CYBER AUTONOMY RANGE

Building a one-of-a-kind facility to ensure autonomous systems are safe from cyber attack

February 2023

SMU Darwin Deason Institute for Cyber Security

CYBER AUTONOMY RANGE

Our Purpose

The Age of Autonomy is imminent. We must secure it.

Autonomous Systems are sensorladen systems that make decisions without human involvement, are situationally aware, and that are able to communicate. These systems include driverless vehicles and 5G/6G towers. They are enabled by sensors, machine learning and/or artificial intelligence, and 5G wireless networks.

However, using machine learning and artificial intelligence expands the attack surface of an autonomous system. The system is vulnerable to traditional attacks and new classes of cyber attacks. For example, a new class of cyber attacks is 'poisoning' machine learning training data with the effect of corrupting or weakening it.

The SMU Darwin Deason Institute for Cyber Security is building a Cyber Autonomy Range (CAR) to ensure that these autonomous systems will be better able to withstand such cyber-attacks. It will test the algorithms, datasets, sensors, and systems themselves through advanced cyber security research and the development of state-of-the-art techniques and tooling.

The CAR merges high-performance computing (HPC), graphics processing unit (GPU) processing, smart sensor networks, and positioning, navigation, and timing (PNT) with cyber range technology. The CAR will help define Autonomous Systems Vulnerabilities and Exposures (ASVE), as a subset of Common Vulnerabilities and Exposures (CVE).

The Cyber Autonomy Range will greatly enhance cyber security research, training, and testing capabilities.

Levels of Autonomy

As we develop more autonomous technology, we need to ensure that the system is secure. Secure systems limit the inconvenience and possibly loss of life from cyber attacks. Figure 1.1 shows the levels of autonomy as applied to a self-driving car.

