Detecting Removal of the Authenticatable Container Tracking System (ACTS) from a Container or Conveyance

James Younkin, Charles Britton, Shane Frank, Scott Stewart

Oak Ridge National Laboratory, Oak Ridge, TN, USA

James Shuler

Packaging Certification Program, US Department of Energy, USA

PATRAM 2019, August 4-8, New Orleans, LA

ORNL is managed by UT-Battelle, LLC
for the US Department of Energy

Agenda

- ACTS Background
  - Concept
  - General Capabilities
  - Peripheral Expansion Bus
  - Data Authentication
  - Impulse Radio – Ultra Wideband
  - Two-way ranging
- Magnetic Attachment
- Removal Detection
- Conclusion

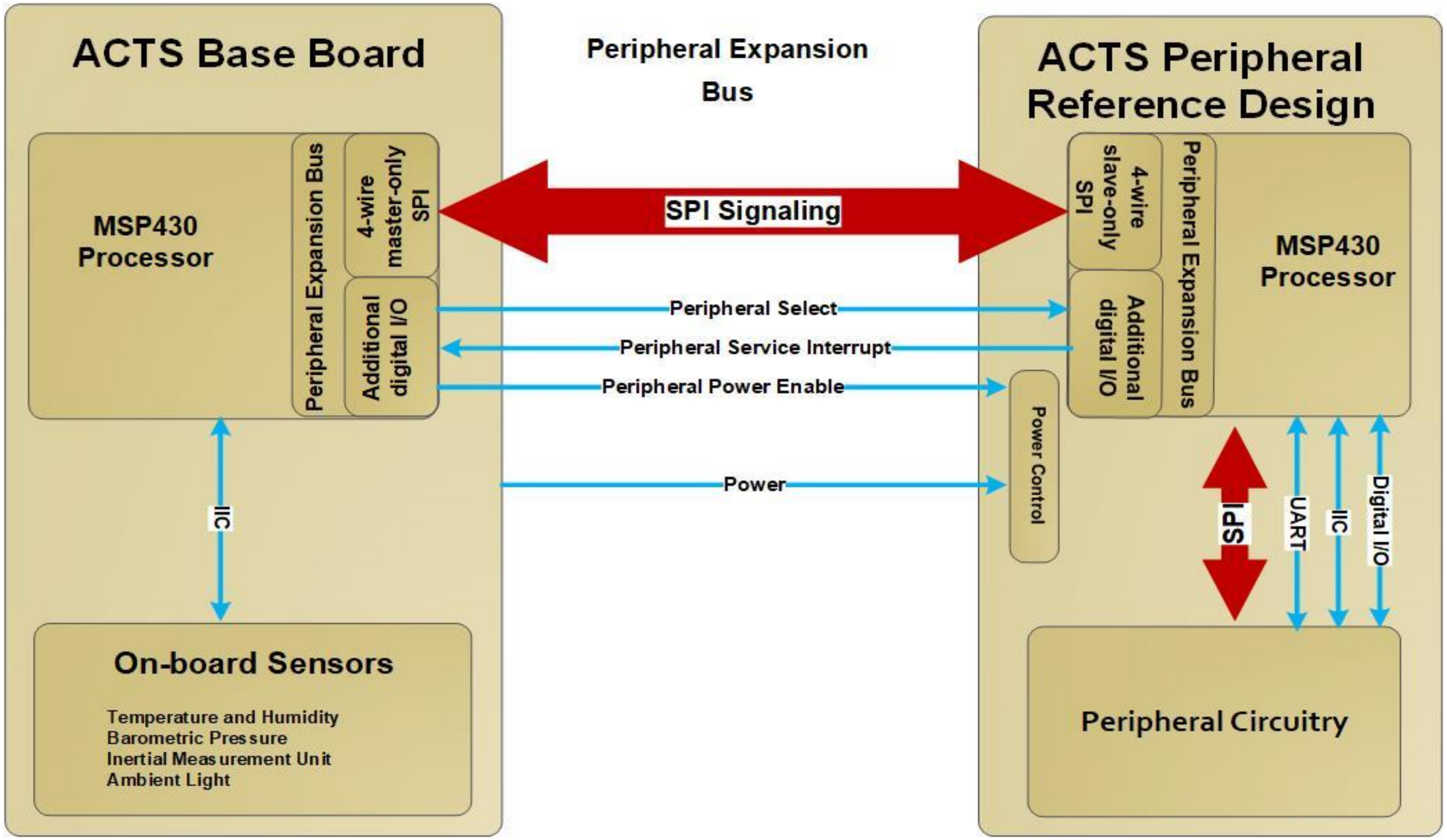
The concept for the Authenticatable Container Tracking System (ACTS)……

- The ACTS concept provides a universal platform, compatible with the ARG-US Transport server, for active monitoring of package containment and location and report status at regular intervals via selectable communication methods.
- ACTS will store sensor events in memory, work with other applicable systems and follow IAEA best practices for data security and authentication.
- ACTS incorporates a universal interface architecture that will enable future peripheral modules to be easily interfaced to the system thus providing an integration path for new technologies.

Design features of the latest version of the ACTS base board allowed the footprint to be reduced.

- Replaced JTAG in-circuit programming connector with Spy-Bi-Wire
- Removed USB console/debug port – use MSP FET programmer console/debug back channel
- Replaced MCU with one in the family having more memory

The ACTS base board Architecture, built on a very low power processor, incorporates a base set of sensors and a peripheral interface for adapting to specific applications.



