Proceedings of the 19th International Symposium on the Packaging and Transportation of Radioactive Materials
PATRAM 2019
August 4-9, 2019, New Orleans, LA, USA

Advancing the Transportation-Security, Tracking, and Reporting System (T-STAR)[1]

James Younkin,
Michael Schultze, Shane Frank,
Brad Stinson, Bogdan Vacaliuc,
Lloyd Clonts, Ronald Salesky
Oak Ridge National Laboratory
Oak Ridge, TN, USA

James Shuler
Packaging Certification Program
US Department of Energy, USA

Thad Thompson,
Caleb Askew
CADRE5
Knoxville, TN, USA

Katherine Holt
Office of Radiological Security
U.S. Department of Energy, USA

ABSTRACT

The Transportation-Security, Tracking, and Reporting System (T-STAR) was developed by the National Nuclear Security Administration, NA-21, Office of Radiological Security (ORS) to provide a transportation security system for detection and tracking during transport of Category 1 and Category 2 radiological material. While many off-the-shelf systems provide asset tracking of the conveyance, few offer detection of a breach into the cargo compartment or the removal of cargo from the conveyance. Systems that do offer this capability often require permanent installation on the conveyance by drilling holes and running cables through the conveyance itself. This is not sustainable in many countries where ORS is building capacity for the security of radioactive materials in use, storage, and transport. ORS has built two generations of T-STAR. Lessons learned from the development and deployment of those systems are being used in the development of a third, Gen 3, system. Gen 3 of T-STAR leverages Oak Ridge National Laboratory technologies to improve the communications capability and reduce power consumption using a multimode communications module developed by the Unmanned Vehicle Development Laboratory and the low power and extensible Authenticatable Container Tracking System tag developed for the US Department of Energy's Packaging Certification Program. T-STAR uses both cellular and Iridium satellite modems to communicate the configuration, status, and alerts to a server monitoring the shipment. A wireless security system employing intrusion detection sensors located in the conveyance together with environmental sensors, a hardware security module for digitally signing communications messages, and a single peripheral expansion slot gives strong situational awareness throughout the duration of transport. This paper details the overarching T-STAR capabilities, architecture, and components and provides insights on deployment.

INTRODUCTION

The Transport-Security, Tracking, and Reporting (T-STAR) system is used to provide secure transport of Category 1 and Category 2 radiological material for domestic and international shipments. The US Department of Energy (DOE) Off-Site Recovery Program currently uses T-STAR and a suite of its security sensors within one domestic and one international conveyance, and such use is expanding.

T-STAR development began in 2014 under the sponsorship and guidance of the National Nuclear Security Administration, NA-21, Office of Radiological Security (ORS). The concept of T-STAR is that it conveys location, operational, and security sensor status at regular intervals together with immediate alerts so both can be used to assess the security of the shipment (Figure 1**Error! Reference source not found.**). Conditions monitored include equipment operation details, if it is communicating, security sensor alarms, and location of the shipment on a geographic map.

