Smart Sensor Network and Sensor-RFID Standards for Supply Chain

ANSI Homeland Security Standards Panel
9th Annual Plenary Meeting
Arlington, Virginia

November 9-10, 2010

Kang Lee
kang.lee@nist.gov
Intelligent Systems Division
Engineering Laboratory
National Institute of Standards and Technology
Sensors are Ubiquitous

Net-centric

Wireless

Security

Web access
**Vision:** anyone will be able to access any device and information seamlessly anywhere in the world with a handheld device in an affordable manner.

**Rational:** The world is moving toward smart devices, such as smart TV, smart phones, smart appliance, smart cars, internet, GPS, RFID, etc., - someday, everything is going to be connected to one another achieving – **Internet of Things.**

**Need:**
- better & compact security protocols,
- address privacy problem,
- more computing power
- robust hardware & software,
- common communication interfaces between devices and systems
- Common interfaces from devices to people,
- lower cost, etc.
What is a smart sensor?

But first - what is a sensor?

Basically a sensor is a device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument.
A Representation of a Smart Sensor

Network

Wired or Wireless Network Communication

Smart Sensor

Signal conversion, signal processing, data fusion, etc

Sensors
Key Features of Smart Transducers (Sensors or Actuators)

- Self-identification and self-description
- Self-calibration
- Time-aware
- Location-aware
- Intelligence (e.g. signal processing, data fusion, event notification, etc.)
- Ease of measurement - output in terms of physical units (e.g. Pascal, Kelvin)
- Standard-based wired or wireless communications
- Enable ease of connection to systems by simply plug and play, hence minimize human intervention
IEEE 1451 Standard
Smart Transducer System Approach

Physical Connection of Sensors

Sensor Node (TIM)
- XDCR
- ADC
- DAC
- D I/O
- Processor

Transducer Electronic Data Sheet (TEDS)

Network Node (NCAP)
- 1451.0 Common Command Set
- 1451.1 Smart Transducer Object Model

Network Connection of Sensors
- Wired or wireless Interface
- Any Network

Physical parameters to be measured
A mix of up to 255 sensors & actuators in a node

XDCR = sensor or actuator

-- items standardized
Sensor ID

Transducer Electronic Data Sheets (TEDS)

TEDS, a memory device attached to the transducer in a sensor node, stores Metadata, transducer identification, measurement range, calibration, correction data, user and manufacture-related information, which can be used for sensor self-identification and description.

Different TEDS are defined:

- Meta-TEDS
- Transducer Channel TEDS
- Physical TEDS
- Calibration TEDS
- Frequency Response TEDS
- Manufacturer-defined TEDS
- End User Application Specific TEDS
- Geo-location TEDS
- and more....
Sensor ID (identification)

Via IEEE 64-bit Global Identifier (EUI-64)

For IEEE 1451.X Standards (for digital sensors)
24-bit Organization ID

<table>
<thead>
<tr>
<th>Company ID – OUI-24</th>
<th>Extension Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 bits</td>
<td>40 bits</td>
</tr>
</tbody>
</table>

For IEEE 1451.4 Manufacturer ID (for analog sensors)

<table>
<thead>
<tr>
<th>Manufacturer ID</th>
<th>Model Number</th>
<th>Version Letter</th>
<th>Version Number</th>
<th>Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 bits</td>
<td>15 bits</td>
<td>5 bits (A-Z)</td>
<td>6 bits</td>
<td>24 bits</td>
</tr>
</tbody>
</table>

36-bit Organization ID

<table>
<thead>
<tr>
<th>Company ID – OUI-36</th>
<th>Extension Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>36 bits</td>
<td>28 bits</td>
</tr>
</tbody>
</table>
IEEE 64-bit Global Identifier (EUI-64)

The 64-bit global identifier EUI-64 (extended unique identifier-64) is a combination of a company_id and the extended identifier. The company_id represented in OUI-24 or OUI-36 (organizational unique identifier) is assigned by the IEEE Registration Authority. The extended identifier is assigned by the manufacturer.

For example: assume that a manufacturer's IEEE-assigned OUI-24 company_id value is ACDE48_{16} and the manufacturer-selected extension identifier for a given component is 234567ABCD_{16}. The EUI-64 value generated from these two numbers is ACDE48234567ABCD_{16}.

<table>
<thead>
<tr>
<th>company_id</th>
<th>extension identifier</th>
<th>field</th>
</tr>
</thead>
<tbody>
<tr>
<td>addr+0</td>
<td>addr+1</td>
<td>addr+2</td>
</tr>
<tr>
<td>AC</td>
<td>DE</td>
<td>48</td>
</tr>
<tr>
<td>10101100</td>
<td>11011110 01001000 00100011 01000101 01100111 10101011 11001101 bits</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>most significant byte</td>
<td>least significant byte</td>
<td>least-significant bit</td>
</tr>
</tbody>
</table>

For example: assume that a manufacturer's IEEE-assigned OUI-36 company_id value is 8765432AB_{16}, and the manufacturer-selected extension identifier for a given component is 567ABCD_{16}. The EUI-64 value generated from these two numbers is 8765432AB567ABCD_{16}.