Peripherals to the motherboard with their own processor and a common interface – read, write, status, configure

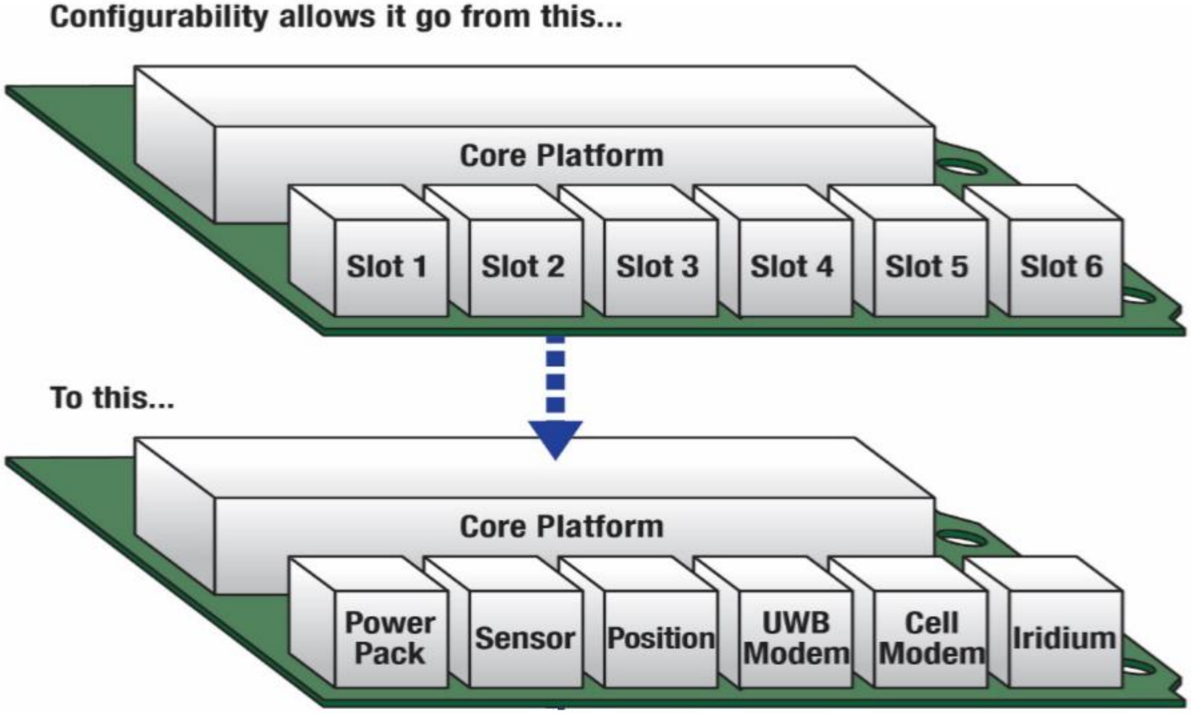
Existing Smart Peripherals

- UWB transceiver
- GPS
- Micro SD Card
- SC-HSM (smart card hardware security module) – IAEA PKI Infrastructure – Encrypt and or sign data – Basically a variant of the micro SD Card peripheral

Peripheral Possibilities

- Iridium transceiver
- Cellular transceiver
- Radiation sensors
- Fiber Loop
- Z-Wave Security Sensor transceiver

Adaptable for multiple applications



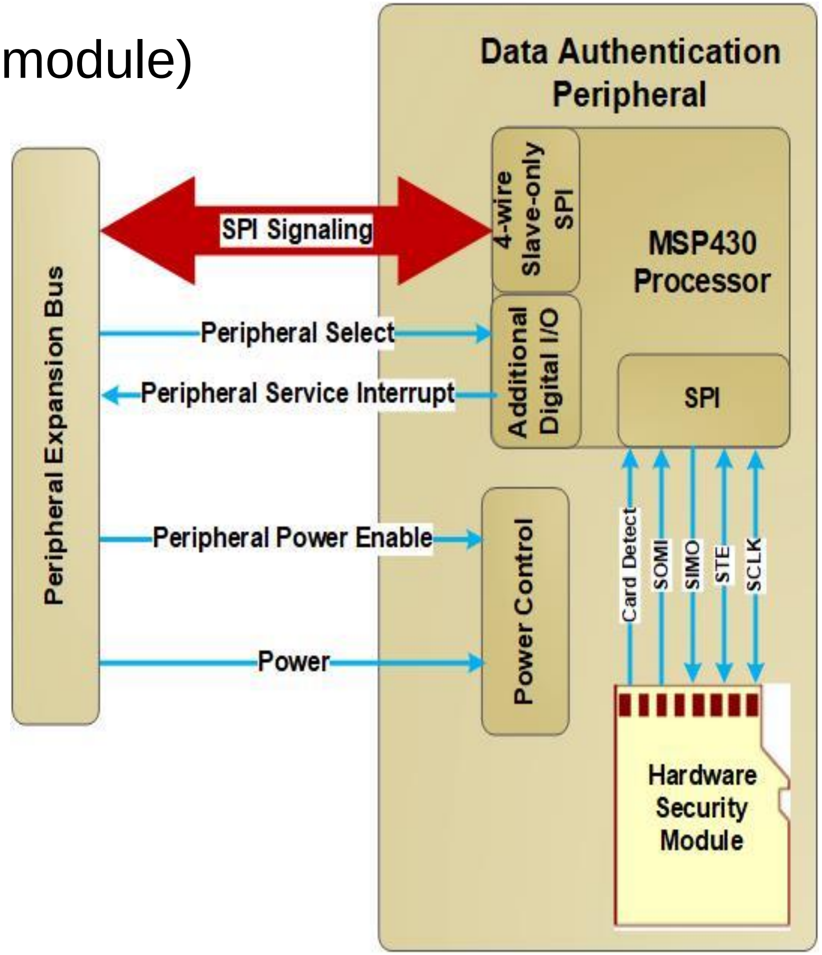
The data authentication peripheral performs public key infrastructure data authentication for digitally signing data to ensure nonrepudiation of transmitted data.