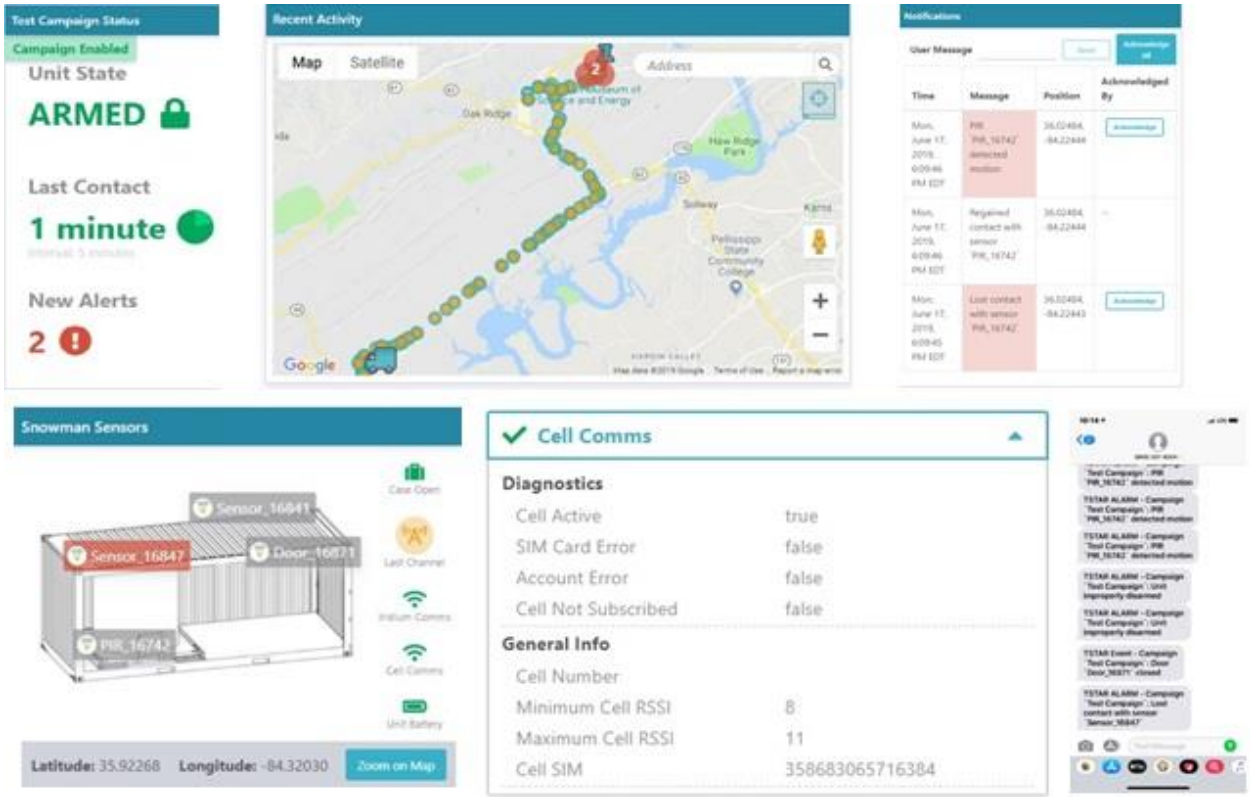

Figure 1. The T-STAR web application running on computers and smartphones provides views that allow assessment of the shipment's status. Via the web application, a user may opt to receive SMS messages of the system notifications.

To be able to assess the security of the shipment remotely using a web application, equipment that delivers pertinent information must be used. T-STAR consists of the electronics that “ride” with the shipment, the cellular communications equipment that can use the available communications and network backhaul infrastructure along the route, the satellite communications used when cellular is not available, and the backend database and monitoring web application (Figure 2). These provide pertinent information necessary for continuous security assessment. The security system employs a wireless sensor network (WSN) of security ssnsors monitoring motion within the conveyance or conveyance door openings and closings. These sensors are battery operated and placed

nonpermanently within the conveyance, and they communicate using a common structured communication protocol.

