Proceedings of the 21st International Symposium on the Packaging and Transportation of Radioactive Materials

PATRAM 25
JULY 27 – AUGUST 1, 2025
SAN ANTONIO, TX / SAN ANTONIO MARRIOTT RIVERCENTER

FUSING EDGE COMPUTING WITH TRANSPORT SECURITY BY LEVERAGING THE CONTROLLER AREA NETWORK TRANSPORT SECURITY TRACKING AND REPORTING (C-STAR) UNIT

Adian Cook
Oak Ridge National Laboratory

Jerry Kirk
Oak Ridge National Laboratory

Joel Asiamah
Oak Ridge National Laboratory

Doug Mann
Oak Ridge National Laboratory

Ken Martin
Oak Ridge National Laboratory

Shannon Morgan
Oak Ridge National Laboratory

ABSTRACT

Rapid advances in embedded system complexity and capability provide exciting opportunities for transportation security deployment. Manufacturers and developers of these embedded systems continue to provide lower costs and more powerful solutions that can be leveraged by researchers and engineers. Furthermore, deploying these devices at the "edge" of the Internet-of-Things (IoT) infrastructure provides opportunities for highly capable applications in transport security. In an edge computation architecture, the device is colocated at the source of the data in the larger IoT structure, which provides computational capability at the location directly where the data are collected. For shipment transport security, this setup provides a direct compute node for digestion of data and mitigation actions in real time. In our application, the vehicle provides a significant amount of these data that can be processed in real time via the Controller Area Network Transport Security Tracking and Reporting (C-STAR) edge device. Use of a computational node, such as the C-STAR, on the vehicle capitalizes on opportunities of edge architectures. This paper discusses this security solution's usability, current deployments, and scalability to further applications in transport security. First, we cover the supported vehicle platforms that can leverage the C-STAR technology. This will be particularly relevant to medium- and heavy-duty vehicles transporting high-risk shipments. Second, we address current deployments of C-STAR. Finally, we discuss additional areas for expansion, such as maturing the onboard algorithms through continuing collaborations.

INTRODUCTION AND MOTIVATION

Safe transportation and security of nuclear materials such as ore, uranium, spent fuel, and waste [1] are complex and highly dynamic tasks with significant transport volume. According to the International Atomic Energy Agency (IAEA), more than 20 million shipments of nuclear and radioactive material are transported globally via all transportation channels [2]. Furthermore, these shipments are at high risk of interception during transport—the IAEA Incident and Trafficking Database reported 630 thefts of nuclear transport occurring between 1993 and 2021, with 310 happening during transport of the materials. Because of the high-risk nature of transporting these materials, advanced safeguards must be deployed to combat adversaries attempting to intercept the materials while in transit.

Because of this constant and dynamic threat, widespread adoption and application of onboard telematics and tracking continue to expand, with several companies providing different solutions [3], [4], [5]. One such onboard solution, the Controller Area Network Transport Security Tracking and Reporting (C-STAR) unit,

enables fleets to leverage a plug-and-play embedded architecture for medium- and heavy-duty applications. Developed, designed, and tested by researchers and engineers at the US Department of Energy's Oak Ridge National Laboratory (ORNL), C-STAR is a powerful edge device that uses data directly from the vehicle communication network to provide an additional layer of physical security and protection. The device focuses on detection of ramming, tipping, and towing, which was the primary concern and consideration of current fleet partners. Discussed in further detail in the following sections, C-STAR uses a synergy of onboard vehicle data, embedded sensors onboard the device, computation collocated at the data source, and cloud infrastructure to strengthen vehicle shipment security.

BACKGROUND

C-STAR employs a combination of complex workflows and rich data sources to enable its core algorithms. First, we discuss the concept of edge computing, which is a common hierarchy in modern computing systems and critical to the functionality of the device. By definition, the C-STAR is an edge device located on the vehicle – it enables edge workflows and capabilities to non-edge devices and will be discussed within the following section. We then discuss the primary data source enabling the functionality of C-STAR, the controller area network (CAN) bus, a communication medium used on most on-road vehicles. C-STAR has a direct connection the vehicle CAN bus, which allows access to a plethora of onboard vehicle data.