SC-HSM (smart card hardware security module)

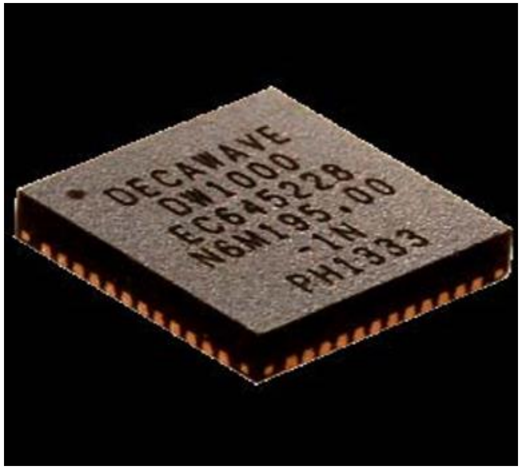
- PKI Infrastructure
- Encrypt and or sign data

Sign transmission packet on the head unit

Validate received packet on the server



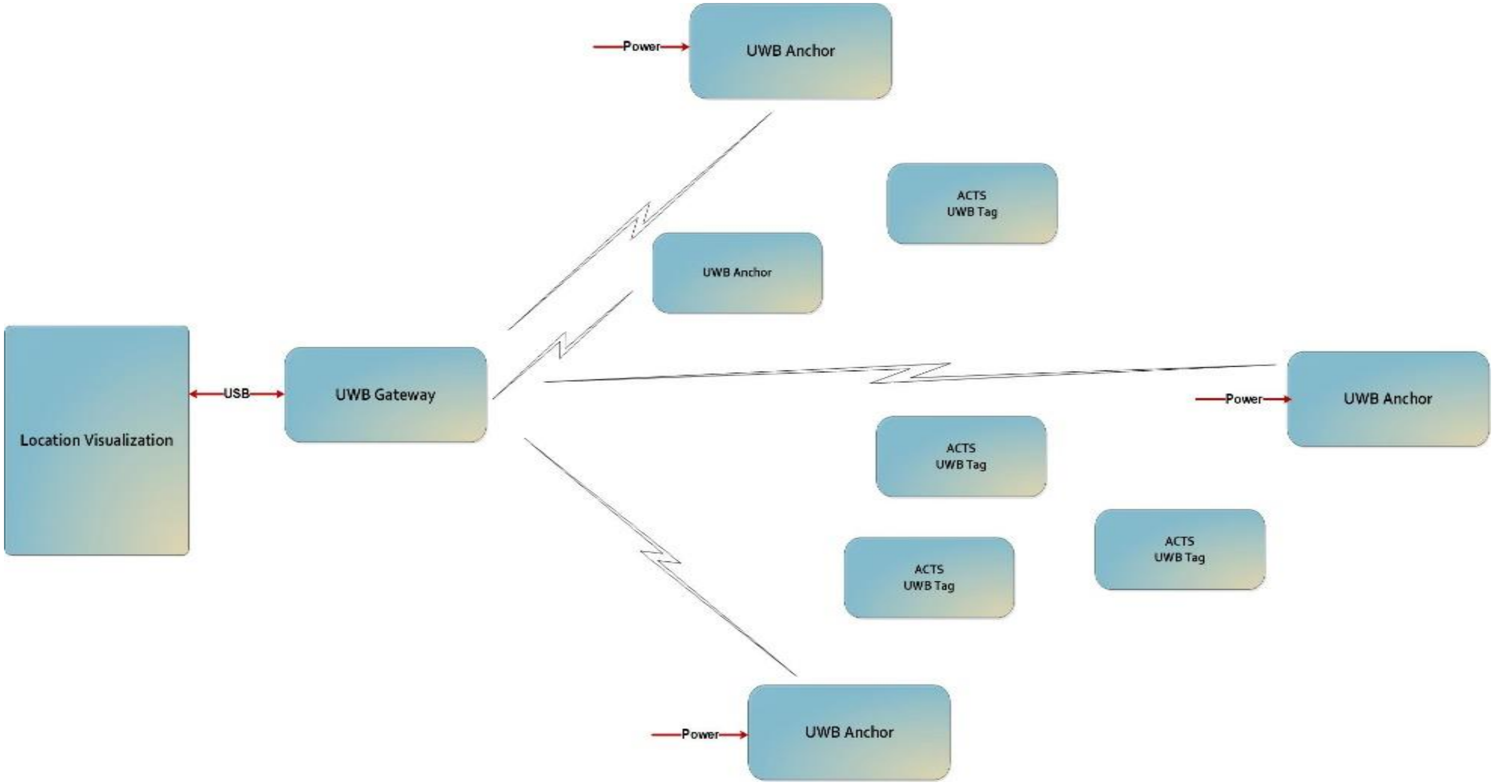
DecaWave DW1000 IR-UWB



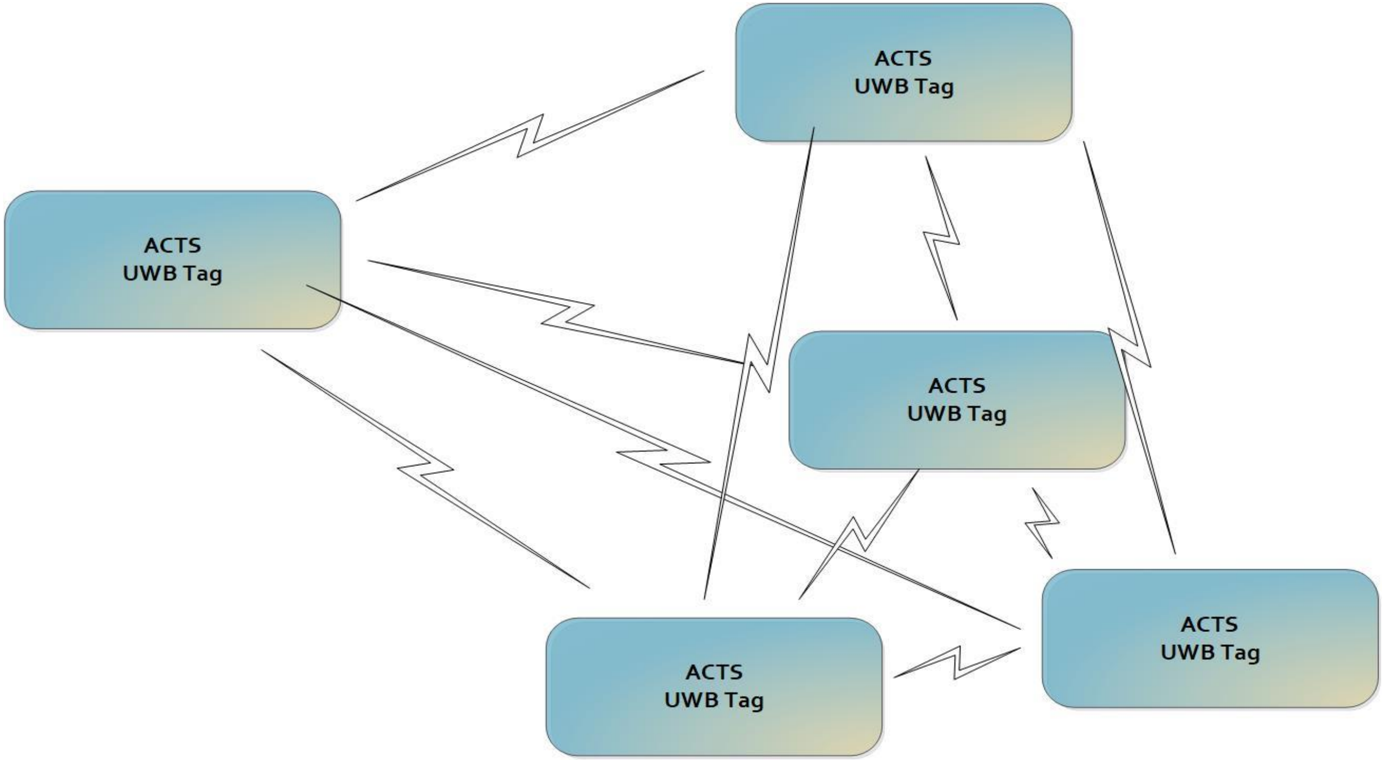
- Single chip UWB transceiver
- IEEE802.15.4-2011 Standard
- Real Time Location capabilities (10cm indoors)
- Up to 6.8 Mbps
- Coherent receiver (300m range)
- Short packet durations (11,000 devices in a 20m radius)
- Highly immune to multipath fading
- Low power consumption (mode dependent)
- Two-way ranging