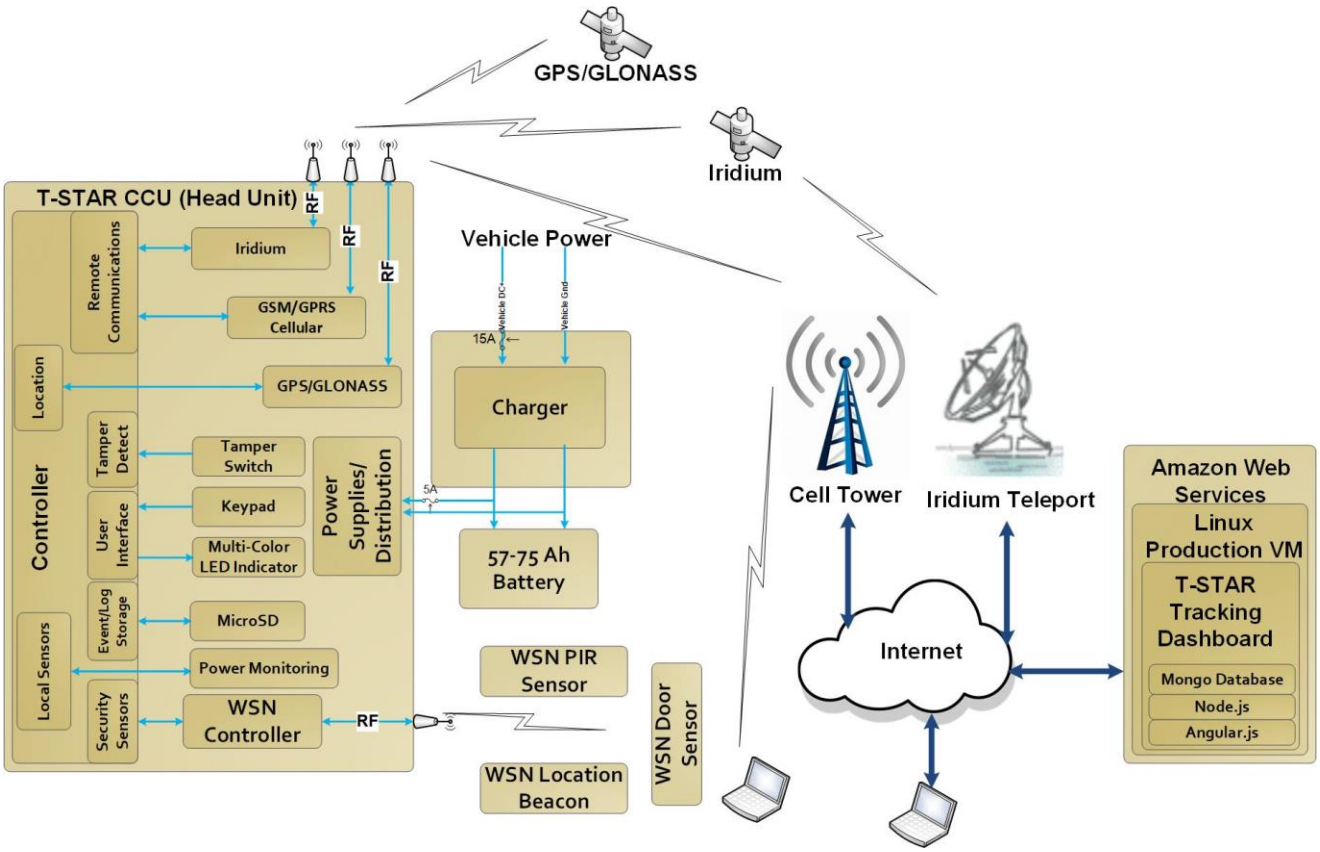

Figure 2. The T-STAR block diagram showing multiple communication modes, onboard and offboard wireless sensors, network infrastructure, and website services to monitor and assess the security of the shipment.

The T-STAR head unit aggregates operational information and security sensor status into messages that are transmitted via an available communications link depending on signal coverage. Based on time and severity, a T-STAR–transmitted message is routed using identification and configuration parameters and database tables to the T-STAR server securely via the internet. The server system parses and processes the message, keeps track of reporting times, translates identifiers into user-familiar names, converts location to geofence entering and exiting events, sends email and/or SMS notifications, and presents the events and information in sequence so the user can accurately assess shipment security.

T-STAR GEN 2

Since its initial development effort, T-STAR has undergone various improvements based on deployment experiences and various use cases. ORS has built three iterations of T-STAR—Gen 1; Gen 2; and a functional variation to Gen 2, the Gen 2i —to improve antenna connection reliability, facilitate SIM and SD card insertion and removal and intercomponent cable routing, and simplify the layout in the enclosure (**Error! Reference source not found.**). T-STAR Gen 2 versions use a Beaglebone Black as their main controller, a GPS/GLONASS receiver, a GSM cellular modem, and an Iridium satellite constellation modem on what is known as the T-STAR head unit.

Figure 3. The Gen 2 variations include the ability to independently switch between two antennas for each RF device, control the GPS device's low-noise amplifier, and altering component placement to facilitate inserting the SD card and SIM cards and enclosure cable routing.

Antenna switching was necessary to maintain GSM and Iridium communications and a GPS signal whether a container was within a closed metal conveyance being transported, outside the conveyance for loading or unloading, or if outside the conveyance, being diverted.

T-STAR GEN 3 DESIGN CONSIDERATIONS

T-STAR Gen 3 reduces power consumption to extend battery life, transitions to LTE cellular communications, expands environmental operation, and uses commercial-off-the-shelf (COTS) security sensors and protocols. Its inertial measurement unit (IMU) sensors help manage power consumption by using conveyance motion to determine if an updated location is needed. Some T-STAR applications can use power from an operating vehicle to maintain a charged battery, while others require a system that can remain operating for long periods using hazard-free batteries depending on the mode of transportation. The overall power usage of Gen 1 and Gen 2 T-STAR head units is high due to the relatively high-power consumption of the Beaglebone Black processing platform together with radiofrequency (RF) components power consumption: GPS, cellular, and satellite modems when powered, acquiring the network, and transmitting and receiving. Separating the system controller from the communications controller is the key design improvement to the head unit. Power savings are achieved by using the radios in smarter ways to reduce the average power consumption of the communications controller by turning radios on and off. The IMU senses motion to inform the system controller's decisions to turn communications components off when the conveyance is not in motion. A change in the WSN reduces power consumption. In earlier T-STAR versions, the operation of the Moteino (Arduino with a radio)–based security sensors required that the Moteino controller in the T-STAR head unit remain powered and continually listening for security sensor packets. The commercial replacement eliminates the requirement to fabricate sensors and offers lower power consumption devices. Other T-STAR Gen 3 features include a hardware security module (HSM) to sign and encrypt data and a peripheral slot to add additional capability.

