ADVANCING THE TRANSPORTATION – SECURITY, TRACKING, AND REPORTING (T-STAR) SYSTEM[1]

M. SCHULTZE
J. YOUNKIN
B. VACALIUC
R. SALESKY
S. FRANK
N. BURCHFIELD
A. HACKETT
Oak Ridge National Laboratory (ORNL)
Oak Ridge, TN, USA
Email: schultzems@ornl.gov

T. THOMPSON
Cadre5, LLC
Austin, TX, USA

C. ASKEW
Cadre5, LLC
Knoxville, TN, USA

Abstract

The Transportation – Security, Tracking and Reporting (T-STAR) System was developed by NNSA NA-21 Office of Radiological Security (ORS) for secure detection and tracking of Category 1 and 2 radiological material shipments. While many off-the-shelf systems provide conveyance asset tracking, few can detect a breach into the cargo compartment or removal of cargo from the conveyance. Typically, such systems must be permanently installed on the conveyance, requiring dedicated containers or vehicles—not sustainable in many countries where ORS is building capacity for security of radioactive materials in use, storage, and transport. T-STAR leverages technologies developed at Oak Ridge National Laboratory to improve communications capabilities and reduce power requirements. The multimode communications module developed by the Unmanned Aerial Systems group and the low power, extensible Authenticatable Container Tracking System (ACTS) tag developed for the US Department of Energy's Packaging Certification Program provide a small footprint tracking system for quick installation. T-STAR uses a cellular and an Iridium modem to communicate configuration and alert information to a server that monitors shipments. A Z-wave© wireless security system allows intrusion detection sensors to be located in the conveyance. Z-wave sensors are readily available, inexpensive, power efficient, replaceable, and low maintenance. Server software can be configured as a standalone system on a light-duty computer hosted by a competent authority or as part of an Amazon Cloud Server accessible via secure login. The server handles messages to/from the field unit and hosts the user interface, accessible on a desktop or mobile device. The user interface implements roles to determine the level of access to shipment information, define geo-fences, and configure notifications. The interface supports multiple languages and provides notifications via a simple lookup file. The paper details overarching T-STAR capabilities, architecture, and components and provides insights on deployment, use, and monitoring during transportation of radioactive material.

1. 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 this type of use is expanding. T-STAR development began in 2014 under the sponsorship and guidance of the National Nuclear Security Administration (NNSA) Office of Defense Nuclear Nonproliferation (NA-

[1] Notice: This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The US government retains and the publisher, by accepting the article for publication, acknowledges that the US government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US government purposes. DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

21), Office of Radiological Security (ORS). The T-STAR concept is to convey location, operational, and security sensor status at regular intervals and to provide immediate alerts so that both can be used to assess the security of the shipment (FIG. 1). Conditions monitored include equipment operation details, whether equipment is communicating, security sensor alarms, and map location of the shipment.

