematic, because the truck systems are trusting of the internal network and will react without regard the authenticity of a message. This means a well crafted message on the internal network can wreak havoc on the truck and potentially shut it down... or worse. Keep in mind, a truck traveling at 70 miles per hour carrying 80,000 lb has an large amount of energy. Here is a quick example of the kinetic energy calculation for moving truck:

$$KE = \frac{1}{2}mv^2$$

$$KE = \frac{1}{2}\frac{W}{g}(1.466S)^2$$

$$KE = \frac{80,000}{2(32.2)}[1.466(70)]^2$$

$$KE = 13,081,819\,\text{ft-lb}$$

For comparison, a .30-06 rifle can propel a 0.308 inch diameter bullet at 3000 ft/second, which is around 3000 ft-lbs of energy. In other words, a truck has as much energy as 4360 rifles being fired at once!

The ability for a truck to cause serious damage in a crash is significant. Crashes are perhaps the most spectacular outcome of a cyber attack, but other subversive results can be achieved, like theft, logistics disruption, a traffic congestion. One particularly scary scenario is if a cyber attack affects many trucks at the same time. The tow and recovery services can easily respond to a couple broken-down trucks, but if thousands of truck came to a halt at the same time, the highway system would be broken. This means medical supplies, food, and fuel are no longer distributed. Its only a few days before serious civil unrest would start if trucking gets shut down. Brainstorming terrible scenarios is somewhat trivial, but our goal is to develop solutions. A compelling industry report from the NMFTA provides much of the rational to address the problem of heavy vehicle cybersecurity [**?**]. The reason for this book and the accompanying Student CyberTruck Experience is to teach the engineers and scientists the necessary elements needed to improve the cybersecurity posture of the transportation industry.

How the Student CyberTruck Experience Started

In 2016, Urban Jonson of the National Motor Freight Traffic Association, Inc. (NMFTA) reached out to Dr. Jeremy Daily while he was teaching mechanical engineering at the University of Tulsa (TU) to discuss some research findings related to heavy vehicle cybersecurity. In this conversation, Dr. Daily confirmed many of the hypotheses in the NMFTA whitepaper on the state of heavy vehicle cybersecurity. This conversation led to an invitation for Dr. Daily to attend the first NMFTA Heavy Vehicle Cyber Security (HVCS) meeting in Virginia. One of the results of the meeting was a recognition for the need to build the human talent needed to address the challenges associated with cybersecurity of heavy vehicles. This initiative is how the Student CyberTruck Experience came into being. A detailed account of the lessons learned in developing heavy vehicle cybersecurity talent was presented at the ESCAR USA 2017 conference [**?**].

1.2 Program Mission

The mission of the Student CyberTruck Experience is to *develop the talent necessary to improve the cybersecurity posture of heavy vehicles.*

This mission is intended to be high level and focused on the big picture. However, it is too general and hard to measure the actual achievement of the mission. There are a few indicators that the program is succeeding in its mission:

1. Graduates of the program have been hired into the industry in a cybersecurity capacity.

2. Graduates have gone onto graduate school and created scholarly works contributing to the body of science around heavy vehicle cybersecurity.

3. Student participants have attended and participated in the CyberTruck Challenge, thus building the overall awareness around heavy vehicle cybersecurity.

4. External sponsors continue to sponsor the research project, which enables undergraduates to focus summer research efforts towards heavy vehicle cybersecurity.

5. The ideas and projects from the Student CyberTruck Experience have been used as ideas for other funded research projects at the federal level.
6. Students consistently receive positive feedback at the HVCS bi-annual meetings.

While this is great feedback as to the success of the program, we need a more measured approach to help students and researchers progress through the program and maximize their potential. There is a famous saying:

> You can only improve what you measure.

This calls for some measurable program learning objectives.

