Advancing the Authenticatable Container Tracking System (ACTS)

James Younkin[1], Charles Britton[1], Shane Frank[1], Scott Stewart[1], Ethan Farquhar[2], Raymond Dunn[2], and James Shuler[3]

[1]Oak Ridge National Laboratory, Oak Ridge, TN, USA

[2]Pacific Northwest National Laboratory, Richland, WA, USA

[3]Packaging Certification Program, US Department of Energy, USA

Abstract

The Authenticatable Container Tracking System (ACTS) is an extensible secure container tag that can be used to optimize chain-of-custody monitoring for packaged nuclear materials as they are being stored, processed, and transported. Based on the ultra–low power TI MSP430 mixed-signal microcontroller, ACTS is an active device that uses an almost-universal core platform that can be appropriately configured with expansion modules to provide the application-specific data acquisition, data logging, container sealing, and communications functions needed for 21st century material accountancy, monitoring, and tracking applications. This core architecture enables appropriately designed modules to be easily interfaced to the basic system, providing an integration path for current and new technologies. ACTS contains a built-in set of sensors and supports an expansion bus for up to six additional communications, tracking, authentication, encryption, sealing, location, or sensing modules that may enhance the monitoring and tracking of designated containers for specific applications. To date, testing has used an IEEE 802.15.4-2011 ultra-wideband–compliant wireless transceiver module that has additional capabilities for indoor positioning and proximity location. Proximity-based location (i.e., where an ACTS tag knows where it is relative to other ACTS tags) will be explored as a continuity-of-knowledge mechanism to determine unauthorized movement of containers in storage arrays of many items. Partners for this system are Oak Ridge National Laboratory, Argonne National Laboratory, Savannah River National Laboratory, Pacific Northwest National Laboratory, and commercialization partner the Aquila Group.

Introduction

Previous papers on the Authenticatable Container Tracking System (ACTS) discussed how the ACTS concept and architecture provides an almost-universal platform for active monitoring of device containment and location and how it reports its status at regular intervals via a chosen communication method, including how it interfaces to the Argonne ARG-US TransPort software for review via a web-based user interface incorporating geographical information system elements, tag event history tables, a current tag status pane, and a tag sensor report generator [1, 2]. Some details of the ACTS peripheral interface and its utility for extensibility, and multiple tag testing campaigns have also been presented [3]. Testing of ACTS modules including a variety of both functional and environmental monitoring outdoors and indoors have also been reported. The testing was initially focused on functionality of the built-in sensors and the software/firmware used to drive them.

This paper will provide further insight into the capabilities and operation of the peripheral expansion capability, the ACTS peripheral interface details, and its distributed processing nature. Finally, using ACTS in safeguards applications where data must be authenticated and ACTS real time location systems capability using the DW1000 impulse-radio ultra-wideband (IR-UWB) radio will be explored.

ACTS Base Board

The ACTS base board consisting of a core microcontroller unit (MCU) (Texas Instruments MSP430) and four onboard sensors is shown in Figure 1. The onboard sensors consist of dedicated environmental sensors (temperature, barometric pressure, relative humidity, and ambient light) and a nine-axis microelectromechanical system inertial measurement unit containing an accelerometer, gyrometer, and magnetometer. The integrated peripherals are interfaced through an Inter-Integrated Circuit (I2C or IIC) interoperable, short-distance, intra-board bus interface by the MSP430. The inertial measurement unit and light sensor can awaken the MSP430 via interrupt control lines based on certain conditions of movement or ambient light change. The base board has its own dedicated battery that powers only the base board processor and resident sensors. Events based on sensor values are stored in memory and can be queued for off-board communications.