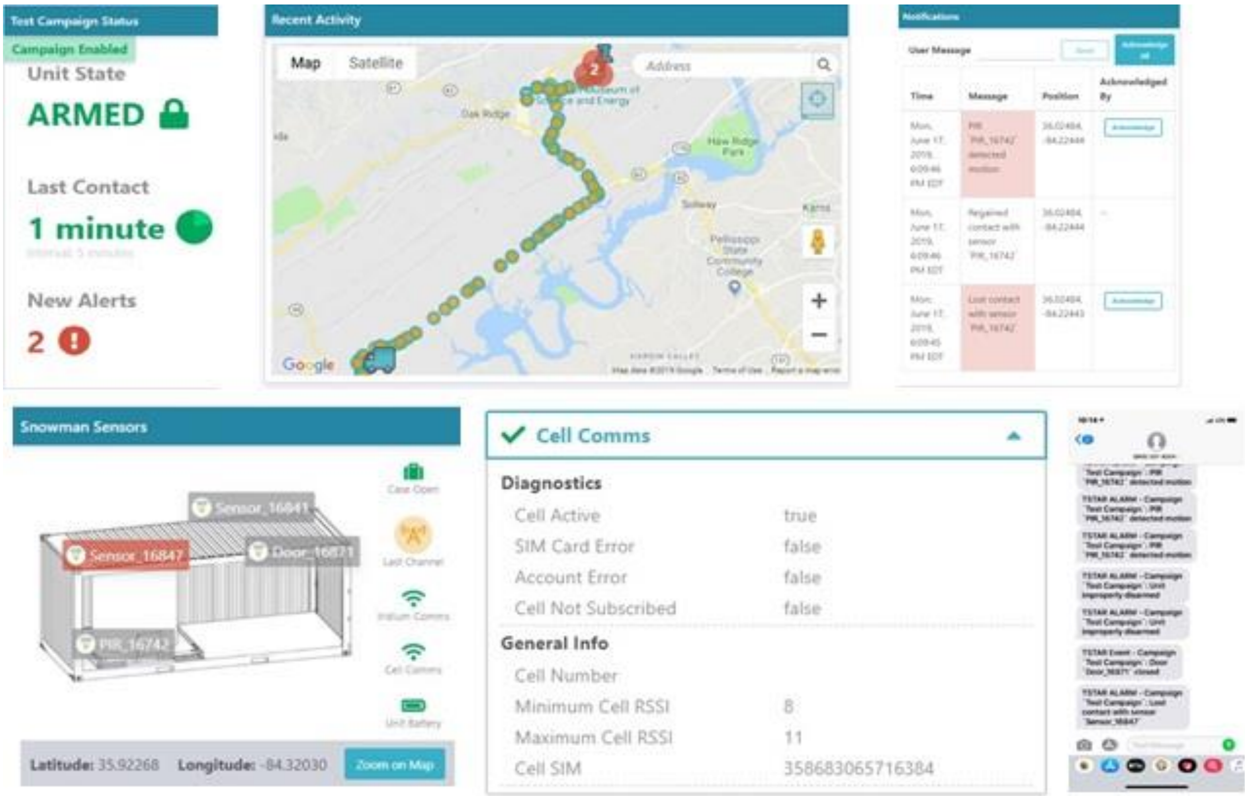

FIG. 1. The T-STAR web application runs on computers and smartphones, providing views that allow assessment of shipment status. Via the web application, a user may opt to receive SMS messages of system notifications.

To assess the security of the shipment remotely using a web application, equipment that delivers pertinent information must be used. T-STAR consists of (1) the electronics that "ride" with the shipment, (2) the cellular communications equipment that can use the available communications and network backhaul infrastructure along the route, (3) the satellite communications used when cellular access is not available, and (4) the backend database and monitoring web application (FIG. 2). These elements work together to provide the user with the pertinent information necessary for continuous security assessment. The security system uses a wireless sensor network (WSN) of security sensors monitoring motion within the conveyance or conveyance door openings and closings. These battery-operated sensors are placed within the conveyance temporarily, and they communicate using a common structured communication protocol.