1.3 Program Learning Objectives

As suggested by Sara Rathburn from Colorado State University's The Institute for Teaching and Learning, learning objectives are written statements organizing and defining the specific knowledge, skill-sets, and/or abilities students should acquire [?]. These learning objectives help students assess their skills and provide specifics for the learning journey to become a productive cybersecurity practitioner. An effective learning objective has three parts:

1. A description of what is expected.
2. The conditions necessary to demonstrate proficiency.
3. The criteria for evaluating performance.

For example, a Program Learning Example could be

- Create a program to reassemble messages that arrive out of order from a J1939 Transport Protocol - Data Transfer to properly receive the data in the same order in which it was sent.

Looking at this objective, there is a clear output of what output is expected. Specifically, the output is the computer program. However, the language writing the code is not specified, so any language would be acceptable. The conditions for the exercise is an out of order message stream from J1939 network. Success will be achieved when the original byte stream matches the reassembled message. The primary action verb in this objective is the word create. Different action verbs suggest different levels of learning, which has been popularized as Bloom's Taxonomy.

1.3.1 The Taxonomy of Educational Objectives (Bloom's Taxonomy)

When developing new course for university, we have to generate a set of course objectives. A well reasoned approach is to create objectives that start with the phrase "By the end of this course, students should be able to..." and the rest of the sentence is the learning objective. To create the learning objective, an action verb is used followed by the object of knowledge they are expected to acquire or construct. There are multiple dimensions of knowledge as well as different levels of thinking about things. A succinct info-graphic was produced at Iowa State University under a Creative Commons License and displayed in Figure 1.1 on the following page. The examples and breakdown of the learning objective space shown in the figure will be used to span the basis for talent generation for the Student CyberTruck Experience.

The learning objectives should focus on accomplishing the program mission. Since the topic of cybersecurity is rapidly changing in the modern era, the learning objectives may need to change to accommodate advances in technology, knowledge, and application. For example, the advent of quantum computing promises to create a paradigm shift in modern cryptography as many “hard” problems that are used as the basis for modern cryptography can be calculated quickly, thus nullifying the underlying algorithms. As of this writing, there have been no practical exploits based on quantum computing.