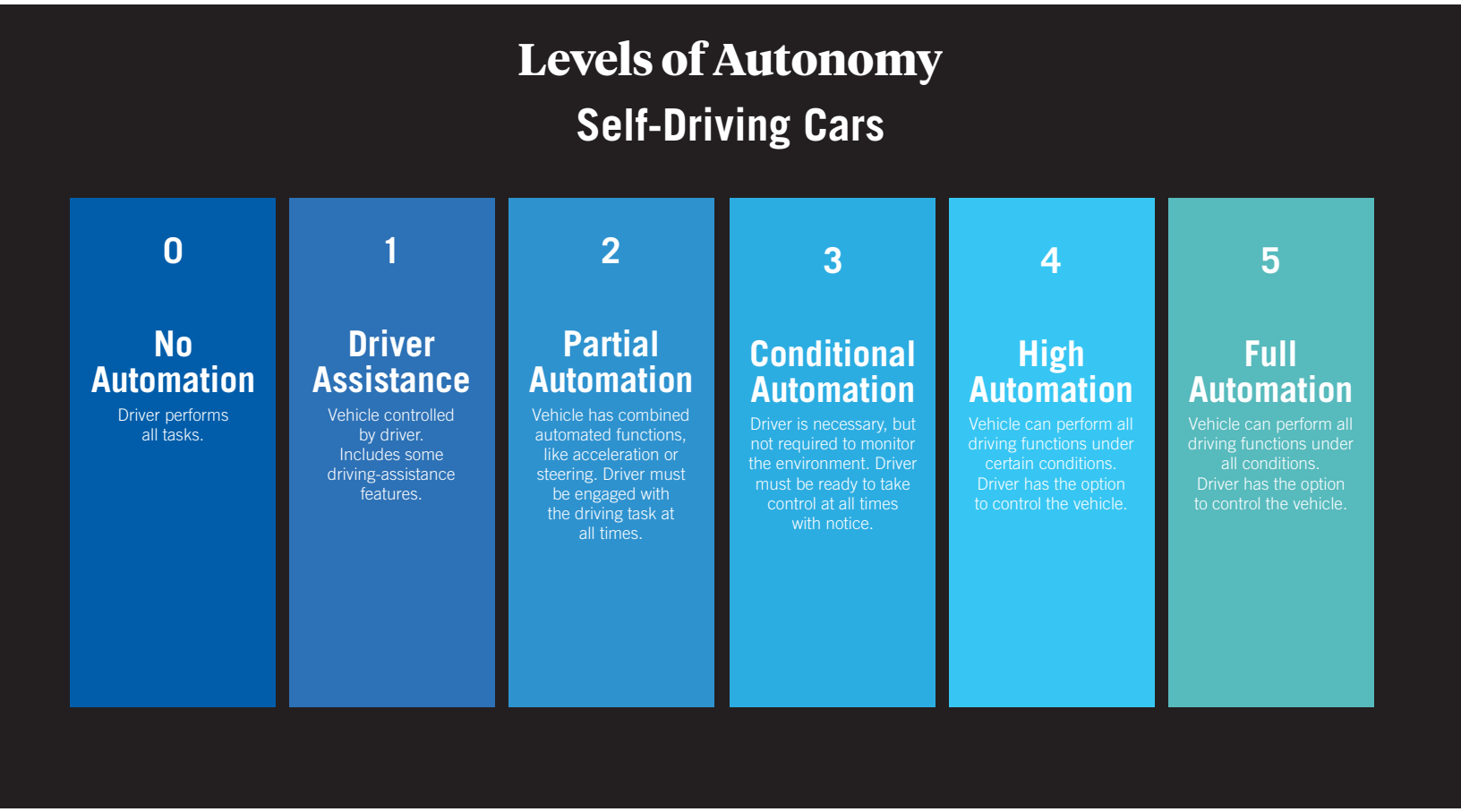

Figure 1.1. The Society of Automotive Engineers published this convenient 6-level system to determine the autonomy level of a car within the autonomous car industry. Autonomy levels increase as you move to the right.

Figure 1.2. Dallas, Texas skyline.

Why Dallas, Texas?

The State of Texas houses important intelligence leaders and is one of the leading tech hubs in the United States. The Autonomy Institute in Austin, TX is just a city away from Dallas. Texas is a testbed for national autonomous system infrastructure. It is ideal to have a facility like the CAR in state to ensure the security of that infrastructure. The CAR will also have access to United States and Texas state sponsors.

Why SMU?

SMU has various connections to telecom/5G/6G wireless network industry leaders, Department of Defense (DoD) contractors, and commercial autonomous system industry leaders, such as Toyota. These connections provide many potential users for the CAR and will broaden the range's impact.

New Cyber Attacks – and a New Defense

With development of autonomy, artificial intelligence, and machine learning, cyber security experts warned of greater cyber risk. Autonomy Stacks are the key enabling technology for Autonomous Mobile Robots (AMR) and present a new very large attack surface for adversaries.

As more companies use machine learning models in their production systems, their machine learning models are exposed to more users and more bad actors. Even those that are not exposed over networks are at risk. Once attackers gain access through traditional cyber attacks, attackers can employ their new attacks as well.

Attackers can leverage inference attacks, an attempt to 'reverse' the model with data mining techniques allowing them to exploit revealed weaknesses or replicate and steal the model. Or, attackers can perform "data poisoning," which is corrupting or weakening the training data used to train the model in order to mislead the autonomous system into making decisions in the attacker's favor.

These attacks and more are critical for companies and agencies to consider when employing artificial intelligence and machine learning. The CAR provides a minimal-risk opportunity to test autonomous systems against attacks like these.

The CAR is a safe and secure facility in which to identify vulnerabilities and consult cyber security experts to improve the autonomous system's resilience against new classes of cyber attacks.

What is a Cyber Autonomy Range?

A Cyber Range is a controlled and isolated technology environment that simulates possible attacks on Systems Under Test (SUT). These SUTs can be IT infrastructure, networks, or software applications. A CAR, however, simulates possible attacks on Autonomous SUTs. Autonomous SUTs can be AI-assisted technology or any technology that enhances automated systems so that the system can make independent decisions based on given data.

The CAR is an ideal host for cyber security-related research, training, and testing. Malicious software released inside the range for testing purposes, such as viruses, trojans, and worms, are contained within segregated resources. The range itself is reconfigurable, allowing environment changes for each event. Events can also be 'rerun' from a known good state, making the range repeatable. Finally, the range is scrubbable. All equipment can be securely wiped of all data to remove malicious elements and keep customer data secure.

The mission of a cyber autonomy range is to create a synthetic environment to safely identify cyber vulnerabilities in a complete autonomous system in a realistic operational scenario.

The Cyber Autonomy Range is

- Controlled
- Reconfigurable
- Repeatable
- Scrubbable

Cyber Autonomy Range at SMU

A CAR creates a synthetic environment in which we can safely identify cyber vulnerabilities in autonomous system(s) in a realistic operational scenario.

To identify cyber vulnerabilities, the CAR will research and test the cyber security of

- Artificial Intelligence/Machine Learning (AI/ML) Algorithms
- Artificial Intelligence/Machine Learning (AI/ML) Datasets
- System Sensors
- System Software and Hardware
- Full-Stack Autonomous Systems

The CAR will be built on top of the SMU Darwin Deason Institute's (DDI) foundation of basic and applied research into cyber security of autonomous systems and multi-domain system of systems. The range will be capable of large-scale system testing and verification through the development of advanced cyber security research in autonomous systems to support both industry and government partners and entities. It will be supported by various technologies such as simulation, radio frequency (RF) systems, control and network, as well as include real-world laboratories in which systems are put into real-world testing.