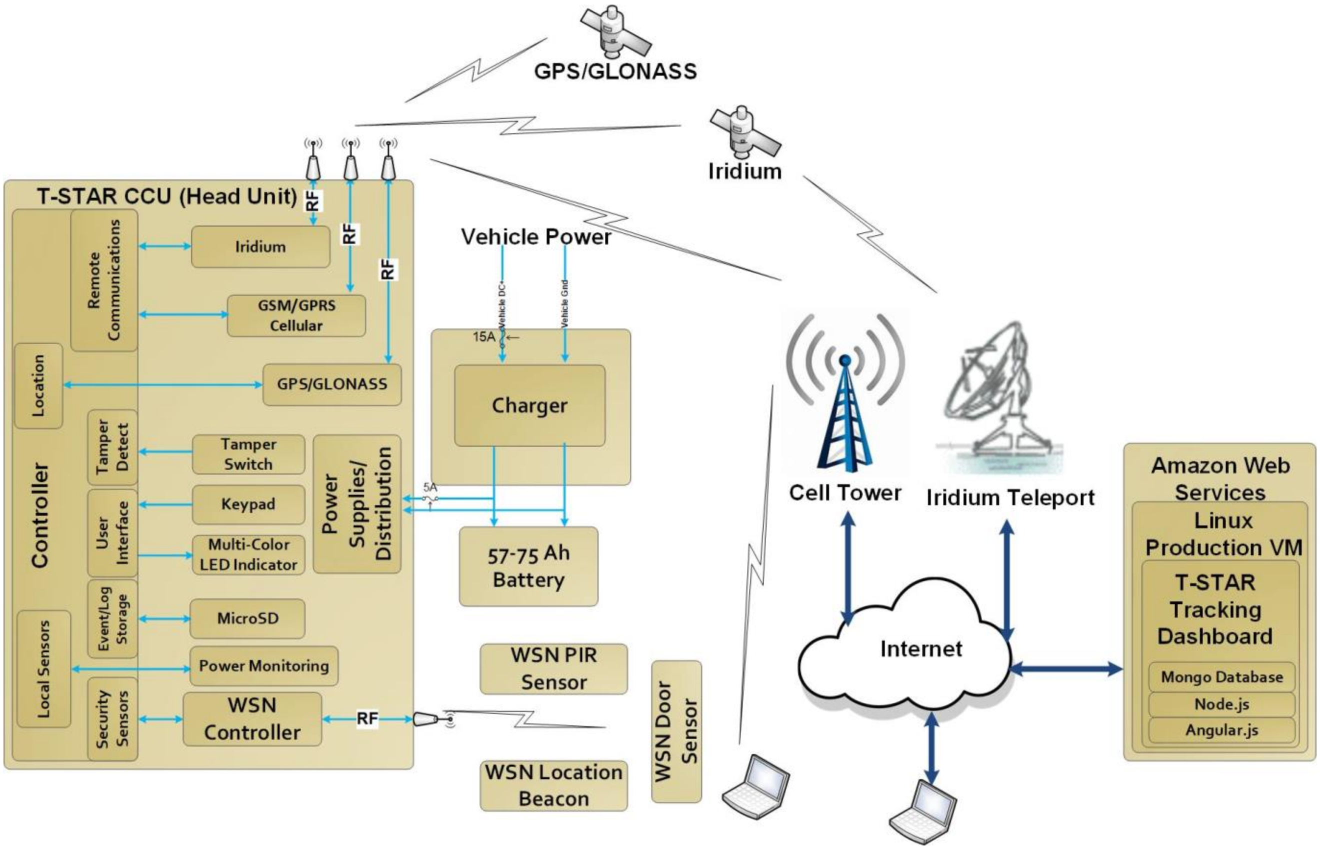

FIG. 2. T-STAR block diagram showing multiple communication modes, onboard and offboard wireless sensors, network infrastructure, and website services that monitor and assess the security of the shipment.

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 urgency, a message is routed to the T-STAR server securely via the internet using identification and configuration parameters and database tables. The server system parses and processes the message, tracks reporting times, translates identifiers into user-familiar names, converts the 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.

2. 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 Gen 2i, a functional variation to Gen 2. Gen 2i includes a more reliable antenna connection, and it facilitates SIM and SD card insertion and removal, as well as intercomponent cable routing. Gen 2i also has a simplified layout in the enclosure (Fig. 3). T-STAR Gen 2 versions use a Beaglebone Black as the 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. 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 outside the conveyance and being diverted.

FIG. 3. Gen 2 variations can independently switch between two antennas for each radiofrequency device, control the GPS device's low-noise amplifier, and alter component placement to facilitate inserting the SD and SIM and routing enclosure cables.