Edge Computing

Edge computing architectures have been deployed in a myriad of applications since the 1990s, varying from simple applications of home security cameras to large cloud computing networks [6]. The fundamental concept of edge computing hierarchies is moving the data processing closer to the data source to provide low latency and fast response to data stimulus [7]. C-STAR collocates its onboard processing power on the vehicle (acting at the edge at the larger network) to provide rapid decision making using real-time data. These data are digested directly by the algorithms running on the device, such as towing detection or other configurable alerts, and relevant events are sent to an Amazon Web Services (AWS) cloud dashboard. Using this interface, a headquarters or a fleet manager can automate a response or directly contact relevant authorities. Figure 1 shows a diagram of the overall architecture of the C-STAR workflow and how it relates to edge computing.

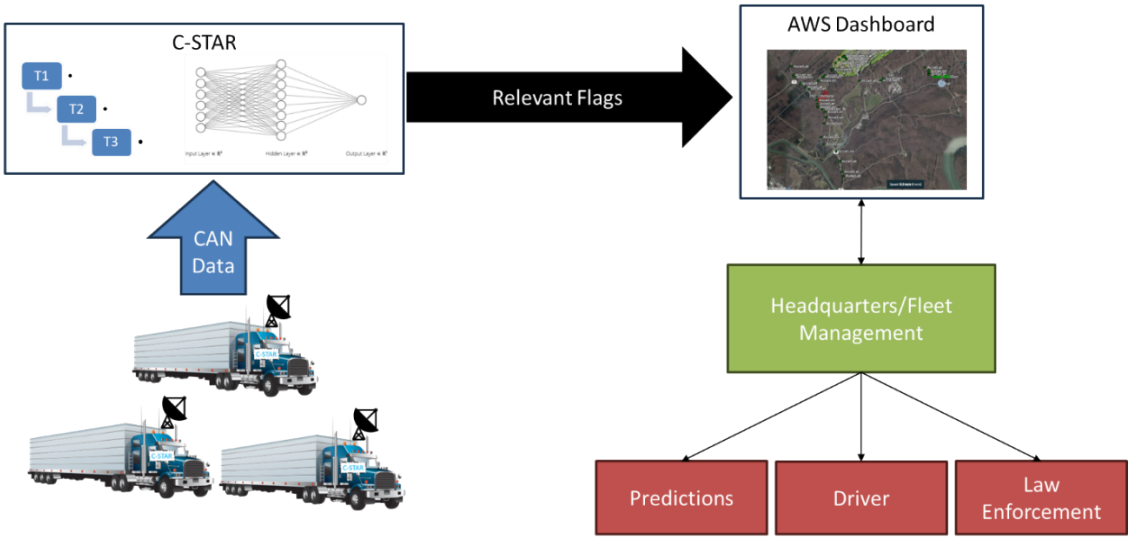

Figure 1. C-STAR edge architecture

CAN

Introduced in the late 1980s and widely adopted in the 1990s ISO 11898 [8], CAN provides a robust communication medium for on-road and off-road vehicles. These vehicles contain several OEM electronic control units (ECUs), such as the engine control module, transmission control module, body control module, and other modules also communicating on the vehicle CAN bus. For example, the engine control module and transmission control module could communicate to deliver proper torque delivery to the wheels while the body control module communicates vehicle status with other onboard ECUs. Physically, this is completed via a two-wire bus located on the vehicle, as shown in Figure 2; a message structure is shown in Figure 3.