Source: decawave.com

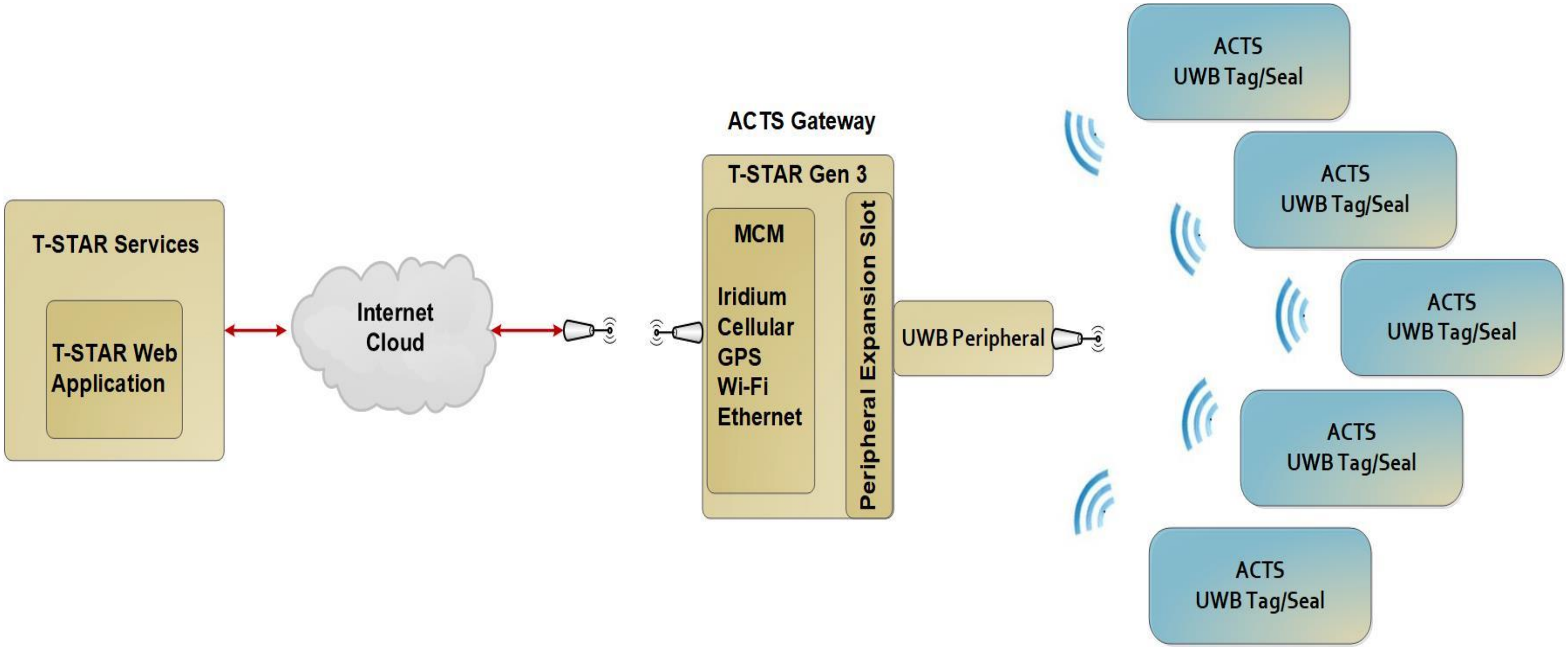
Infrastructure based ranging to locate items for an inspection inventory uses an infrastructure of anchor transceivers at known locations and a visualization system to show tagged assets.



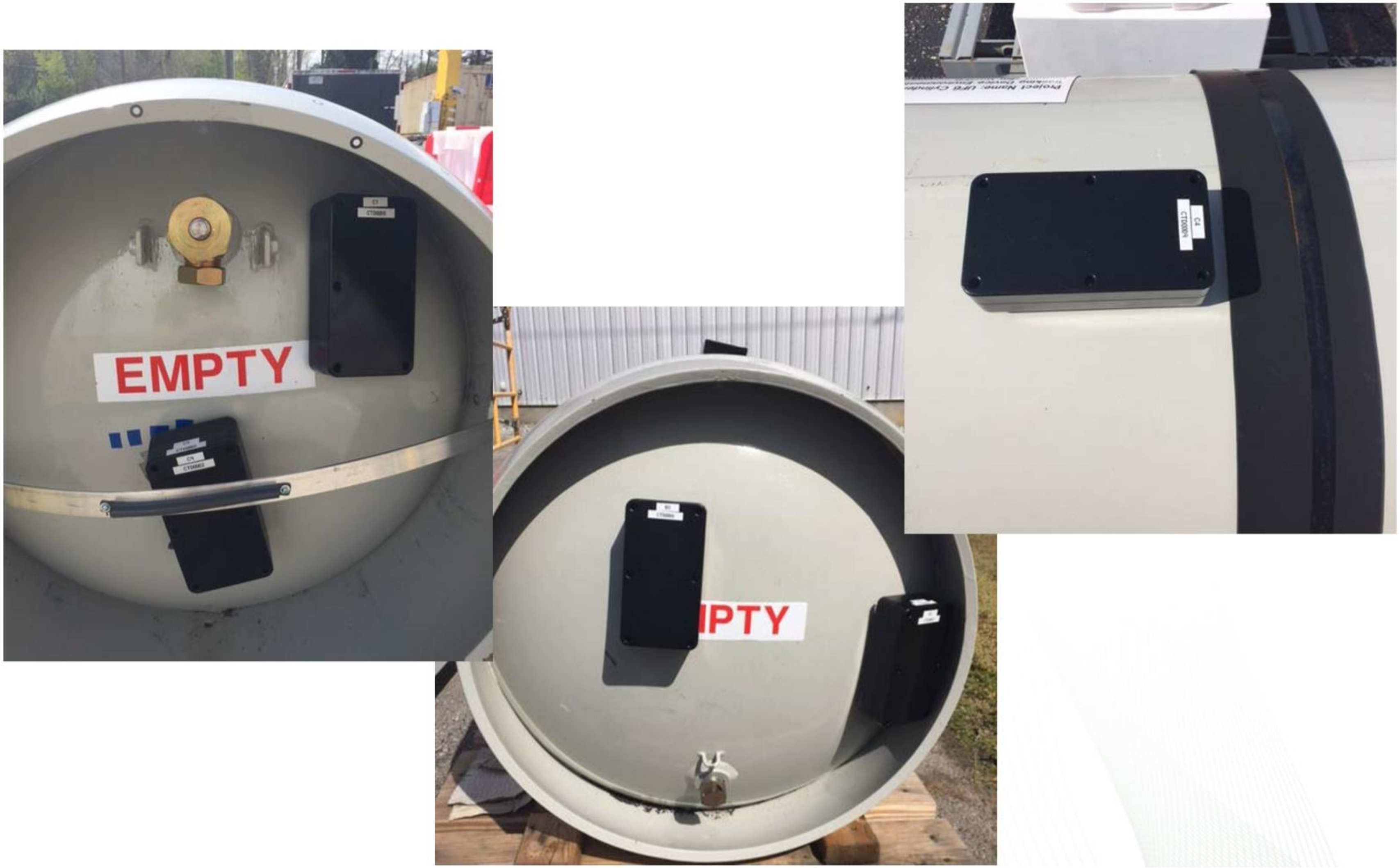
Relative ranging between tags lets each tag determine the distances to neighboring tags to determine relative movements.