3. T-STAR GEN 3 DESIGN CONSIDERATIONS

T-STAR Gen 3 reduces power consumption to extend battery life, transitions to long-time evolution (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 a location needs to be updated. 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 power consumption from radiofrequency (RF) components such as GPS, cellular, and satellite modems when powered, acquiring the network, and transmitting and receiving. A key improvement to the T-STAR Gen 3 head unit was implemented by separating the system controller from the communications controller. The radios are turned on and off as needed, reducing the average power consumed by the communications controller. The IMU senses motion and informs the system controller's decisions to turn communications components off when the conveyance is not in motion. A change in the WSN also 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 devices that consume less power. Other T-STAR Gen 3 features include a hardware security module (HSM) to sign and encrypt data and a peripheral slot to add capability.

The multidisciplinary research conducted at 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 the 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 the operating characteristics and power savings, and assessed the commercial market as a viable global source for T-STAR sensors.

4. 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 the 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 (FIG. 4) consists of onboard dedicated environmental sensors (temperature, barometric pressure, relative humidity, and ambient light) and a nine-axis microelectromechanical system IMU that consists of an accelerometer, a gyrometer, and a magnetometer [2]. The IMU is used to detect motion or idleness, orientation, and other measurements.

FIG. 4. The low-power ACTS circuitry with sensor suite and peripheral expansion slots extends capabilities, while the IMU 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 the 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 allows for reuse of a significant amount of existing firmware

5. 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 with highly accurate ranging capabilities for indoor positioning and proximity location, a GPS peripheral, and a microSD card peripheral. Proximity-based location (which allows an ACTS tag to know 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, along with additional signals that control selecting the peripheral via its slot, enabling power to the bus (Fig. 2). Peripheral modules are based on a common reference design and an interface control document that describes the registers and information through the modules to the base board MCU. Using the peripheral module reference design as a template simplifies new module development by allowing reuse of existing hardware designs and repositories of shared code. Following the reference design also ensures successful integration. Like the ACTS base board, each module 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 can 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 FIG. **5**.

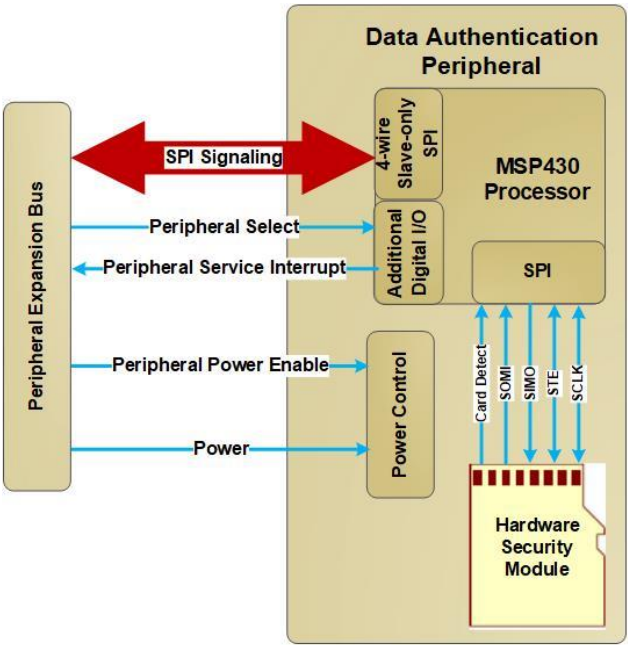

FIG. 5. A data authentication peripheral performs public key infrastructure data authentication for digitally signing data to ensure nonrepudiation of transmitted data.

6. 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.

7. 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 to provide precise indoor and outdoor locations [2]. The Decawave DW1000 is a transceiver 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 address relatively short-range wireless personal area networks, and a portion of the standard specifically addresses the IR-UWBs that are now authorized by regulatory bodies in most of the main geographies worldwide [5]. The standard also includes specific support for high-precision ranging.

8. 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]. While commercially available, BVLOS systems lack network diversity. MAVNet can 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 (FIG. 6). The ACTS controller communicates serially with the MCM.