CAR Conceptual View

Autonomy can be present in the application, the middleware, the system, and/or the hardware of an autonomous system. In order to test all 4 levels of the high-level autonomy stack shown in Figure 1.3, the CAR will leverage a Mission Simulator, a World Simulator, a Cyber Generator, and Orchestration to assess the cyber security of an autonomous system.

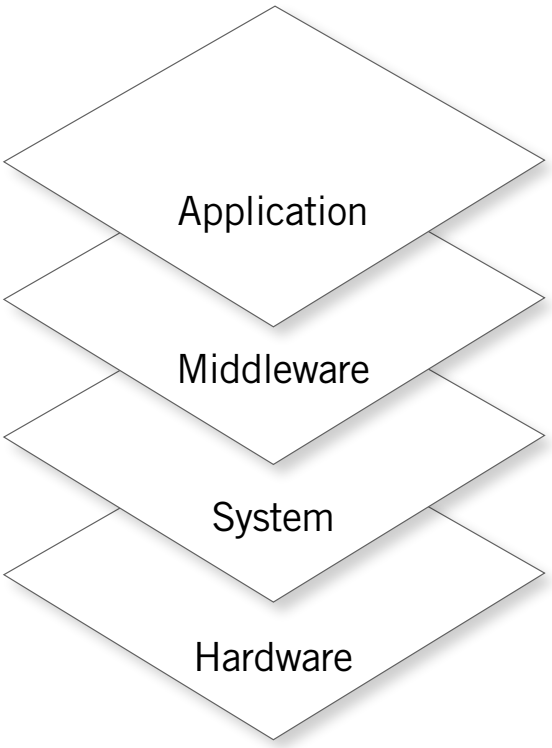

Figure 1.3. A high-level overview of an autonomy stack of an autono- mous system. Autonomy can be involved with any number of these levels.

The Mission Simulator generates missions for the system to complete, and if needed, generates defensive and offensive forces. The World Simulator then provides realistic geographic and signaling input for the autonomous system to use as real data. At this point, the autonomous system is acting as though it were operating in the real world with real-world data and inputs.

The Cyber Generator systematically generates cyber attacks that target the system and its four layers of subsystems. As the autonomous system reacts to these attacks, the CAR uses Orchestration to analyze the results and plan the next event.

The CAR's process for testing autonomous systems is summarized in Figure 1.4.

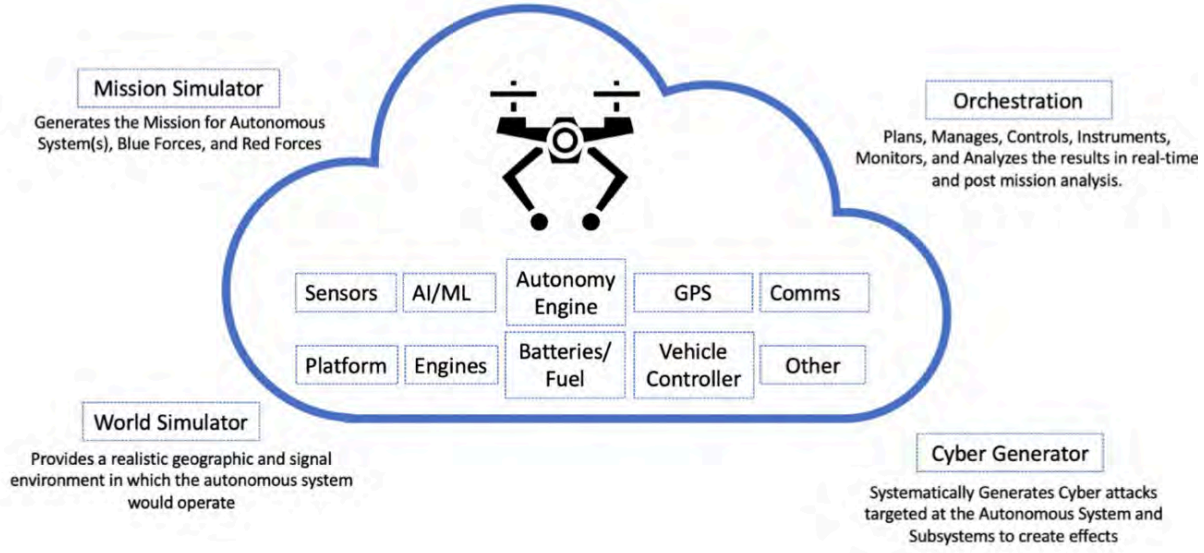

Figure 1.4. CAR uses a Mission Simulator, a World Simulator, a Cyber Generator, and Orchestration to assess the cyber security of an autonomous system.