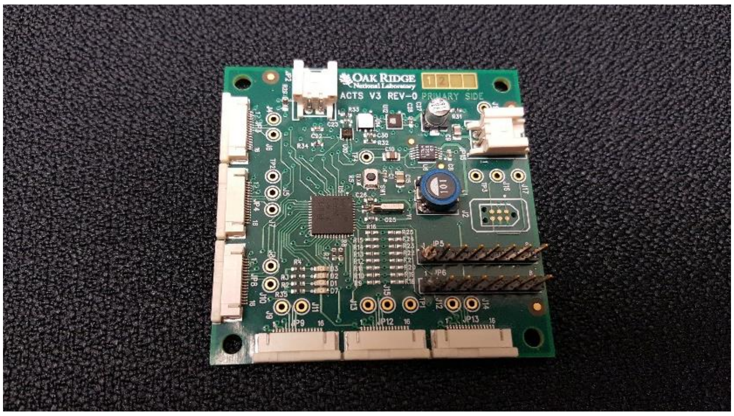

Figure 1. The size of the ACTS base board has been significantly reduced.

The latest version of the ACTS base board replaced 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 USB connection and circuitry that provided a console/debug connection to ACTS was removed to reduce board space. The functionality of the console/debug connection is now provided by a backchannel connection inherent to the MSP_FET, an MSP MCU programmer, using additional pins alongside the Spy-Bi-Wire connection. The MSP_FET is the USB programmer that provides the JTAG or Spy-Bi-Wire connection between the software development PC and the MSP430. It also provides a secondary virtual COM port that can be wired to a MSP430 UART. To increase the capability to perform two-way ranging, the MCU was also changed from a different MSP430 part to one with more RAM.

Peripheral Expansion

At its inception, the ACTS requirements addressed the need for a universal interface architecture to accommodate various communication modules, sensor types, and future technologies. The ACTS base board provides the base functionality required for a tracking system. To meet the specific of the application requirements, the peripheral modules provide specialized functionality that the base board does not provide. A Global Positioning System (GPS) peripheral module has been built, and a smaller-footprint IR-UWB peripheral module has been designed.

The peripheral expansion bus consists of six dedicated connectors that allow peripheral modules to be connected to the base board. The peripheral expansion bus interface 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). Power is provided to the peripheral by the base board, or the peripheral can be powered independently. The MSP MCU has native SPI functionality for both SPI master and SPI slave operation. The SPI expansion bus uses the MSP430 in a master configuration with the expansion peripherals' MSP430 configured as slaves. Connectivity between the base board and peripheral expansion bus is provided by a 16-pin, 0.5-mm pitch ribbon connector.