The multidisciplinary research nature of Oak Ridge National Laboratory (ORNL) includes funding and direction for a variety of projects in security, remote sensing, and advanced communications. Technologies from two of these projects provide viable solutions to some of the T-STAR Gen 2 deficiencies. The Authenticatable Container Tracking System (ACTS) and Multimodal Autonomous Vehicle Network (MAVNet) are leveraged for T-STAR Gen 3. ORNL evaluated Z-Wave as a low-power replacement for the Moteino security sensors, determined operating characteristics and power savings, and assessed the commercial market as a viable global source for T-STAR sensors.

ACTS CIRCUITRY AND FIRMWARE

ORNL developed ACTS under the sponsorship and guidance of DOE's Environmental Management Packaging Certification Program to optimize chain-of-custody monitoring for packaged nuclear materials as they are being stored, processed, and transported. Based on the ultra-low-power Texas Instruments MSP430 mixed-signal microcontroller (MCU), ACTS is an active device that uses a universal core platform that can be configured with up to six expansion modules to provide application-specific data acquisition, data logging, container sealing, and communications functions needed for material accountancy, monitoring, and tracking applications [1]. This ACTS architecture enables appropriately designed modules to be easily interfaced to the core system, providing an integration path for current and new technologies.

The ACTS circuitry (Figure 4) consists of onboard dedicated environmental sensors (temperature, barometric pressure, relative humidity, and ambient light) and a nine-axis microelectromechanical system inertial measurement unit (IMU) that consists of an accelerometer, gyrometer, and magnetometer [2]. The IMU is used to detect motion or no motion and orientation, among other measurements.

Figure 4. The low-power ACTS circuitry with sensor suite and peripheral expansion slots extends capabilities, while the inertial measurement unit senses motion to reduce power consumption and allow smarter control of the communication device's power.

The latest version of the ACTS circuitry replaces the JTAG in-circuit programming connector with a Spy-Bi-Wire in-circuit programming connection using a spring-loaded-pin connection mechanism that reduces board space. The Spy-Bi-Wire is a serialized version of the JTAG protocol. The functionality of a console connection to facilitate firmware development and debugging is provided by a backchannel connection inherent to th MSP430 MCU programmer [3]. T-STAR Gen 3 benefits from using ACTS circuitry, onboard sensors, and expansion peripherals to have an *always-on* ultra-low-power controller, motion-sensing capability, and the ability to expand capabilities. Leveraging ACTS technology also includes reusing an extensive amount of existing firmware

ACTS PERIPHERAL EXPANSION

At its inception, the ACTS project addressed the need for a universal interface to accommodate various communication modules, sensor types, and future technologies. The ACTS base board provides the functionality required for a tracking system. To meet the specifics of any application requirements, the peripheral modules enable specialized sensor or communications technologies that the base board does not provide. Peripherals that currently exist for ACTS are an IEEE 802.15.4-2011 ultra-wideband-compliant impulse wireless transceiver module that has highly accurate ranging capabilities for indoor positioning and proximity location, a GPS peripheral, and a microSD card peripheral. Proximity-based location (in which an ACTS tag knows where it is relative to other

ACTS tags) is used as a continuity-of-knowledge mechanism to determine unauthorized movement of containers in storage arrays of many items.

The peripheral expansion bus is implemented using the 4-wire de facto standard serial peripheral interface (SPI) signals and additional signals to control selecting the peripheral by its slot and enabling power to it (Figure 2). Peripheral modules are based on a common reference design and an interface control document that describes the registers and information through them to the base board MCU. Using the peripheral module reference design as a template simplifies new module development because existing hardware designs and repositories of shared code can be reused. Following the reference design also ensures successful integration. Like the ACTS base board, each contains an ultra-low-power MSP430 MCU.

The peripheral processor allows the details of the peripheral to be abstracted away from the base board processor. Using an MCU on a peripheral module allows any peripheral circuitry to be implemented and the processing needed to control it to be distributed to the peripheral without requiring the peripheral circuitry to be directly controlled and processed by the base board MCU. An example of an expansion peripheral using the reference design is provided in Figure 5.