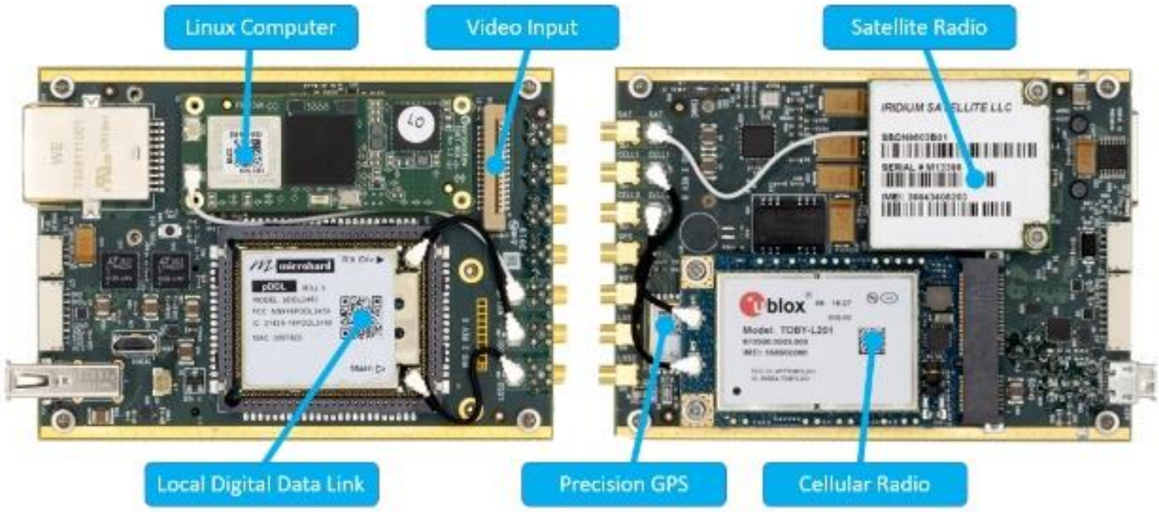

FIG. 6. The multichannel communication module offloads the communications tasks from the controller and autonomously determines the optimum communication channel.

The MCM uses special low-power firmware to ensure the most efficient use of the radios. 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, reliable autonomous communication.

9. Z-WAVE SENSOR NETWORK

The T-STAR system requires an energy-efficient, responsive WSN that can detect sensor failure or removal. It must be responsive to multiple sensors with minimal latency and must allow for adding or swapping a sensor easily and securely. 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, 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, it 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 to 926 MHz, with the exact chosen frequency dependent upon the country of operation

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

10. 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 RF identification devices (RFIDs) (FIG. 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 that 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.

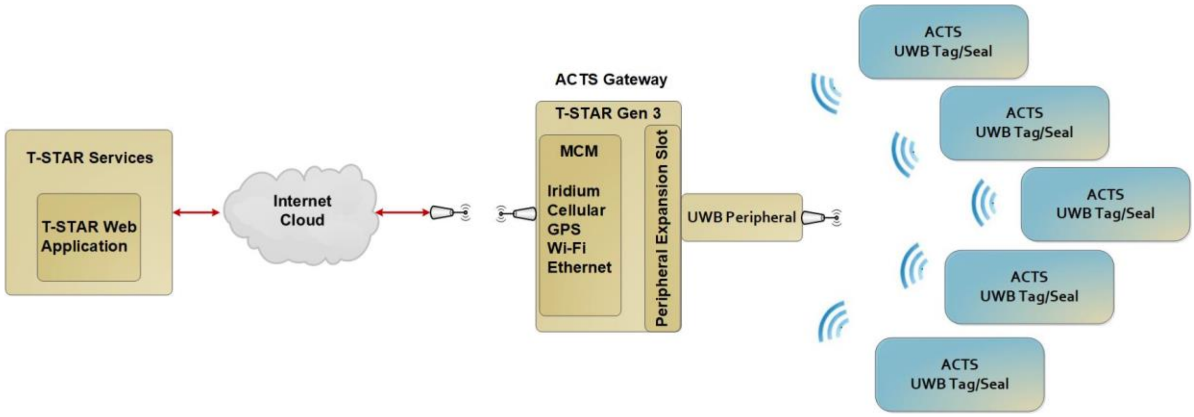

FIG. 7. With a UWB impulse-radio peripheral in the T-STAR peripheral slot, ACTS tags/seals on containers being shipped can be continuously inventoried and reported on during the shipment.