The CAR will use SMU's NVIDIA SuperPOD and HPC cluster to provide significant additional computing resources to support the cyber security testing. The NVIDIA SuperPOD sets the stage for AI/ML speeds of up to 25 times faster than current levels.

The NVIDIA SuperPOD uses GPUs, a circuit specializing in processing large amounts of data in parallel. The shared resource machine uses 20 NVIDIA DGX A100 nodes, each using 8 GPUs to accelerate computations and train AI models. These GPUs make the SuperPOD ideal for machine learning, which uses statistics to find patterns in large data sets. The CAR's use of the SuperPOD allows for faster analysis without sacrificing test quality.

CYBER AUTONOMY RANGE

Building CAR

The Cyber Autonomy Range Facility

The CAR Facility will support the development and training of cyber security engineers and fundamental research.

The facility will support

- Briefings
- Classroom Training
- Secure Testing
- Lab Space
- Data Center

Figure 2.1. Artist rendition of the User Center shows multiple workstations and a presentation screen.

CAR User Center

The CAR User Center is a Phase 1 space that is under renovation on SMU's East Campus. It is located in room 111 of the Johnson Square Building.

The User Center is a multi-purpose room featuring a large presentation screen, high-end workstations for 6-8 people, and space, rack and workbench for System Under Test (SUT).

In Phases 2, 3, and 4, more multi-purpose User Centers will be added.

SMU Data Center

The SMU Data Center includes four full-height racks, access to an HPC cluster, and access to SMU's NVIDIA SuperPOD. It is a 'lights out' facility, meaning it is a fully automated, remotely managed facility that can operate without staff. The lights can be turned off, saving energy and administrative costs.

During Phase 1, the CAR will use two racks in the existing SMU Data Center, allowing for two segregated tests. During Phases 3 and 4, CAR will expand its use of the data center to 8 or more additional racks.

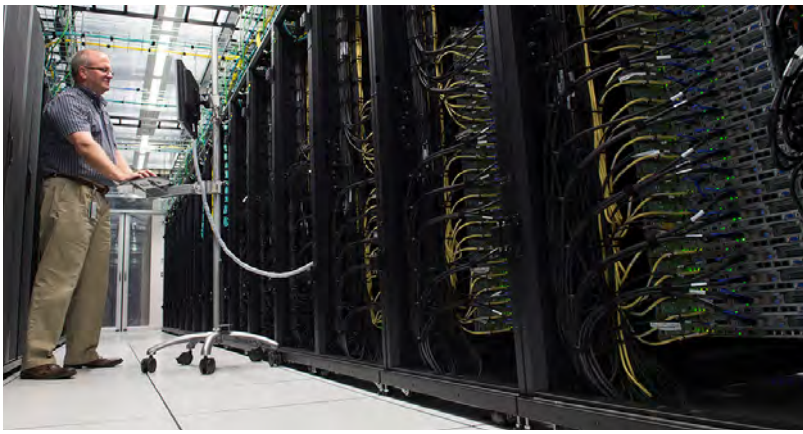

Figure 2.2. SMU Data Center.

Figure 2.3. SMU's NVIDIA SuperPOD.

CAR Auditorium

The CAR Auditorium is a Phase 3 addition. It is the ideal space in the CAR facility for presentations and briefings.

The Auditorium features tiered seating to ensure that every attendee has an unimpaired view of the presentation. Opposite the seating is a large screen for visual aids, as well as a modern podium for speakers.

Figure 2.4. Artist rendition of the auditorium features tiered seating and a large screen.

CAR Conceptual Architecture

The CAR User Center and its dedicated racks are segregated, meaning there are no external network connections allowed. The CAR dedicated racks include the Data Center's high speed switch and the computer servers.

Prohibiting external network connections allows the CAR to keep malicious tools used for cyber security testing from spreading on the internet, and keeps external malicious software from entering CAR cyber space. This segregation allows the CAR to remain a clean, controlled, and isolated cyber environment.

The SMU Data Center and the CAR User Center are connected via a CAR dedicated fiber cable. Since the Data Center's HPC, long-term storage, and NVIDIA SuperPOD are not segregated, there is a firewall between them and the CAR dedicated fiber cable to maintain security.