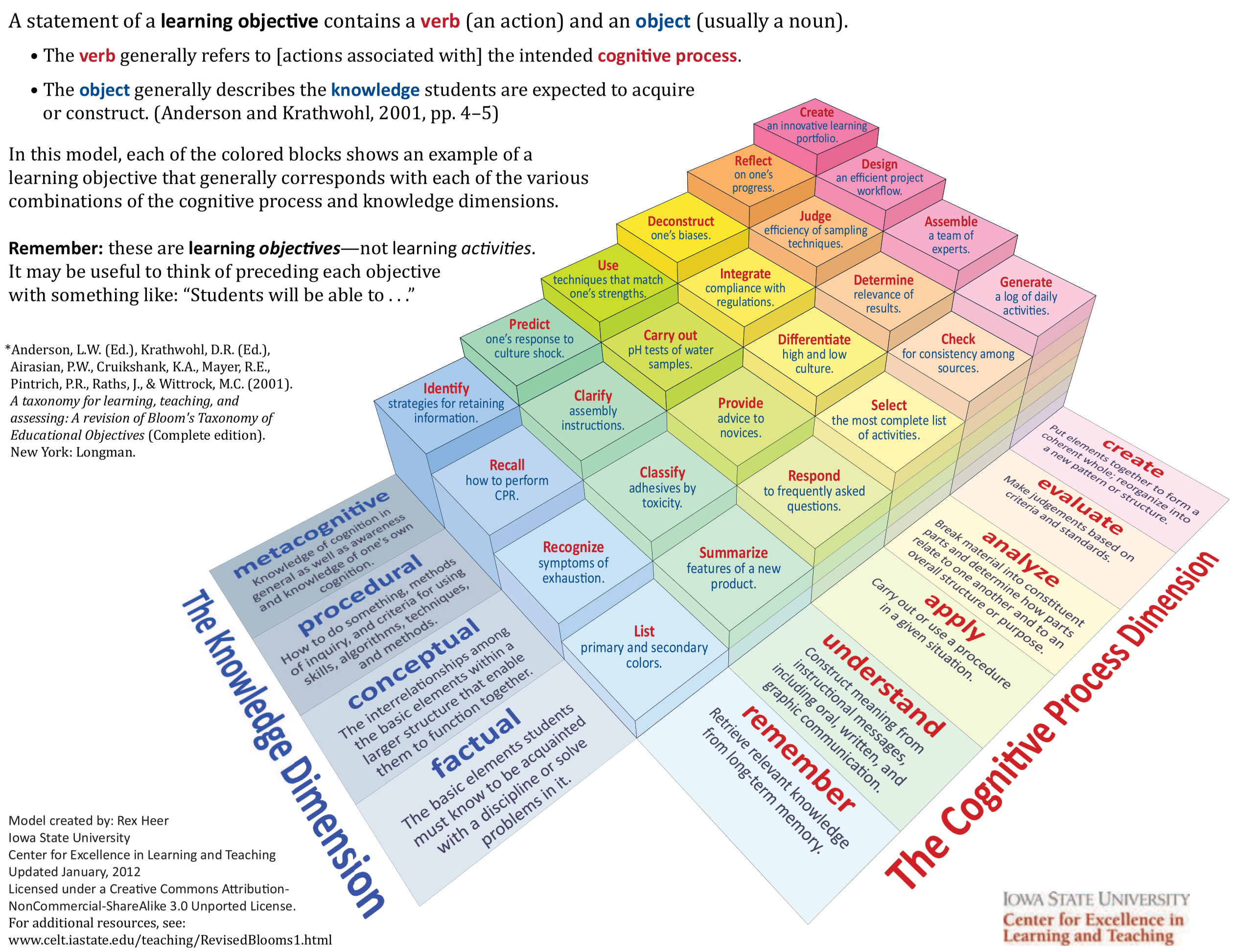
Often Bloom’s Taxonomy is constructed as a pyramid or cake as shown in Figure 1.2 on page 6. This is a simpler graphic to digest and use as a model for your own level of knowledge. Often the base layers are necessary to accomplish a mastery of a higher layer. For example, to apply a cryptographic algorithm on a heavy truck network, you would need to understand the limitations of J1939 and have knowledge of the truck system. The larger foundations are needed to achieve the higher order thinking. This means learning objectives that are focused on the top of the pyramid, like evaluate and create, require a mastery of the layers below. Thus students should strive to achieve the highest level of contemplation in an effort to have the broadest experience.

However, when a new student is introduced to a field, like heavy vehicle cybersecurity, they cannot immediately go to the top layer. Moreover, the process of building the knowledge foundation is critical to success. As such, the learning objectives in the program will vary across the cognitive process dimension. This enables a student to enter the program at their level and still have a objectives to challenge them. For example, a computer science student may have training and experience using data structures in C and an engineering student may have practical experience fixing air brake systems. These students would each bring their own level of expertise to the program and enter the quest for knowledge at different levels. The CS student may be able to quickly declare a structure for a CAN data frame in a C header file, but the ME student may need to learn about C data structures and data types, then understand how to create a struct. In other words, the level of effort in achieving mastery of the learning objectives may be different for each student.

1.3.2 Program Learning Objectives

To achieve the program mission, students who go through the Student CyberTruck Experience (CyTeX) should be able to...

1. List the major Original Equipment Manufacturers (OEM) and Tier 1 Suppliers for on-highway heavy vehicles.



A statement of a **learning objective** contains a **verb** (an action) and an **object** (usually a noun).

- The **verb** generally refers to [actions associated with] the intended **cognitive process**.
- The **object** generally describes the **knowledge** students are expected to acquire or construct. (Anderson and Krathwohl, 2001, pp. 4–5)

In this model, each of the colored blocks shows an example of a learning objective that generally corresponds with each of the various combinations of the cognitive process and knowledge dimensions.