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.



ACTS Tags Magnetically Attached to UF6 Cylinders



Anomaly Detection with ACTS Magnetometer Data

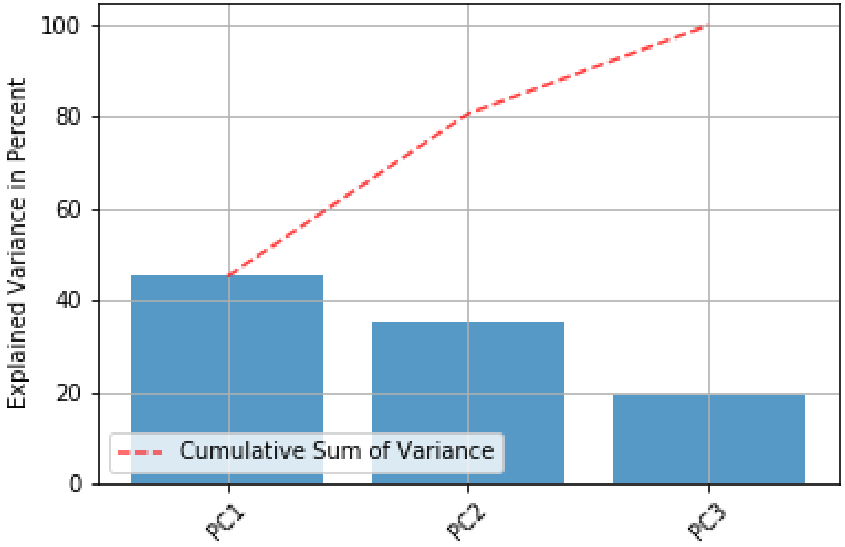
- Hypothesis:
  - An anomaly detection approach will perform better than simple thresholds for detection tag removal from metal objects
- Test Design:
  - Collected data with the ACTS tag being removed from a metal surface in different ways
  - Ground truth was indicated by the state of a switch
- Method:
  - Principal component analysis was used in conjunction with a T^2 statistic to test for anomalies indicative of removal in the 3-axis magnetometer data

Anomaly Detection – Data Cleaning

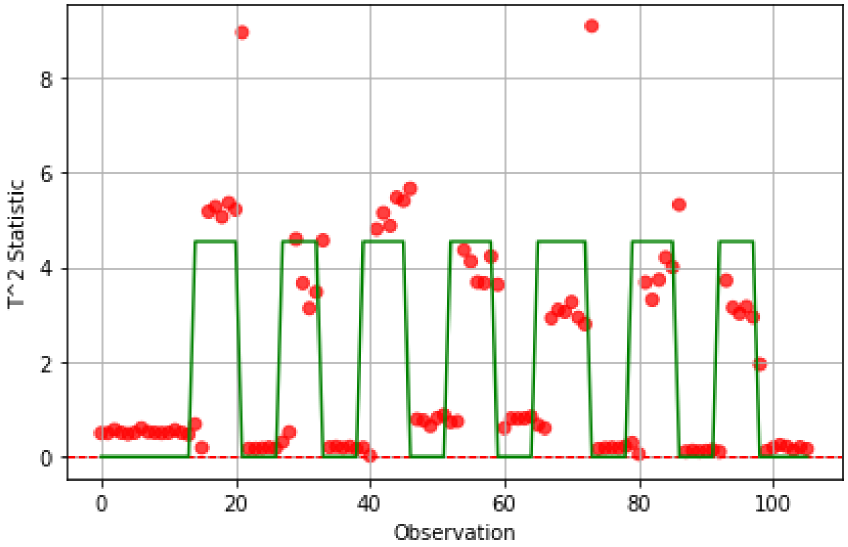
- Data Split:
  - Data was split 50-50 between testing and validation data sets
- Standardization
  - The z-score method was used to standardize the test data set
  - The mean and standard deviation of the test data set were also used to standardize the validation data set

Anomaly Detection Method – Dimensionality Reduction

- Principal component analysis (PCA):
  - Dimensionality reduction approach
  - Translates raw data into a new dimension space with orthogonal components that aim to captures as much of the variance in the original data as possible
- Plot shows the variance captured in principal component space as additional axis are added.
- PC3 explains all the variance because it has the same dimensionality as the original magnetometer data
- 2 PCs were chosen for our method