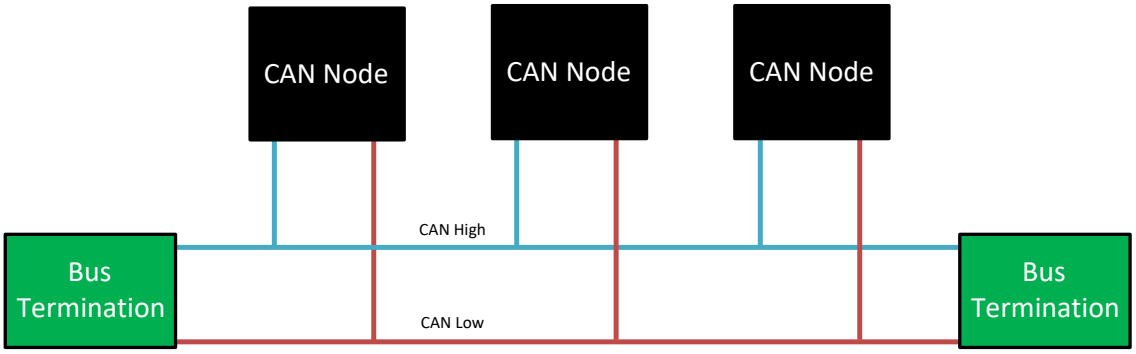

Figure 2. CAN bus structure

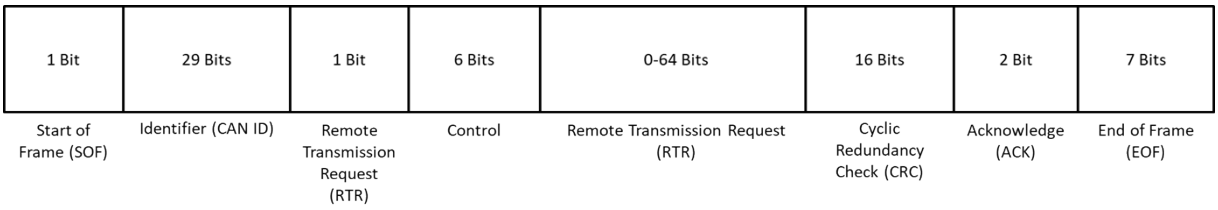

Figure 3. CAN message format

Within this CAN standard, other application-specific standards exist—one such standard, SAE J1939 [9], [10], provides an additional layer of standardization for medium- and heavy-duty vehicles [11]. J1939 provides extensive guidance for multiple CAN layers, but this paper focuses on the arbitration/CAN identifier (AID) and data field shown in Figure 3. On a typical CAN bus, these are unknown values containing only binary data that are unreadable to the user. However, J1939 provides a standardized AID and data field that can be interpreted on a wide range of medium- and heavy-duty vehicle platforms. Figure 4 shows an example AID in hexadecimal format for J1939.

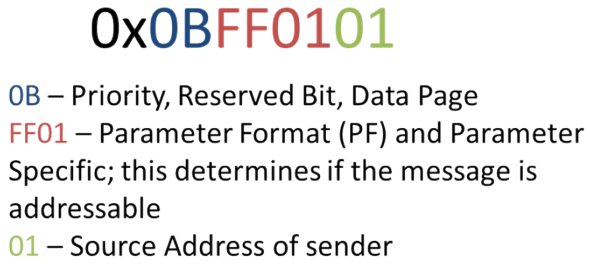

Figure 4. J1939 AID example

C-STAR FUNCTIONALITY

As constructed, C-STAR connects directly to the vehicle J1939 CAN bus via the onboard diagnostic port (OBD) on medium- and heavy-duty vehicles. This setup provides direct access to CAN traffic from several ECUs mentioned earlier. The C-STAR software runs on a real-time Linux processing unit that provides a platform for deploying the core functions focused on ramming, tipping, and towing detection. Although all core functions can be accomplished using onboard vehicle CAN data, a global navigation satellite system comprising a GPS and inertial measurement unit is included for additional redundancy, geofencing, and data supplementation. Figure 5 shows a simple layout of the device.