Remember: these are **learning *objectives***—not learning *activities*. It may be useful to think of preceding each objective with something like: "Students will be able to . . ."

*Anderson, L.W. (Ed.), Krathwohl, D.R. (Ed.), Airasian, P.W., Cruikshank, K.A., Mayer, R.E., Pintrich, P.R., Raths, J., & Wittrock, M.C. (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's Taxonomy of Educational Objectives* (Complete edition). New York: Longman.

Create an innovative learning portfolio.
Reflect on one's progress.
Design an efficient project workflow.
Deconstruct one's biases.
Judge efficiency of sampling techniques.
Assemble a team of experts.
Use techniques that match one's strengths.
Integrate compliance with regulations.
Determine relevance of results.
Generate a log of daily activities.
Predict one's response to culture shock.
Carry out pH tests of water samples.
Differentiate high and low culture.
Check for consistency among sources.
Identify strategies for retaining information.
Clarify assembly instructions.
Provide advice to novices.
Select the most complete list of activities.
Recall how to perform CPR.
Classify adhesives by toxicity.
Respond to frequently asked questions.
Recognize symptoms of exhaustion.
Summarize features of a new product.
List primary and secondary colors.
metacognitive
Knowledge of cognition in general as well as awareness and knowledge of one's own cognition.
procedural
How to do something, methods of inquiry, and criteria for using skills, algorithms, techniques, and methods.
conceptual
The interrelationships among the basic elements within a larger structure that enable them to function together.
factual
The basic elements students must know to be acquainted with a discipline or solve problems in it.
The Knowledge Dimension
create
Put elements together to form a coherent whole; reorganize into a new pattern or structure.
evaluate
Make judgements based on criteria and standards.
analyze
Break material into constituent parts and determine how parts relate to one another and to an overall structure or purpose.
apply
Carry out or use a procedure in a given situation.
understand
Construct meaning from instructional messages, including oral, written, and graphic communication.
remember
Retrieve relevant knowledge from long-term memory.
The Cognitive Process Dimension

Model created by: Rex Heer
Iowa State University
Center for Excellence in Learning and Teaching
Updated January, 2012
Licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
For additional resources, see:
www.celt.iastate.edu/teaching/RevisedBlooms1.html

Iowa State University
Center for Excellence in Learning and Teaching

Figure 1.1: Revised Bloom's Taxonomy used in creating learning objectives [?].