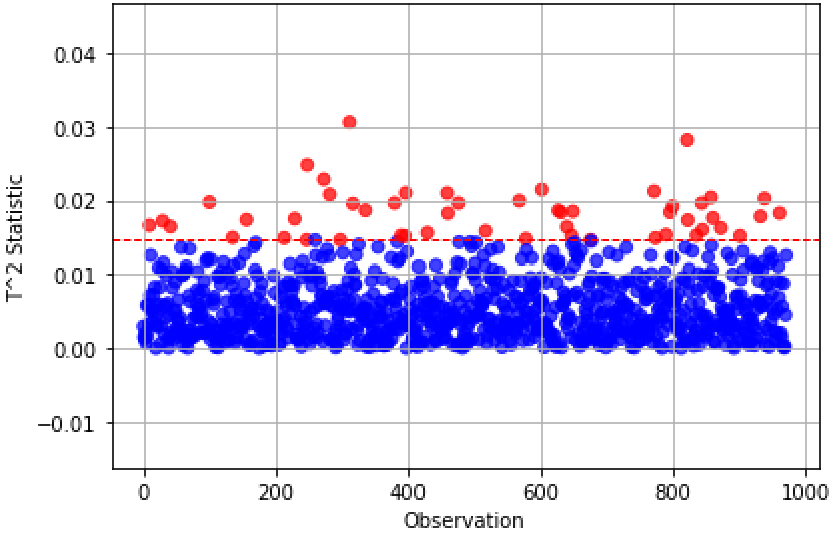
Anomaly Detection Method – Hotelling's T^2 Statistical Test



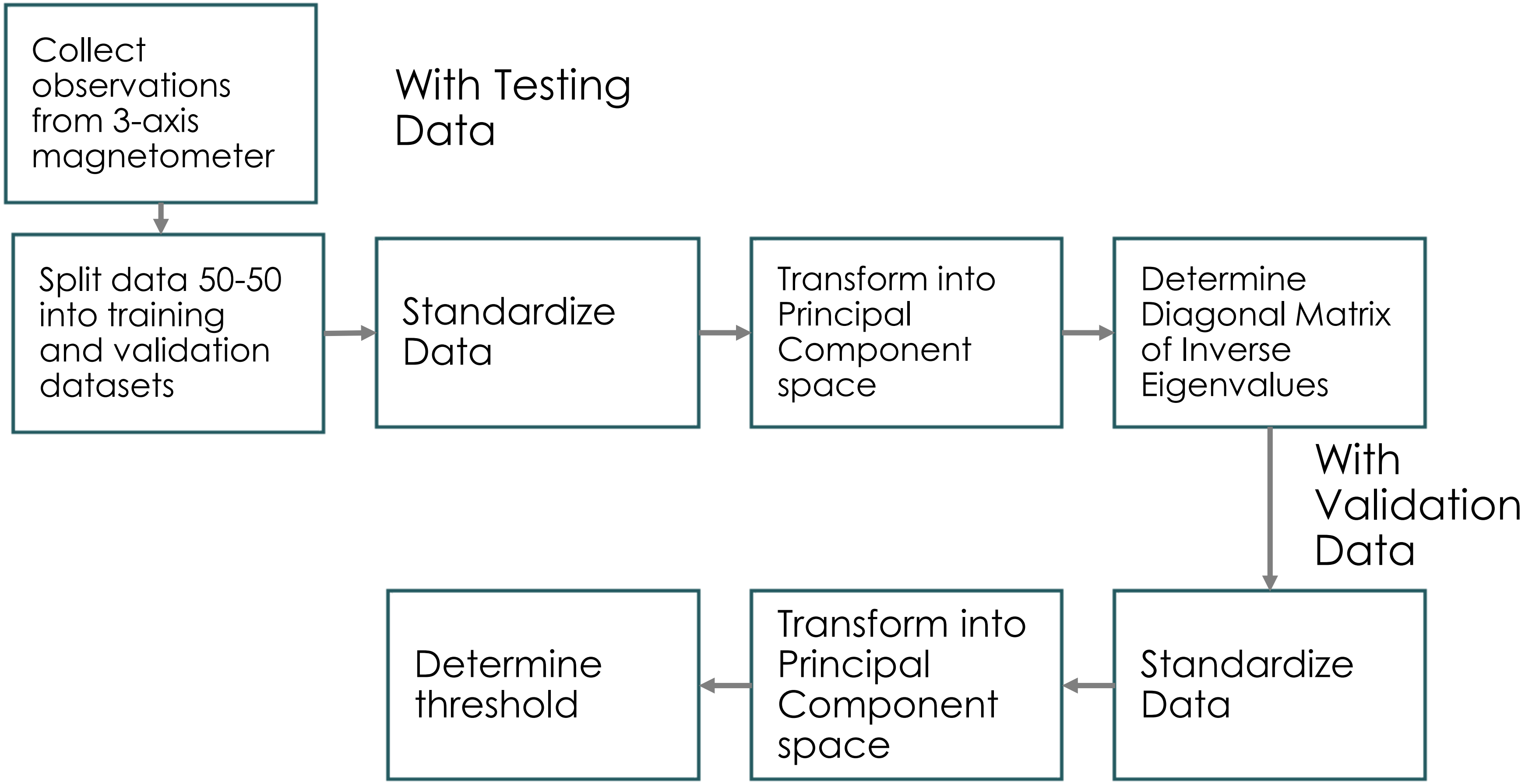
- Once in PCA space, the Hotelling's T^2 statistical test can be used to test how far an observation is from the center of the PC model
  - "Normal" data should be clustered near other "normal" data in PC space
  - Anomalies will be further away from the normal data
- Figure shows observations on the x-axis and the calculated T^2 statistic on the y-axis
- Green line is "ground truth" where a high value indicates that the tag is being removed from the metal sheet it is attached to