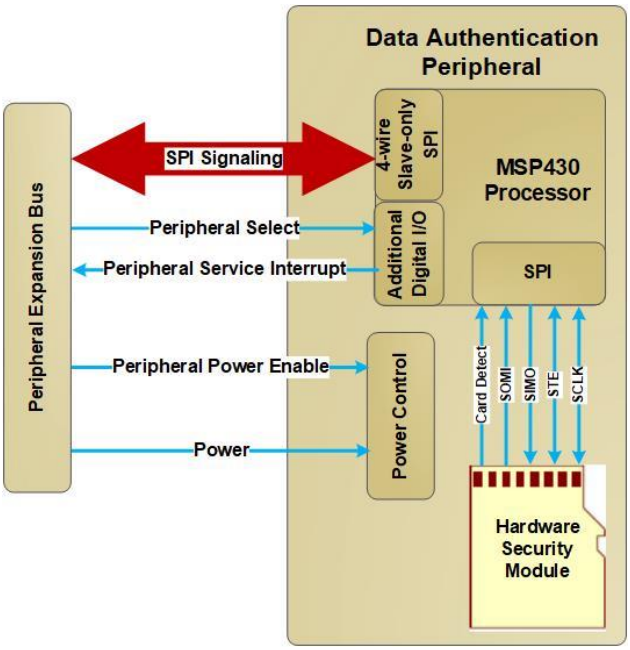

Figure 5. A data authentication peripheral performs public key infrastructure data authentication for digitally signing data to ensure nonrepudiation of transmitted data.

DATA SECURITY PERIPHERAL FOR SIGNING DATA

Data authentication is a key mechanism used to ensure data integrity and nonrepudiation for confirming that data received by a system is in fact the data that was generated by the system. The key principle of data authentication is signing the data at the data source. An accepted way of protecting the security keys and certificates associated with public key infrastructure (PKI) is to use specialized hardware storage and processing modules as a secure key store. Cryptographic operations, including data signing, are performed on these devices by sending the data to be signed to these devices and retrieving the cryptographic results, allowing the keys to remain protected on the device. These hardware modules are typically provided in various form factors: smart card, USB, microSD card, or integrated circuit.

IMPULSE-RADIO ULTRA-WIDEBAND COMMUNICATIONS PERIPHERAL

Since its inception, ACTS has been used with an impulse-radio ultra-wideband (IR-UWB) transceiver module to perform basic communications and provide precise indoor and outdoor locations [2]. The Decawave DW1000 is a complete, single-chip complementary metal-oxide-semiconductor ultra-wideband (UWB) transceiver integrated circuit that implements the UWB physical layer of the IEEE 802.15.4-2011 standard, enabling wireless sensor networks and real-time two-way-ranging-based location systems that can locate objects to within 10 cm [4]. The IEEE 802.15.4 standard was designed to deal with relatively short-range wireless personal area networks, and there is a portion of the standard that specifically addresses IR-UWBs that have now been authorized by regulatory bodies in most of the main geographies worldwide [5]. The standard also includes specific support for high-precision ranging.

MULTIMODAL AUTONOMOUS VEHICLE NETWORK

The Unmanned Vehicle Development Laboratory at ORNL is actively involved with beyond visual line of sight (BVLOS) communication systems that are an enabling component for unmanned system operations [6]. Commercially available BVLOS systems lack network diversity; however, MAVNet is able to seamlessly use three different radio systems, each operating at different latency scales to effect a global communications capability. T-STAR Gen 3 leverages this technology to implement a multichannel communications module (MCM). The MCM provides Iridium, cellular, GNSS, WiFi, Ethernet, and Bluetooth communications channels (Figure 6). The ACTS controller communicates serially with the MCM.