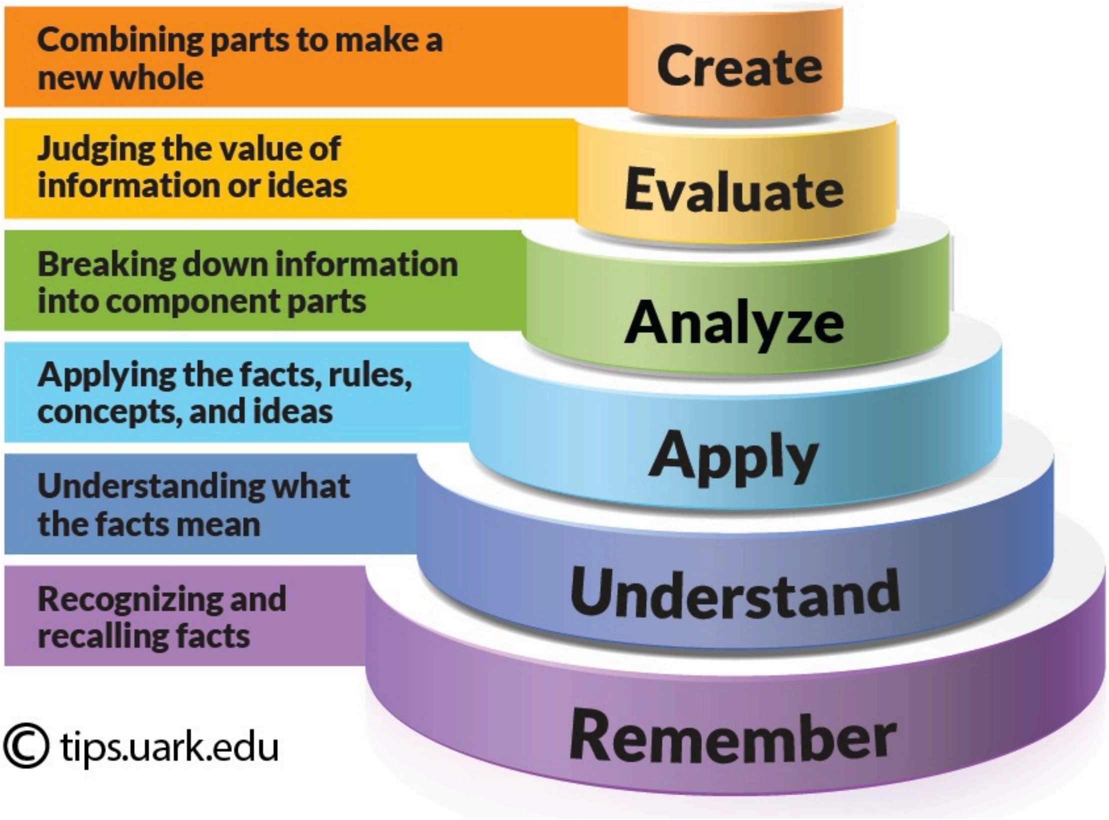

Combining parts to make a new whole
Create
Judging the value of information or ideas
Evaluate
Breaking down information into component parts
Analyze
Applying the facts, rules, concepts, and ideas
Apply
Understanding what the facts mean
Understand
Recognizing and recalling facts
Remember
© tips.uark.edu

Figure 1.2: Bloom's Taxonomy from Jessica Shabatura.

2. Recognize a unified diagnostic service (UDS) message in SAE J1939 communication.
3. Recall the different layers of the Open Systems Interconnection (OSI) networking model.
4. Identify the different electronic control units (ECUs) used on heavy vehicles.
5. Summarize the strengths and weaknesses of the controller area network.
6. Classify trucks and trailers by weight class and use.
7. Clarify the way CAN bus data is used for the freight carriers, OEMs, tier 1 suppliers and telematics providers.
8. Predict potential cybersecurity attacks through an electronic logging device (ELD).
9. Respond to J1939 request messages for VIN, Component Identification, and other J1939 on request messages.
10. Provide a secure API for a CAN to Ethernet electronic device to network log data on a computer.
11. Carry out cryptographic message authentication for intra-vehicle communications.
12. Use certificates and public key infrastructure (PKI) to securely update a vehicle connected device.
13. Select the fastest cryptographic approach to secure diagnostic communication between a gateway and a diagnostic application.
14. Differentiate between best practices for IT security and heavy vehicle network security.
15. Integrate X.509 Certificates and PKI into embedded hardware security modules connected to vehicles.
16. Deconstruct heavy vehicle event data recorder (HVEDR) data sets from raw binary to time history graphs.
17. Check and verify digitally signed data from a CAN Logger
18. Determine the contents of a CAN frame based on an oscilloscope trace of the signals on the CAN bus wires.
19. Judge the real-time performance of HMAC and CMAC approaches to verifying the integrity and authenticity of CAN messages.
20. Reflect on the challenges for implementing secure solutions to legacy vehicles already on the road.

21. Generate a solution to stream maximum bit rate CAN data over an IP network.

22. Assemble a system to detect and defend against intrusions on the CAN bus.

23. Design a printed circuit board to bridge multiple networks while securely storing cryptographic key material.

24. Create an original research poster advancing the cybersecurity posture of heavy vehicles.

Notice these objective make use of every verb in the graphic shown in Figure 1.1 on page 5. Additional objectives will be enumerated within each chapter of the manual as the specifics of the content and exercises are matured.