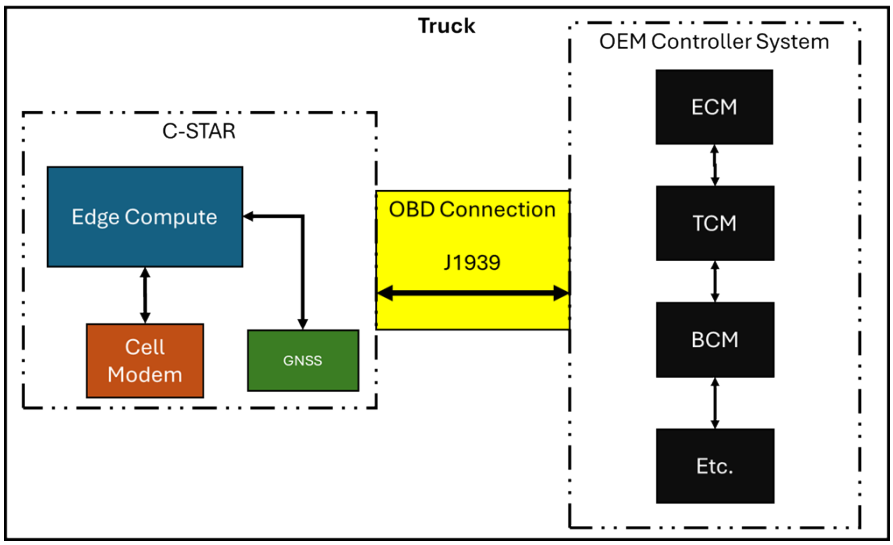

Figure 5. C-STAR layout

The three core functions of C-STAR primarily focus on physical security of the shipment and are based on detecting ramming, tipping, and towing:

- **Ramming** – abnormal lateral or longitudinal movement of the truck (Figure 6, left)
- **Tipping** – abnormal roll of the truck (Figure 6, center)
- **Towing** – truck is being towed away (stolen) from an area, such as a truck stop theft (Figure 6, right)

Figure 6. C-STAR primary functions of ramming, tipping, and towing detection

To accomplish these functionalities, C-STAR leverages the concepts discussed in the Introduction:

- **Edge computing** – colocation of data processing at the data source with real-time cloud monitoring provides rapid response to data changes and localized computation/sensing
- **CAN communication** – direct connection to the vehicle for a plethora of onboard data via the CAN bus that provides data from several onboard ECUs
- **J1939 standardization** – current deployment on Class 8 trucks provides significant flexibility and modularity for most heavy-duty trucks using J1939

C-STAR DEPLOYMENT

C-STAR (Figure 7) is currently being deployed on ORNL trucks and with an ORNL fleet partner for further validation and testing on an active vehicle. Typically, the box is placed in the cab of the truck rigidly mounted behind the driver. As mentioned, CAN communication is provided using a cable directly connected to the OBD port under the dash. C-STAR has been used on several trips using ORNL vehicles and partner trucks. However, for privacy, only two ORNL-specific trips are discussed here.

Figure 7. C-STAR

ORNL to Chattanooga, Tennessee

On this 4.5 h trip from the ORNL Global Research Evaluation, Analysis, Research, and Security Facility, interstate and smaller surface roads were traveled. The weather was warm, sunny, and with light cloud cover. The truck under test was a 2019 LT International pulling a CONEX trailer with C-STAR strapped to the console directly behind the driver. The MAVNet trace from this drive is shown in Figure 8, which shows the entire trip from ORNL. Figure 9 shows the associated speed trace for this drive that illustrates the tracked vehicle speed in meters per second over the trip. The plots are high-level tools used to track the movement of the vehicle/shipment.