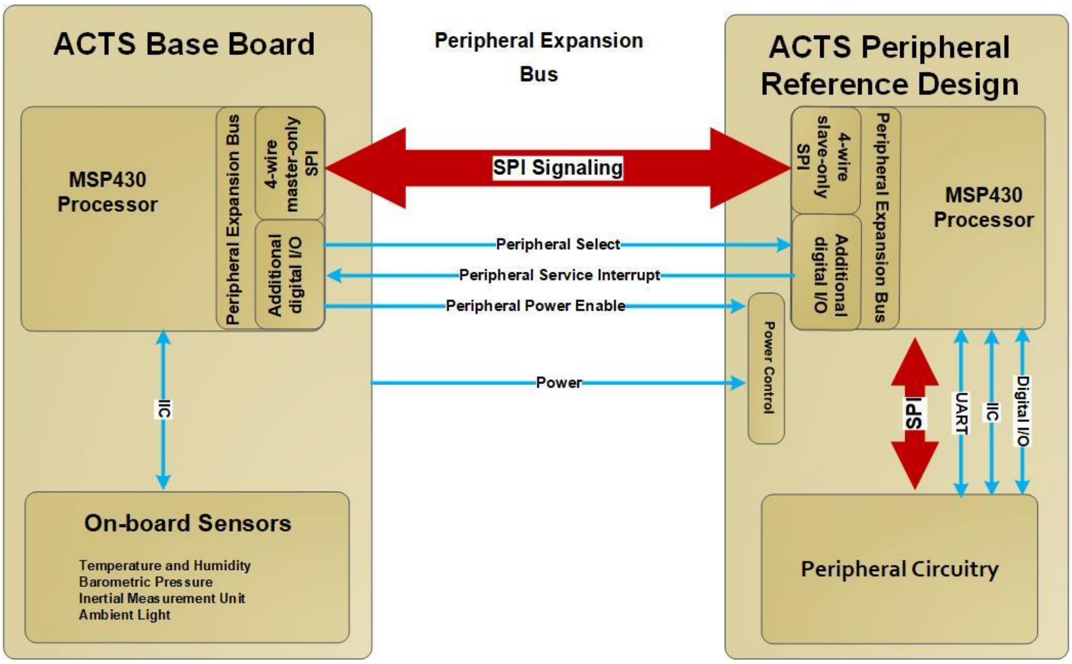

Figure 2. The ACTS base board architecture, built on the low-power MSP family of processors, incorporates a base set of relevant sensors and a peripheral interface for matching ACTS to specific applications.

Peripheral module designs are based on a common peripheral reference design and an interface control document that describes the common registers and information contained in the registers presented by the peripheral modules to the base board MCU. Having a peripheral module reference design as a template simplifies new peripheral module development since existing hardware designs and existing code bases of common code can be reused. Following the reference design also insures successful integration. Like the ACTS base board, the peripheral reference design is also based on the low-power MSP430 MCU to take advantage of the multiple native interfaces of the 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 it allows the processing needed to control it to be distributed to the peripheral and not require the peripheral circuitry to be directly controlled and processed by the base board MCU. The native digital interfaces available to the MSP430 family of MCUs typically are interfaces for IIC, universal asynchronous receiver-transmitter, SPI, and general purpose digital signals. With the native digital interfaces, analog I/O channels, timers, and counters available in MSP430 devices, any peripheral should be capable of being implemented for ACTS.

The interface control document governs the common behavior that the base board communicates with peripheral modules. The interface control document describes a common command set and register description for identifying, configuring, obtaining the status, and reading from and writing to the peripheral modules. Using a common interface to a common MCU simplifies peripheral module development by allowing reuse of common firmware. The base board MCU can identify each type of peripheral module and configure the tracking application to utilize the functionality provided by the specific combination of peripheral modules plugged into the base board. The base board communicates with each peripheral module distinctly by “selecting” it for communications by the peripheral select line associated with the slot that the peripheral module is connected to. The base board can also manage the power use of peripherals by turning power to the peripherals off and on for specific conditions.

Having a peripheral expansion bus with an assortment of ACTS peripheral modules (such as communications, GPS, or other sensor modules) allows tailoring an ACTS system for the concept of operations and with the hardware that meets the regulatory requirements for specific applications and locations. The peripheral classes for ACTS, shown in Table 1, consist of modules that provide communications, data storage and security, additional sensors, containment monitoring, and location services. Being able to select specific peripheral modules means that the same base hardware, software, infrastructure, database, and reporting are used for an ACTS system whether the ACTS tag is configured for a typical nuclear material tracking application with a cellular network with GPS locations, an active seal, and radiation sensors or if it is configured for large local data storage with encryption, additional sensors, and no off-tag communication.

Table 1. Possible Peripheral Types by Peripheral Classes

Communications	Data Storage and Security	Additional Sensors	Containment Monitoring	Location Services
Cellular-3G, LTE	Micro SD Card	Gamma	Active Fiber Seal	GPS
Iridium	Smart card hardware security module	Neutron		UWB Indoor Location (Using UWB Communications Peripheral)
UWB				UWB Nearest Neighbors (Using UWB Communications Peripheral)
Wi-Fi				

Data Security Peripheral for Signing Data

Data authentication is a key mechanism used for international safeguards 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 as close to the data source as possible. For ACTS to be used in a safeguards regime, that would mean that the information provided by ACTS would need to be signed by ACTS before any data transmission or retrieval, and the signature be embedded in the data packet or accompany the packet as a separate transmission or file. The International Atomic Energy Agency currently uses a public key infrastructure for the data signing function. A secure way of protecting the security keys and certificates associated with public key infrastructure is to use specialized hardware storage 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, and allowing the keys to remain protected on the device. These hardware modules typically are provided in various form factors: Smart card, USB, MicroSD card, and even integrated circuit. To be able to support the public key infrastructure , the crypto-hardware security module currently deployed at the International Atomic Energy Agency department of safeguards for the provision and use of security credentials like data authentication keys, an ACTS peripheral could be developed to use either the integrated circuit or the MicroSD card form factor of the hardware security module.The base board would pass data to be signed to the hardware security module peripheral, the hardware security module peripheral would generate the cryptographic signature of the data using the key, the base board would retrieve the results, and the base board would store or queue the results for transmission using a communications peripheral.