11. 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 it incorporates an onboard battery charger and monitor and a Z-Wave WSN controller (FIG. 8). The first two boards (FIG. 9) are undergoing testing for proper operation. The MCM is complete and fully functional. A significant amount of firmware has been developed during board testing. After the SPI peripherals have been tested, the controller unit will be integrated with the MCM and the Z-Wave controller and sensors.

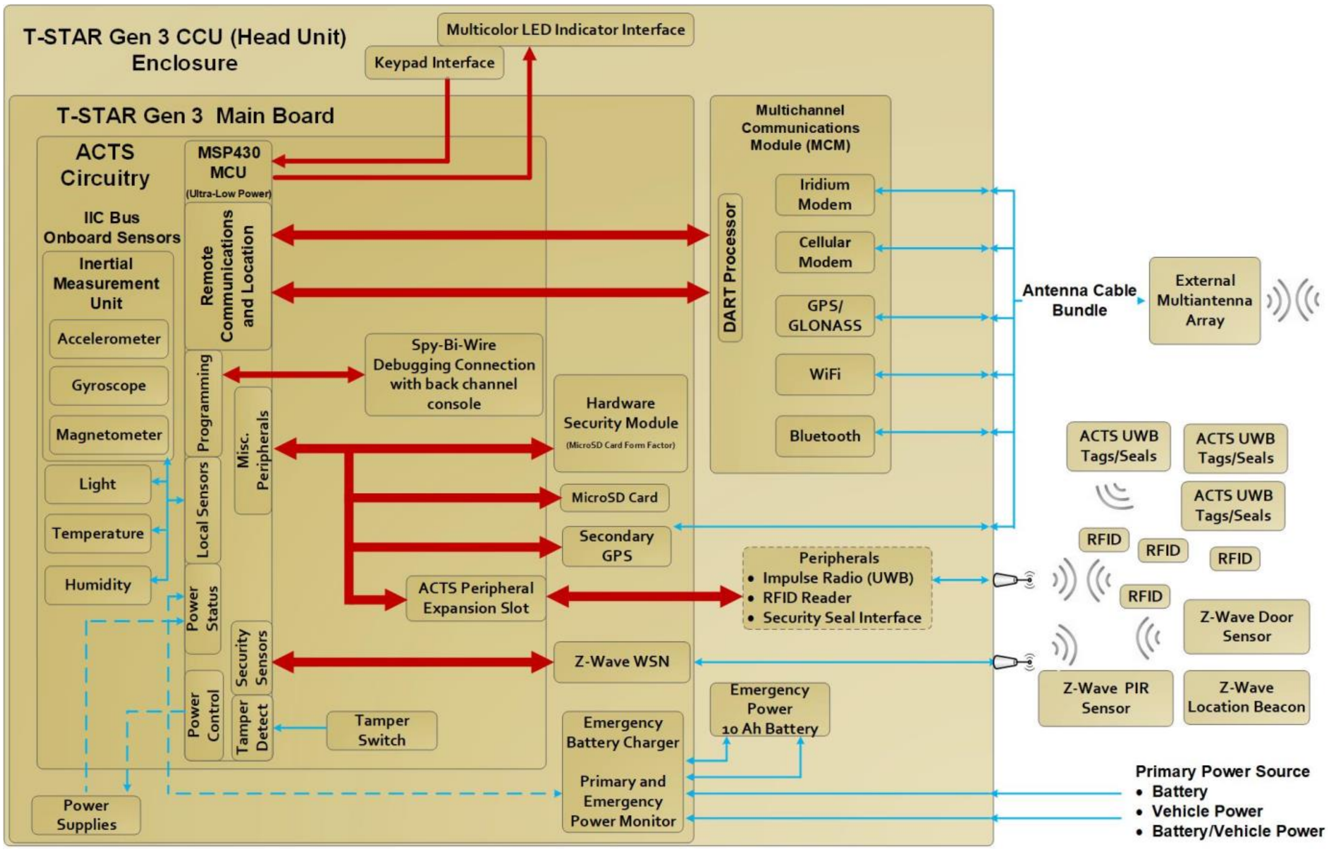

FIG. 8. ACTS circuitry, with its onboard sensors and expansion peripheral slot implementation, is fused into the T-STAR Gen 3 design. A significant enhancement to the design is the multichannel communications module.

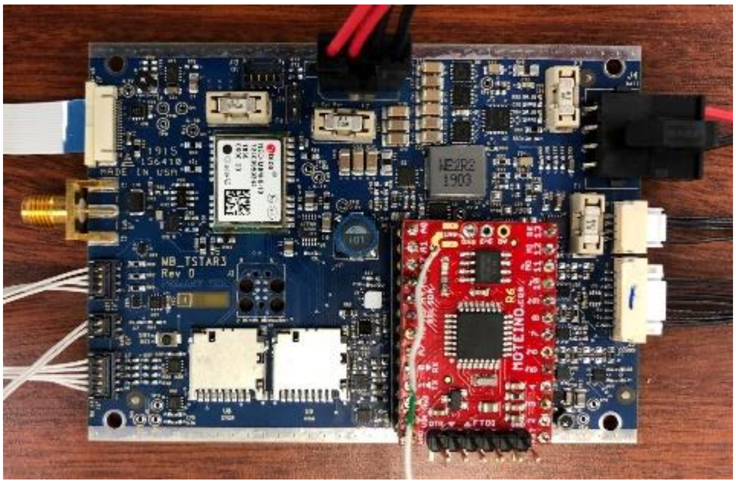

FIG. 9. The T-STAR Gen 3 board controls operation of the T-STAR head unit. A suite of onboard environmental sensors; an IMU; and interfaces to the MCM, HSM, microSD card, keypad, LED indicator, GPS unit, peripheral expansion slot, and WSN are included.

12. SUMMARY

T-STAR Gen 3 leverages hardware and firmware from ACTS and MAVNet to reduce power consumption, extending longevity when operating on battery power, and to improve and extend communications capability and reliability. MAVNet's robustness is requisite for controlling unmanned aerial vehicles from anywhere in the world as they are operating anywhere in the world. T-STAR Gen 