1.4 Exercises

While the learning objectives are fantastic for what we want to achieve, the specific activities to accomplish those goals need to be defined. Through the manual, we will present exercises that focus on helping students to achieve a learning objective. These exercises are created at different levels of the taxonomy, which enables a learner to start at a level appropriate to their skills. Successful completion of all the exercises should lead to the accomplishment of all learning objectives. The idea of successful completion means we have to have a measurement for success.

Exercise 1.1. [Evaluate] Reflect on on the program learning objectives in Section 1.3.2 and determine what is missing. Write a new learning objective using a verb that is not already in the list. Justify the reason for the new objective and submit it to your cohort for discussion.

For each exercise, the

1.5 Assessments

In school, formal assessments typically come in the form of quizzes, exams, and essays. These tools are part of a traditional pedagogy where students learn to achieve the grade and the rewards associated with the good grades. In this model, the teacher is primarily responsible for the assessment tools. However, the teacher feedback and assessment needs to transition to self or peer assessment when schooling ends and graduates enter the work force. Since the Student CyberTruck Experience mission is workforce centric, these self assessment skills are necessary to develop.

The exercises used throughout the program should have measurable outputs. Many times the outputs are binary (e.g. the approach worked or it didn't), but some outputs are qualitative or quantitative. For quantitative outputs, there are typically thresholds of performance to measure success. For example, if an exercise is to build a CAN to Ethernet translator device, the quantitative measure of success could be the message rate through puts of the device. The exercise should include the testing functions required to perform the assessments; and the outputs of the tests should be compared to a threshold or standard of performance. For qualitative results, the arguments and analysis need to be presented clearly to peers, mentors, and instructors to ensure the concept is effectively communicated. Feedback is the primary form of assessing qualitative outputs.

1.5.1 Formative Assessments

Formative assessments are frequent small tests of ideas and concepts with low-stakes. They are meant to have little to no pressure and provide quick feedback on the progress towards achieving mastery of the learning objectives. Some types of formative assessments include:

- Conversations to determine levels of knowledge, like trivia questions
- What-if scenarios
- Bouncing ideas off peers
- Confirming concepts with mentors
- Sketching diagrams and flow charts

Formative assessments are frequently used in writing code and are synonymous with debug statements. Simply put, a debug statement is a small test to ensure the code is working according to your idea and design.

Students should develop their own set of self-critiquing skills and frequently perform their own formative assessments. The more of these frequent assessments that take place, the more likely for success. Furthermore, the documentation and communication of these formative assessment results are important to "managing your boss," which is an important workplace behavior where a subordinate will frequently update the manager on progress and challenges. Articulating what you've done, how you tested it, and explaining the results are welcome communications for any good manager.

An example of the formative assessment for Exercise 1.1 is the discussion with your peers and instructor. There are no grades associated with the exercise and the questions and discussion around your proposed objective will give you feedback on if it is clear and measurable.

1.5.2 Summative Assessments

In school, summative assessments are less frequent, high stakes exercises like examinations and term papers. Since the focus of the Student CyberTruck Experience is project based, the summative assessment is the successful completion of the project. This begs the question of what success means. In an engineering design, a customer will voice a need or desire. One of the first jobs of the design engineer is to restate the problem into a set of measurable requirements. Since a good requirement is measurable, the project essentially assesses itself. The project is completed once all the requirements are demonstrated to be satisfied. This means it is possible to perform a summative assessment completely by yourself. However, an external review of the project is highly recommended.

For the CyTeX program, the realization of the summative assessment is the research poster presented at the NMFTA's fall HVCS meeting. These posters are viewed by all the attendees, which range from motor carriers, to government researchers, military scientists, and cybersecurity professionals. Students are expected to explain their poster contents and address questions from the attendees.

An example of the summative assessment for Exercise 1.1 is the acceptance of the proposed learning objective into the program. Perhaps it will be included in the next version of this manual!