Impulse-Radio Ultra-Wideband Communications Peripheral

Since its inception, ACTS has been used with an IR-UWB transceiver module to perform basic communications and provide precise indoor and outdoor location. The DW1000 is a complete, single-chip complimentary metal-oxide-semiconductor Ultra-Wideband transceiver IC that implements the UWB physical layer of the IEEE802.15.4-2011 standard enabling wireless sensor networks and two-way ranging based real time location systems locating objects to within 10 cm [4]. The IEEE802.15.4 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-UWB 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.

For ACTS, a primary benefit of the IR-UWB peripheral module is its ranging and location capability. Although various schemes exist to perform ranging and location functions, they basically fall into two categories: (1) received signal strength indication and (2) signal propagation time measurement. Propagation time-based schemes using IR-UWB can achieve far more accurate results than received signal strength indication–based schemes [6].

Basic two-way ranging is accomplished between two DW1000s by exchanging messages with each other to determine the time it takes for the radio waves to travel between them. Using these times and the speed of the radio waves, the distance between the two DW1000s can be calculated. The asymmetric double-sided two-way ranging method, where multiple exchanges communicating the timing between two DW1000s occur, is an alternate method used in some implementations to reduce clock and frequency drift errors [7].

Inspection Inventory

Increases in efficiency and reductions in operating costs can be obtained by using ranging to locate items that require an inventory. A locating infrastructure of anchor transceivers positioned at known points is needed to determine the absolute position of tagged assets in 2-D or 3-D space. This scenario is shown in Figure 3. The same UWB modules used in the tags are used in the infrastructure anchors. The location and identifiers of the tagged items can be visualized on a PC. Since the infrastructure is quite small and wireless, the anchors can be temporarily set up by placing anchors around the facility at inventory time and registering their locations in the visualization software. If a permanent infrastructure is desired, the possibility that the fixed anchor locations will be subject to tampering must be considered.

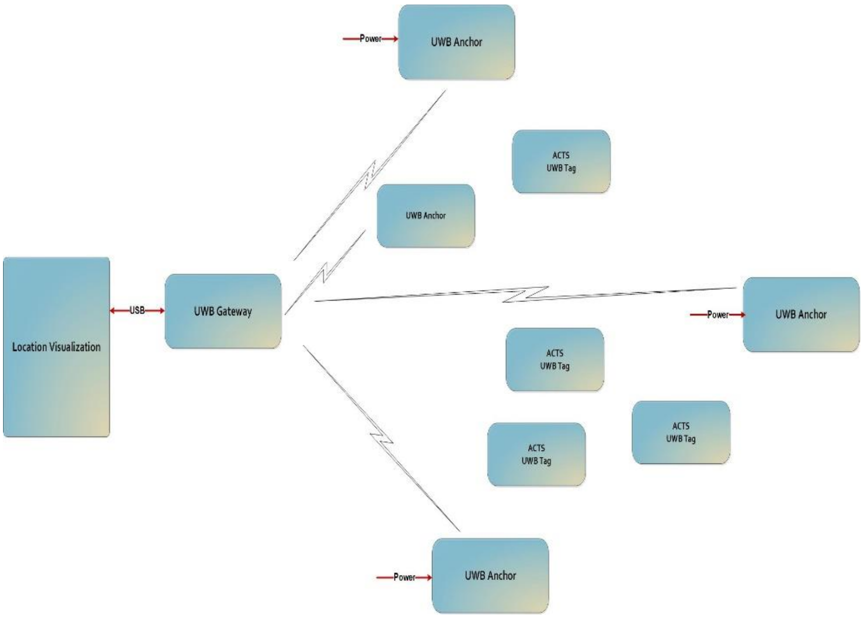

Figure 3. Infrastructure-based ranging to locate items uses an infrastructure of anchor transceivers at known locations and a visualization system to show tagged assets.