3 replaces the custom wireless security sensor network with COTS security sensors and protocols. The MCM's expansion slot and additional communications channels allow for interfacing with any number and type of instrumentation and sensors to collect more pertinent data, 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] BRITTON, C. L., et al., "Enhanced containment and surveillance system: Active Container Tracking System (ACTS)," 37th Annual ESARDA Meeting (Manchester, England, 2015).

[2] BRITTON, C. L., PICKETT, C. YOUNKIN, J., FRANK, S., FLOYD, D., SHULER, J., NYCZ, A., WILLEMS, R., LIU, Y., CRAIG, B., KREMENTZ, D., and FARQUHAR, E., "Testing of the Authenticatable Container Tracking System (ACTS)," 18th International Symposium on the Packaging and Transportation of Radioactive Materials (Proc., Int. Symp., Kobe, Japan, 2016).

[3] YOUNKIN, J., BRITTON, C., FRANK, S., STEWART, S., FARQUHAR, E., and SHULER, J., "Advancing the Authenticatable Container Tracking Systems (ACTS)," INMM (Baltimore, MD, 2018).

[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] STINSON, B., DUNCAN, A., VACALIUC, B., HARTER, A., ROBERTS, C., and THOMPSON, T., "MAVNet: Design of a Reliable Beyond Visual Line of Sight Communication System for Unmanned Vehicles," Association For Unmanned Vehicle Systems International Xponential (Chicago, Illinois, 2019).

[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.