1.6 Research

Every year we continue to research topics that can be relevant and helpful to improving the cybersecurity posture of the trucking industry. These projects are curated from the needs of the trucking companies, current technologies, topics of interest, and achievability. The list of projects is curated in the fall of each year and proposed to the sponsors. Once agreed upon, the projects are presented to the students. Student select the projects based on interest, but often they don't have enough background to know where to go. In those cases, the exercises herein can lay the foundation of knowledge and experience to take steps towards accomplishing the research.

Research can lead new discoveries and novel methods, but the likely output of the research for this program is a well thought out engineering design project. The engineering design process is as follows:

Ask Understand the needs of the customer, which means you have to know who the customer and their use cases. Restate and define the problem with a series of measurable engineering specifications, criteria, and constraints.

Imagine Brainstorm and explore different possible solutions to the problem.

Plan Select the most promising solution and draw/sketch out a solution. Determine the resources needed

Create Implement a prototype the solution. Acquire the parts and materials needed and build the solution

Test Evaluate the prototype to determine if it works and satisfies the design constraints

Iterate the process and improve the implementation and refine the requirements.

Share Communicate your design and solution to the appropriate audience.

There are many info-graphics on the Internet to visualize this process. The final poster presentation is the final step in sharing your results. The poster should capture the engineering design process and the things you've learned along the way, even if you learned that something doesn't work.