Relative Location

In this scenario, fixed anchor infrastructure is not used, so tags only establish where they are located in relation to other tags. The relative distance to each responding tag is determined. In storage situations where the movement of items within the storage area will be restricted, the detection of the movement of tagged items could be determined in this manner. By adding a single anchor at a fixed location in Figure 4, geofencing of the tags can be performed. If a tagged item is moved beyond a specified distance from the reference tag, an invalid movement event can be logged.

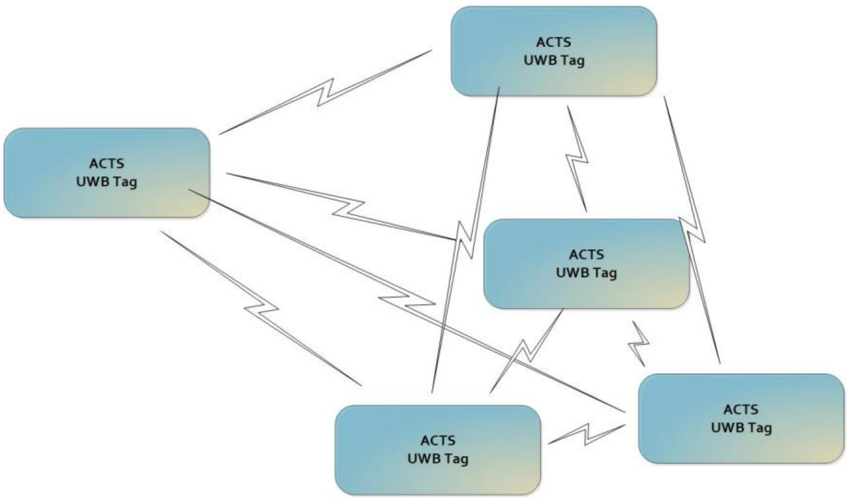

Figure 4. Relative ranging between tags lets each tag determine the distances to neighboring tags and identify relative movements.

Conclusions

The vision for ACTS is to provide a secure container tag that can be used to optimize chain-of-custody monitoring for packaged nuclear materials as they are being stored, processed, and transported. At its inception, the ACTS requirements addressed the need for a universal interface architecture to accommodate various communication modules, sensor types, and future technologies. An ACTS data security peripheral would allow data acquired by ACTS sensors to be digitally signed to ensure data integrity and nonrepudiation, which is one of the data security requirements for safeguards applications. The IR-UWB peripheral enables two-way ranging for locating ACTS tags in 2-D or 3-D space to facilitate an inventory or to detect the repositioning or movement of ACTS tagged items.

Acknowledgements

This material is based upon work supported by the U.S. Department of Energy, Office of Environmental Management, Packaging Certification Program.

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] J. Anderson, H. Lee, P. De Lurgio, C. M. Kearney, B. Craig, I. H. Soos, H. Tsai, Y. Liu, and J. Shuler, "Tracking and Monitoring with Dosimeter-Enabled ARG-US RFID System," Waste Management 2012 Conference, February 26–March 1, 2012, Phoenix, Arizona, USA.

[3] 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

[4] Decawave, "APS010 APPLICATION NOTE: Wireless Sensor Networks and the DW1000," 2015. Available: https://thetoolchain.com/mirror/dw1000/aps010_dw1000_wsn.pdf.

[5] Decawave. [Online]. Available: http://www.decawave.com.

[6] Decawave, "APS003 Application Note: Real Time Location Systems, An Introduction," 2015. Available: https://www.decawave.com/sites/default/files/aps003_dw1000_rtls_introduction.pdf.

[7] Decawave, "APS013 APPLICATION NOTE: The Implementation of Two-way Ranging with the DW1000," 2015. Available:

https://www.decawave.com/sites/default/files/aps013_dw1000_and_two_way_ranging_v2.2.pdf.