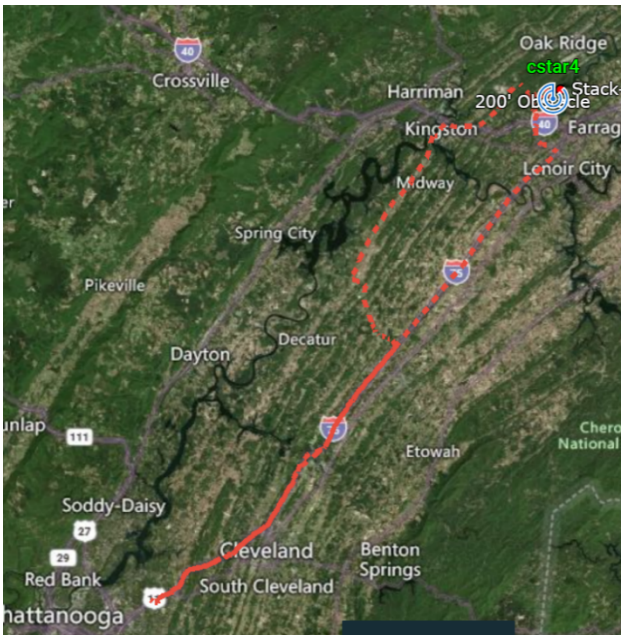

Figure 8. MAVNet trace

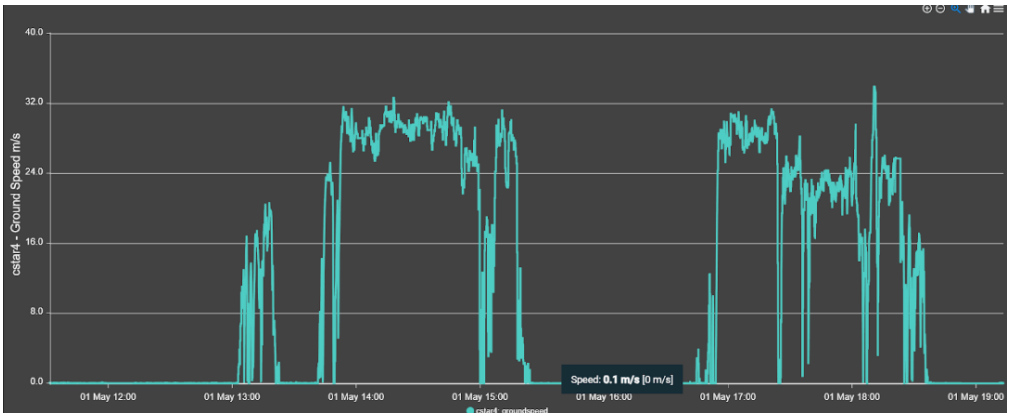

Figure 9. Speed trace

Figure 10 shows the trip alerts, with several alerts being shown in the MAVNet interface and triggered by the C-STAR algorithm. These alerts occurred because of the low threshold values calibrated on the device in the initial phases of deployment. Furthermore, Figure 11 shows the specificity of the GPS tracking while navigating a truck stop.

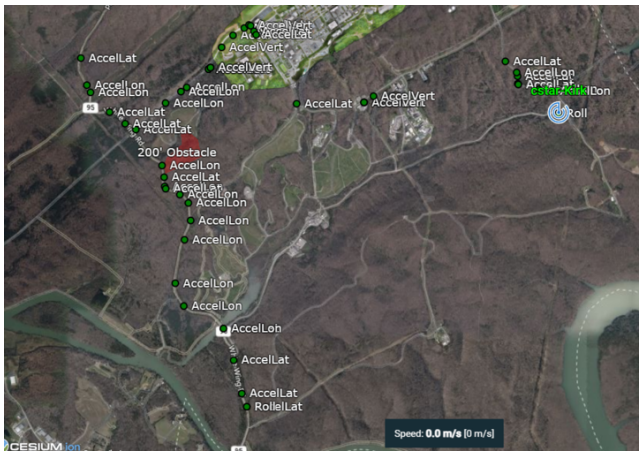

Figure 10. Sample alerts

Figure 11. GPS tracking

ORNL to Tennessee Tech University

On this 2.5 h trip, interstate and smaller surface roads were traveled. The weather was mild with mixed rain and clouds. The truck under test was a 2014 Peterbilt 389 without a trailer with C-STAR strapped to the console directly behind the driver. The MAVNet trace from this drive is shown in Figure 12 and associated speed trace in Figure 13.