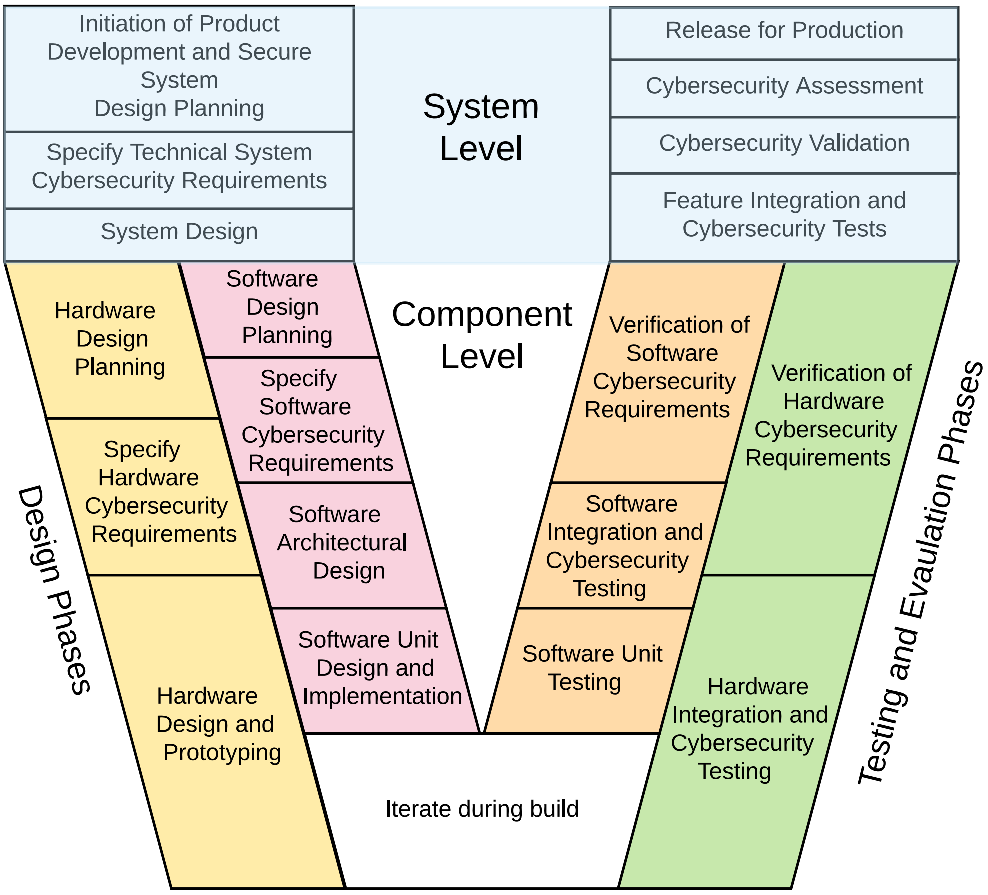

Initiation of Product Development and Secure System Design Planning
Specify Technical System Cybersecurity Requirements
System Design
System Level
Release for Production
Cybersecurity Assessment
Cybersecurity Validation
Feature Integration and Cybersecurity Tests
Hardware Design Planning
Software Design Planning
Component Level
Verification of Software Cybersecurity Requirements
Verification of Hardware Cybersecurity Requirements
Specify Software Cybersecurity Requirements
Specify Hardware Cybersecurity Requirements
Software Architectural Design
Software Integration and Cybersecurity Testing
Design Phases
Testing and Evaulation Phases
Software Unit Design and Implementation
Software Unit Testing
Hardware Design and Prototyping
Hardware Integration and Cybersecurity Testing
Iterate during build

Figure 1.3: Systems engineering process diagram for designing more secure cyber-physical systems.

1.7 Systems Engineering Approach

The engineering design process is often visualized in an iterative loop. Another visualization, popular among systems engineers, is the systems V ("vee") diagram. The V-diagram is used by in SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems to describe the process taken to design and develop more secure cyber-physical systems [?]. The graphic for this process is shown in Figure 1.3.

The V diagram is setup so the design phases are on the left and the testing phases are on the right. The top of the diagram contains the systems level approach, while the bottom V is separated into hardware and software designs. Many processes are iterative and follow the engineering design process within their own blocks. Often the hardware and software teams need to work closely together. For example, a systems level requirement may be to securely store cryptographic keys. Often this is done with a dedicated hardware security module (HSM). The hardware team needs to build the circuit to support the HSM and the software team needs to use the key material stored on the HSM. The software team may have to use evaluation hardware prototypes to implement the communication protocols and product algorithms.

During your work in the Student CyberTruck Experience, take some time to reflect where you are working in the diagram of Figure 1.3. This reflection should help you understand the different levels of effort and teamwork needed to bring secure solutions into fruition.

1.8 Anticipated Schedule

The training for which this maual is designed is focused on a 16 week course, which is typical of a college semester. Many students will come into the training with sufficient background in some topics, but others should be fruitful for exploration. However, the schedule and contents are intended to develop the necessary talent needed to succeed in heavy vehicle cybersecurity research.

Week 1 Receive and build hardware kits with CAN, LEDs, and the potentiometer. Setup software and the tool chain needed to perform the exersises.

Week 2 Perform some basic programming with Arduino by writing some short test scripts to demonstrate hardware functionality.

Week 3 Gather CAN data from an running SAE J1939 network on a heavy vehicle. Parse single frame data according to SAE J1939. Plot the Engine Speed data.

Week 4 Understand and parse SAE J1939 Transport Protocol Data.

Week 5 SAE J1939 Address Claims, launch cyberattacks on a vehicle.

Week 6 Gather diagnostic data with a vehicle diagnostic adapter using RP1210.

Week 7 Parse data from a Unified Diagnostic Session (UDS) using ISO-14229.

Week 8 Explore seed-key exchanges for diagnostic sessions.

Week 9 Legacy networks J1708 and J1587.

Week 10 Introduction to Ethernet and networking concepts.

Week 11 IP based networks, TCP, and UDP.

Week 12 Build a CAN to Ethernet Bridge

Week 13 Cryptography and Cybersecurity

Week 14 Symmetric Algorithms (AES) and Message Authentication Codes

Week 15 Asymmetric Algorithms, Certificates, Digital Signatures and Diffie-Hellman Key Exchanges

Week 16 Implementing Security with Hardware Security Modules