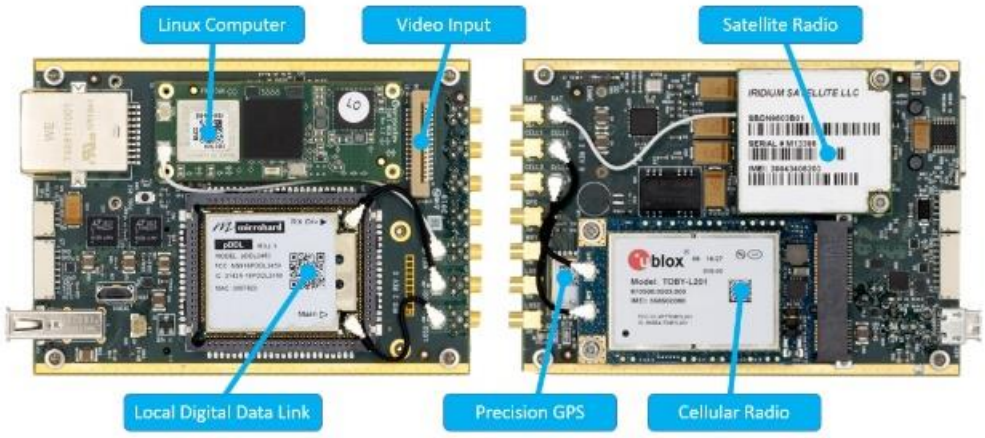

Figure 6. The multichannel communication module offloads the communications tasks from the controller and autonomously determines the optimum communication channel.

The MCM uses special low-power firmware to use the radios in the most efficient way. The firmware ensures that the most appropriate communications path is used based on the radio environment. If cellular infrastructure is available, it is used; otherwise, the satellite infrastructure performs the communication. T-STAR Gen 3 uses the MCM to reduce power consumption and provide robust and reliable autonomous communication.

Z-WAVE

The T-STAR system requires a WSN that is energy efficient and responsive and can detect sensor failure or removal. It must be responsive to multiple sensors with minimal latency and make adding or swapping a sensor easy but secure. Ideally COTS sensors can be installed with minimum invasion in the monitored conveyance. Because the Moteino system used in prior T-STAR implementations is

mainly a “roll and package your own” implementation requiring fabrication, the Gen 3 development effort took a new look at available technology. Z-Wave has been commercially available since 2003 and, as of the end of 2018, enjoys a robust corporate ecosystem and an outlook for future innovation [7].

The Z-Wave devices operate on a mesh network principle with up to 255 nodes possible. Any device within the network may be designated as a primary or secondary controller. Controllers store the routing table of all devices in network and determine whether a device is permitted to be in a network. Controllers can be portable (i.e., be allowed to move around within a network and not be in a fixed location). There are presently more than 2,600 Z-Wave certified interoperable products. Of interest to the T-STAR effort is the number of home security and access control vendors in the Z-Wave Alliance. This bodes well for wide availability of the sensors T-STAR uses for monitoring a conveyance. Z-Wave devices operate over a frequency range of 865.2 MHz to 926 MHz, with the exact chosen frequency dependent upon the country of operation

After an extensive evaluation of Z-Wave sensors, a Z-Wave controller, and Z-Wave operation and characteristics, Z-Wave was chosen to replace the Moteino-based security sensor infrastructure. Using Z-Wave sensors as the security sensors saves power and provides a commercial source for security sensors. Z-Wave sensors operate longer on their battery source than the currently implemented Moteino sensors. T-STAR Gen 3 includes a socket for either using either a Moteino or a Z-Wave controller as the wireless security sensor interface. Custom Z-Wave sensors can be fabricated.

T-STAR GEN 3 EXPANSION POSSIBILITIES

The peripheral expansion slot allows for expansion of T-STAR to a very wide field of use. It is conceivable that T-STAR Gen 3 could be a gateway for multiple containers with electronic tags and seals and radiofrequency identification devices (RFIDs) (Figure 7). Optical fiber seal electronics could be embedded on a peripheral module for sealing the T-STAR enclosure to the physical location in a conveyance and/or sealing the container T-STAR is being used to track. A radiation sensor interface could be implemented as a peripheral. With the additional communications capabilities of the MCM, Ethernet, WiFi, Bluetooth, and more, communications with any number of instruments could be performed.