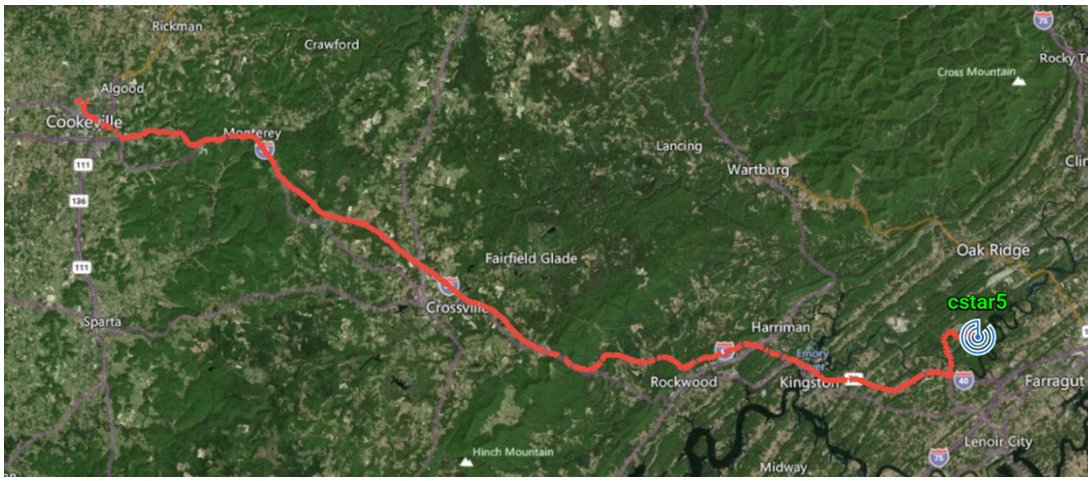

Figure 12. Mavnet trace

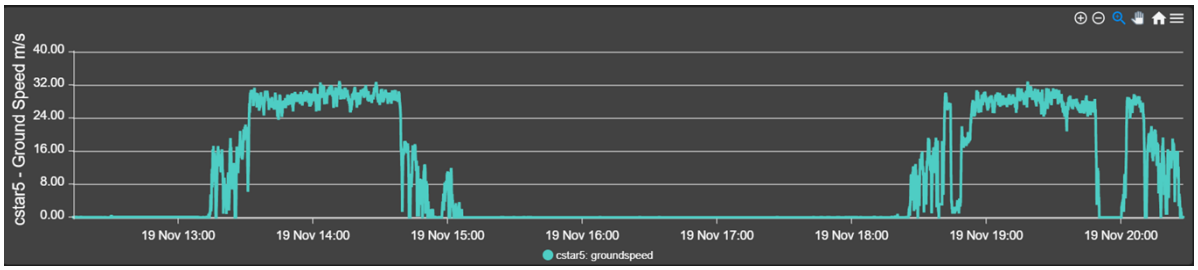

Figure 13. Speed trace

In addition to investigating C-STAR alerts, the team also analyzed the incoming (Figure 14) and outgoing data (Figure 15) from the device, along with server use. The spikes between November 18th and 19th are the results of testing C-STAR. In addition, the AWS server use of C-STAR (Figure 16) is within the operational boundaries of the server. This use confirms that the data being pulled from the device can be monitored in real time by a headquarters or fleet manager without losing critical driving data.