Anomaly Detection Method – T^2 Threshold

- The validation data set was used to draw a threshold where 95% of the validation data set values were accepted as “normal”
- This is shown in the figure to the right
- For operations:
  - An anomaly would be indicated if a certain percentage of data were over the threshold within a set time window
  - Thresholds could be adjusted to achieve desired true to false positive alarm rates



Operational Anomaly Detection Workflow – On Deployment



Collect observations from 3-axis magnetometer

With Testing Data

Split data 50-50 into training and validation datasets

Standardize Data

Transform into Principal Component space

Determine Diagonal Matrix of Inverse Eigenvalues

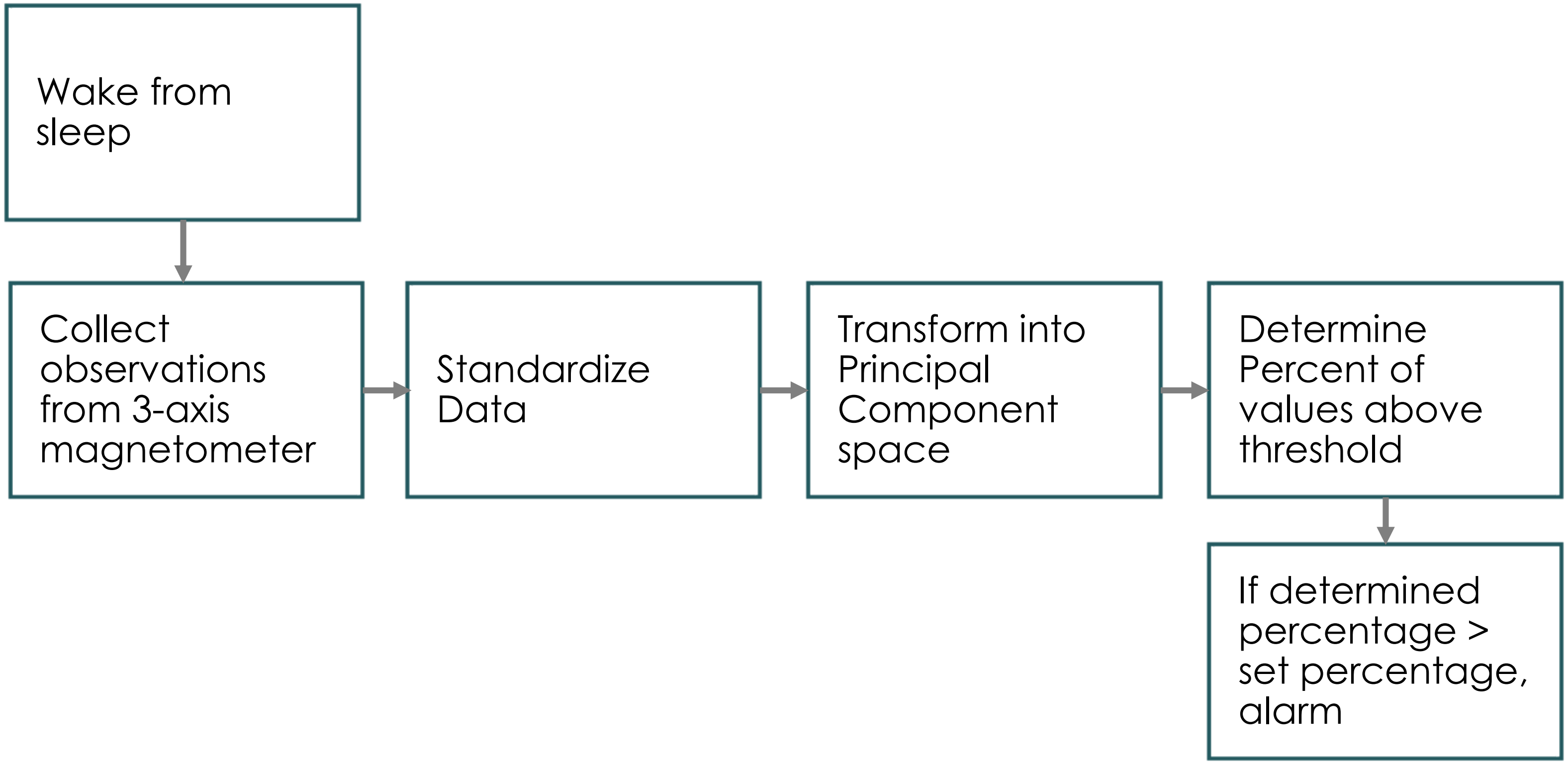
With Validation Data

Standardize Data

Transform into Principal Component space

Determine threshold

Operational Anomaly Detection Workflow – Monitoring


Wake from sleep
Collect observations from 3-axis magnetometer
Standardize Data
Transform into Principal Component space
Determine Percent of values above threshold
If determined percentage > set percentage, alarm

Conclusion

- ACTS is a unique universal platform that can be tailored to a variety of package tracking applications
- Can support a variety of communications, location services, and containment monitoring needs
- An ACTS data security peripheral would allow data acquired by ACTS sensors to be digitally signed
- The IR-UWB peripheral enables two-way ranging for locating ACTS tags in 2D or 3D space to facilitate an inventory or to detect the repositioning or movement of ACTS tagged items.
- ACTS can use an anomaly detection approach common to machine learning using data from an internal three-axis magnetometer to determine if the tag has been removed from a metal container.