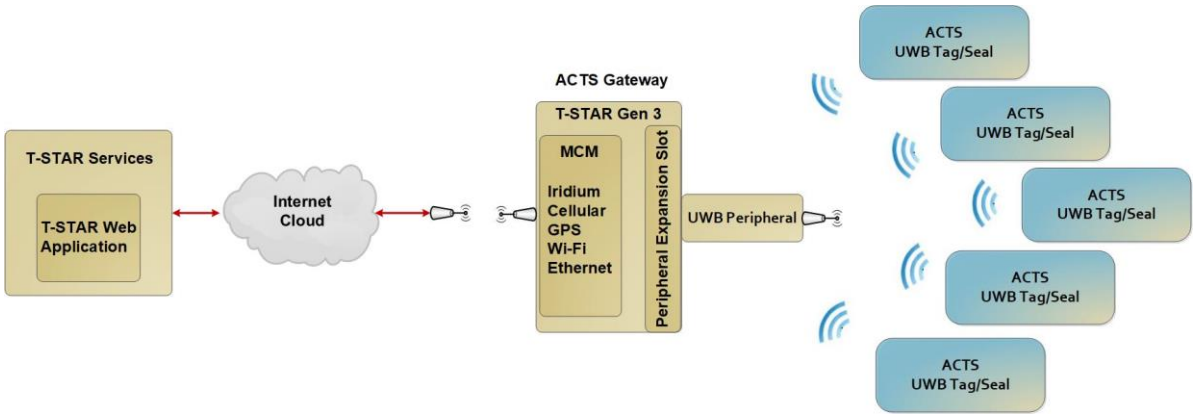

Figure 7. With a UWB impulse-radio peripheral in the T-STAR peripheral slot, ACTS tags/seals on containers being shipped can be continuously inventoried and reported during the shipment.

T-STAR GEN 3

T-STAR Gen 3 adds an expansion slot and a smart card HSM for PKI data signing and encryption. T-

STAR Gen 3 leverages the next-generation advanced autonomous communications module and incorporates an onboard battery charger and monitor and a Z-Wave WSN controller(Figure 8). The first two boards (Figure 9) are undergoing testing for proper operation. The MCM is complete and fully functional. A significant amount of firmware has been developed during the board-testing process. After testing the SPI peripherals, the next step will be to integrate the controller unit with the MCM and the Z-Wave controller and sensors.