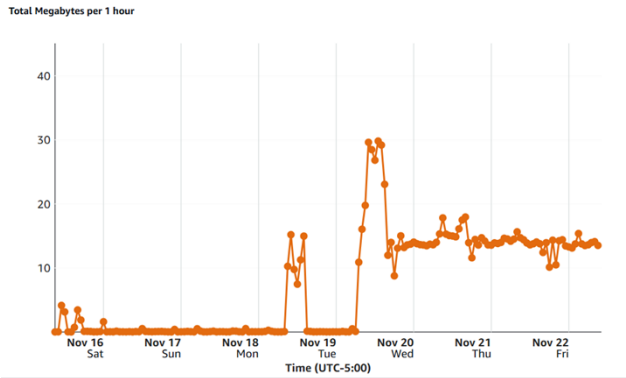

Figure 14. Server incoming traffic

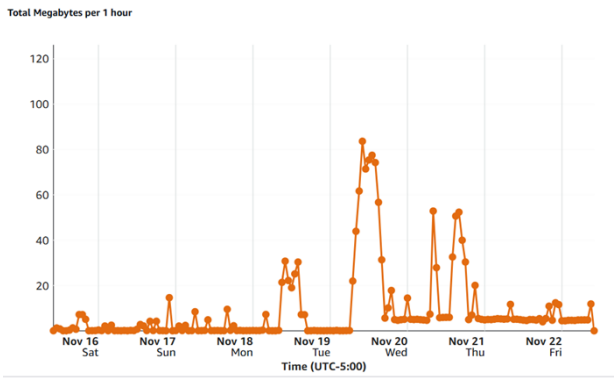

Figure 15. Server outgoing traffic

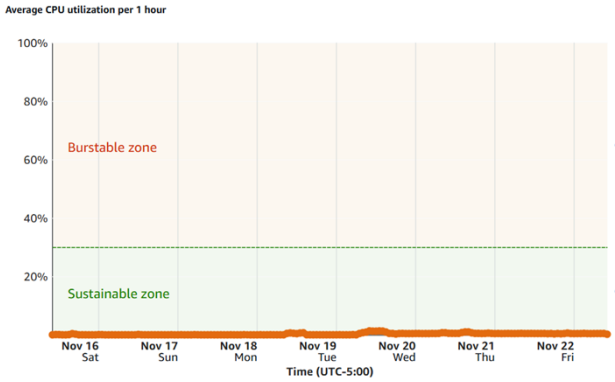

Figure 16. Server CPU utilization

CONCLUSIONS AND FUTURE WORK

This paper presents an ORNL-developed device for tracking high-risk shipments, monitoring their onboard systems, and reporting key information. We also illustrated that a combination of edge computing techniques, vehicle onboard sensors, and the vehicle CAN bus provide a rich data source for deploying onboard algorithms for securing the physical shipment. Furthermore, we described two sample deployments of the device and showcased the data coming from the vehicle. In these deployments, we demonstrated the detection capabilities of C-STAR, as well as the current hardware and software performance on the truck.

In subsequent iterations of C-STAR, we will integrate additional AI workflows for more advanced detection and tracking. As threats evolve, telematics and other tracking technologies will require increasingly sophisticated algorithms to safeguard shipments and cargo from adversarial attacks. In addition, other AI-powered tasks such as predictive maintenance, trip analysis, and other vehicle characterization can be applied onboard C-STAR to further enhance the device's capabilities.

The impact of this research effort is two-fold – first, the C-STAR enables explicit edge capabilities to non-connected and non-autonomous vehicles. Concretely, this gives connectivity and computation for detection and mitigation to otherwise isolated vehicles. Second, the C-STAR taps into an already data dense environment for advanced algorithms. The onboard vehicle data is extensive, covers most components located on the vehicle, and continues to expand in breadth and depth. Detailed use cases using onboard vehicle data, external datasets, and AI workflows using this platform are covered extensively in an adjacent paper submitted to this conference.

ACKNOWLEDGMENTS

This material is based upon work supported by the US Department of Energy, National Nuclear Security Administration, Office of Radiological Security under the project management of Shea Cotton.

REFERENCES

[1] "Transport of Radioactive Material - World Nuclear Association." Accessed: May 28, 2025. [Online]. Available: https://world-nuclear.org/information-library/nuclear-fuel-cycle/transport-of-nuclear-materials/transport-of-radioactive-materials

[2] "The Role of Safety and Security in Transport of Radioactive Material Discussed at Vienna Conference." Accessed: May 28, 2025. [Online]. Available: https://www.iaea.org/newscenter/news/the-role-of-safety-and-security-in-transport-of-radioactive-material-discussed-at-vienna-conference

[3] "Telematics: How It Improves Fleet Management & Maintenance." Accessed: Jun. 06, 2025. [Online]. Available: https://www.fleetio.com/blog/fleet-telematics

[4] O. Ghaffarpasand, M. Burke, L. K. Osei, H. Ursell, S. Chapman, and F. D. Pope, "Vehicle Telematics for Safer, Cleaner and More Sustainable Urban Transport: A Review," *Sustainability*, vol. 14, no. 24, p. 16386, Dec. 2022, doi: 10.3390/su142416386.

[5] J. Boylan, D. Meyer, and W. S. Chen, "A systematic review of the use of in-vehicle telematics in monitoring driving behaviours," *Accid. Anal. Prev.*, vol. 199, p. 107519, May 2024, doi: 10.1016/j.aap.2024.107519.

[6] N. Kuever, "Cloud and edge computing for IoT: a short history," Bosch Digital Blog. Accessed: May 28, 2025. [Online]. Available: https://blog.bosch-digital.com/cloud-and-edge-computing-for-iot-a-short-history/

[7] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An Overview on Edge Computing Research," *IEEE Access*, vol. 8, pp. 85714–85728, 2020, doi: 10.1109/ACCESS.2020.2991734.

[8] "History of CAN technology." Accessed: May 28, 2025. [Online]. Available: https://www.can-cia.org/can-knowledge/history-of-can-technology

[9] "J1939_202306: Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document - SAE International." Accessed: May 28, 2025. [Online]. Available: https://www.sae.org/standards/content/j1939_202306/

[10] "J1939 Standards Overview," Kvaser. Accessed: Jun. 06, 2025. [Online]. Available: https://kvaser.com/about-can/higher-layer-protocols/j1939-standards-overview/

[11] "Alternative Fuels Data Center: Maps and Data - Vehicle Weight Classes & Categories." Accessed: May 28, 2025. [Online]. Available: https://afdc.energy.gov/data/10380