There is an additional firewall between the CAR dedicated racks and the internet and dedicated SMU campus-wide fiber cable. Figure 2.5 shows the conceptual architecture of the Cyber Autonomy Range.

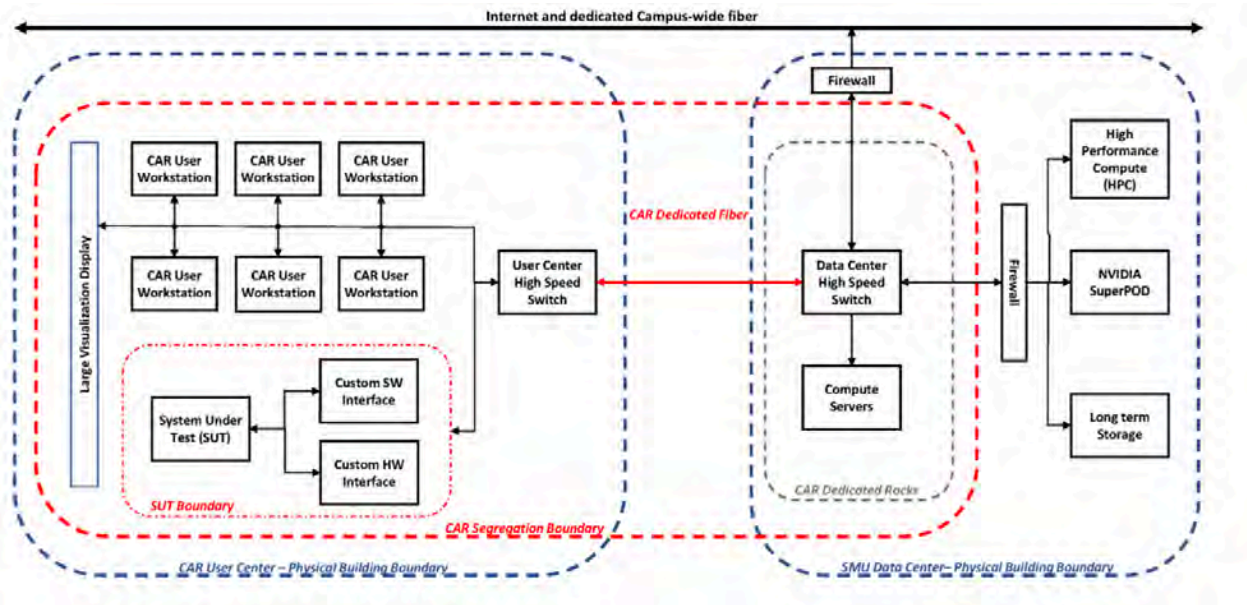

Figure 2.5. User Center and Data Center conceptual architecture shows the relationship and boundaries between the two entities.

Notional CAR Facility

Figure 2.6 shows the entire new CAR facility in Phase 3. The CAR is a 3,000 - 6,000 square-foot facility with an auditorium, a dedicated hardware-in-the-loop (HWIL) lab, a test bay for large systems (vehicles), a lobby, and restroom facilities. In Phase 3, the CAR will expand its use of SMU's Data Center by 4-8 additional racks and will have network infrastructure to support 1000 Gb networks.

Figure 2.6. CAR Facility in Phase 3.

Figure 2.7. CAR Facility in Phase 4.

As shown in Figure 2.7, Phase 4 CAR will add additional spaces and expand the racks used by the CAR. There are user centers, an auditorium, restrooms, a large vehicle test bay, and a larger dedicated hardware-in-the-loop (HWIL) lab. The expanded HWIL lab will have additional racks and additional workspaces.

Mark Bradbury

Cyber Security Research, Darwin Deason Institute for Cyber Security

(972) 742-7116

mbradbury@smu.edu

Eric Larson, Ph.D.

Associate Professor in Computer Science

(214) 768-7846

eclarson@lyle.smu.edu

Mitchell A. Thornton, Ph.D, P.E.

Executive Director, Darwin Deason Institute for Cyber Security

Cecil H. Green Chair of Engineering and Professor

(214) 768-1371

mitch@lyle.smu.edu

http://lyle.smu.edu/~mitch/

Darwin Deason Institute for Cyber Security

Mailing Address:
P.O. Box 750122
Dallas, TX 75275-0122

Delivery Address:
6251 Airline Rd Junkins 308
Dallas, TX 75205-2333

Phone: 214-768-3189
Email:
deasoninstitute@smu.edu

www.smu.edu/Lyle/Centers- and-Institutes/DDI

SMU Darwin Deason Institute for Cyber Security