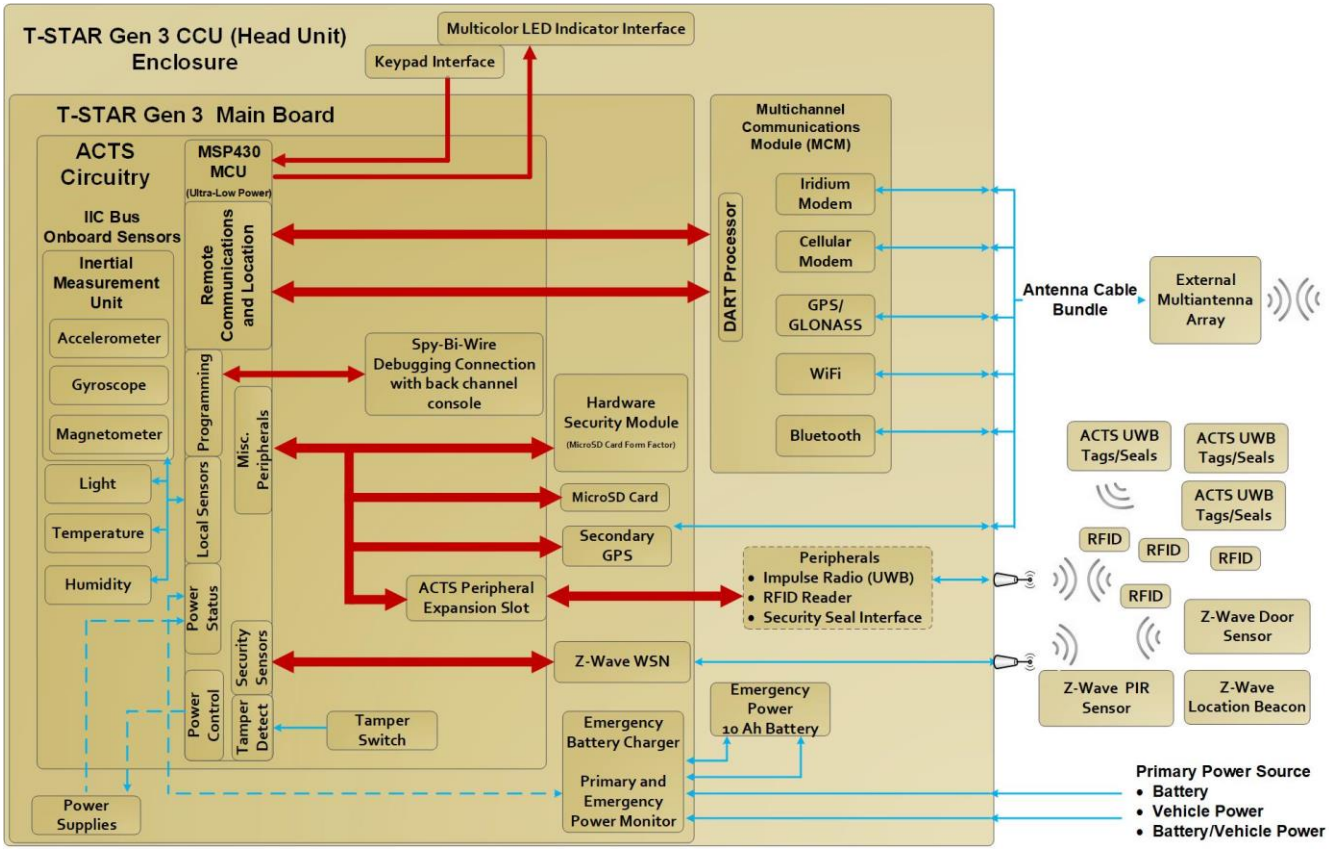

Figure 8. ACTS circuitry, with its onboard sensors and expansion peripheral slot implementation, is fused into the T-STAR Gen 3 design. A significant enhancement to the design is the multichannel communications module.

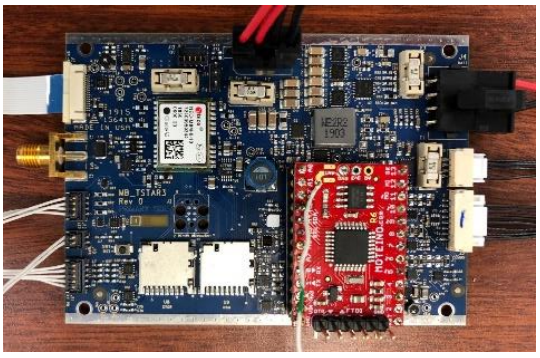

Figure 9. The T-STAR Gen 3 board controls the operation of the T-STAR head unit. A suite of onboard environmental sensors; an IMU; and interfaces to the MCM, HSM, microSD card, keypad, LED indicator, GPS unit, peripheral expansion slot, and WSN are included.

SUMMARY

T-STAR Gen 3 leverages hardware and firmware from ACTS and MAVNet to reduce power consumption (extend longevity when operating on battery power) and improve and extend communications capability and reliability. MAVNets robustness is requisite for controlling unmanned aerial vehicles anywhere in the world from anywhere in the world. T-STAR Gen 3 replaces the custom wireless security sensor network with COTS security sensors and protocols. The expansion slot and additional communications channels of the MCM allow interfacing of any number and types of instrumentation and sensors to collect more pertinent data for providing better situational awareness for the entire journey of sensitive cargo.

ACKNOWLEDGMENTS

This material is based upon work supported by the DOE Office of Environmental Management, Packaging Certification Program and the National Nuclear Security Administration, NA-21, ORS.

REFERENCES

[1] C. L. Britton et al., “Enhanced Containment and Surveillance System: Active Container Tracking System (ACTS),” presented at the 37th Annual ESARDA Meeting, May 18–21, 2015, Manchester, England.
[2] C. L. Britton, C. Pickett, J. Younkin, S. Frank, D. Floyd, J. Shuler, A. Nycz, R. Willems, Y. Liu, B. Craig, D. Krementz, and E. Farquhar, “Testing of the Authenticatable Container Tracking System (ACTS),” Proceedings of the 18th International Symposium on the Packaging and Transportation of Radioactive Materials, September 18–23, 2016, Kobe, Japan.
[3] J. Younkin, C. Britton, S. Frank, S. Stewart, E. Farquhar, and J. Shuler, “Advancing the Authenticatable Container Tracking Systems (ACTS),” INMM 2018, July 22–26, 2018, Baltimore, MD, USA.
[4] Decawave, “APS010 APPLICATION NOTE: Wireless Sensor Networks and the DW1000,” 2015, https://thetoolchain.com/mirror/dw1000/aps010_dw1000_wsn.pdf.
[5] Decawave, http://www.decawave.com.
[6] B. Stinson, A. Duncan, B. Vacaliuc, A. Harter, C. Roberts, and T. Thompson, “MAVNet: Design of a Reliable Beyond Visual Line of Sight Communication System for Unmanned Vehicles,” Association For Unmanned Vehicle Systems International Xponential 2019, April 29–May 2, 2019, Chicago, Illinois, USA.
[7] Z-Wave Alliance, “2018 End of Year Z-Wave Ecosystem Report,” 2018, https://z-wavealliance.org/wp-content/uploads/2019/01/Z-Wave-Alliance-End-of-Year-Report-FINAL-for-web.pdf.