<table>
<thead>
<tr>
<th>company_id</th>
<th>extension identifier</th>
<th>field</th>
</tr>
</thead>
<tbody>
<tr>
<td>addr+0</td>
<td>addr+1</td>
<td>addr+2</td>
</tr>
<tr>
<td>87</td>
<td>65</td>
<td>43</td>
</tr>
<tr>
<td>10000111 0110101 01000101 01000111 01010101 1011 0101 01100111 10101011 11001101 bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>most significant byte</td>
<td>least significant byte</td>
<td>least-significant bit</td>
</tr>
</tbody>
</table>

http://standards.ieee.org/regauth/oui/t
ISO/IEC and IEEE Collaboration

Through the ISO and IEEE Partner Standards Development Organization (PSDO) Agreement, IEEE 1451.X family of standards were adopted as ISO/IEC/IEEE 21451 standards:

– ISO/IEC/IEEE 21450
– ISO/IEC/IEEE 21451-1
– ISO/IEC/IEEE 21451-4
– ISO/IEC/IEEE 21451-7
ISO/IEC/IEEE Sensor Standards

Network

- 21451-1
  - 21450
  - NCAP

- 21451-1
  - 21450
  - NCAP/TIM or Instrument

- 21451-1
  - 21450
  - NCAP

- 21451-1
  - 21450
  - NCAP/TIM

Wireless Protocols
- 8802-11 (WiFi)
- 8802-15-1 (Bluetooth)
- 8802-15-4 (ZigBee)
- 8802-15-4 (6LoWPAN)
- Proposed 3G/4G/WiMax/LTE

Wireless Protocols
- 18000 (RFID Air Interface)
- 24730 (RTLS)

Point-to-Point

21451-4
- MMX

Digital TEDS

21451-4
- MMX

Analog Signals

21451-4
- MMX

= Sensor / Actuator / TEDS

= Wireless

= Sensor + RFID
A Basic RFID System

Consisting of Tags, Readers, and IT infrastructure

Tag = chip + antenna

Tag returns unique ID code

Plus sensor data

Detailed product information from secure web-accessible databases via a network

Tag reader or Interrogator or Wireless node

IEEE 1451.7 Standard

Commands & responses

Sensor Data
Integration of Sensors and RFID Creates Unique Business Opportunities

**Rationale:** In manufacturing, production, and supply chain systems,

- RFID tag tells what a product is, but does not tell what condition it has been gone through throughout its life cycle.
- Sensors can monitor and report the product’s condition by measuring temperature, vibration, presence of chemical and other parameters.
- Combining tags and sensors could expand the overall functionality and capability of the RFID systems.
- Networking RFID systems can realize the same benefits of wireless sensor mesh networks.
- Universal RFID and sensor standards ensure interoperability and enable successful RFID adoption and deployment worldwide,

  e.g., ease the processing of secure cargo containers shipped worldwide.
RFID Systems in Supply Chain

Supply Chain Automation with RFID

1. Add tag to each can of cola
2. Cans in cases; each case and palette is tagged.
3. Reader powers up tags as they cross dock.
4. Tags power up, send EPC's one by one.
5. Reader talks to Savant, queries ONS server; EPC matched to remote database entry.
6. Distribution center reads palette contents
7. Cola boxes routed to SpeedyMart, inventory updated.
8. Smart shelves track display inventory in real time to initiate restocking.
10. Fridge reader tracks cola supply
11. Tags enable automatic sorting at recycle.

Remote server uses PML to store description of product for each EPC.

Source: EPCglobal
Sensor networks integrated with RFID systems for product condition monitoring and asset tracking in Supply Chain

Supply Chain Automation with RFID

1. Add tag to each can of cola
2. Cans in cases; each case and palette is tagged.
3. Reader powers up tags as they cross dock.
4. Tags power up, send EPC’s one by one.
5. Reader talks to Savant, queries ONS server; EPC matched to remote database entry.
6. Distribution center reads palette contents
7. Cola boxes routed to SpeedyMart, inventory updated.
8. Smart shelves track display inventory in real time to initiate restocking.
10. Fridge reader tracks cola supply
11. Tags enable automatic sorting at recycle.

Add sensors to RFID with Standardized sensor interfaces

Source: EPCglobal
• **Air Interface Security** -
  provides methods for the sensor to take advantage of the security built into a particular RFID air interface.
  ✓ the tag passing a security status code to the sensor informing the sensor of the security state of the tag.
  ✓ the sensor then appropriately limits its command execution according to a security function code programmed by the user.

• **Direct Sensor Security** -
  provides choices for sensor security:
  ✓ a simple password system for reader-only authentication
  ✓ encrypted two-way authentication of reader and sensor
  ✓ authentication of reader and sensor on each command/response exchange
  ✓ encryption of data flow in the link
### 21451.7 Prim. Sensor Characteristics (TEDS Type 1)

<table>
<thead>
<tr>
<th>Field</th>
<th>Name</th>
<th>Size</th>
<th>Example/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TEDS type</td>
<td>3 bits</td>
<td>001&lt;sub&gt;2&lt;/sub&gt;</td>
</tr>
<tr>
<td>2</td>
<td>Sensor Type</td>
<td>7 bits</td>
<td>0001110&lt;sub&gt;2&lt;/sub&gt; = Relative Humidity</td>
</tr>
<tr>
<td>3</td>
<td>Units extension</td>
<td>5 bits</td>
<td>Sub-type, e.g., for chemical sensors</td>
</tr>
<tr>
<td>4</td>
<td>Sensor map</td>
<td>16 bits</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Data resolution</td>
<td>5 bits</td>
<td>Sensor capability</td>
</tr>
<tr>
<td>6</td>
<td>Scale Factor Significand</td>
<td>11 bits</td>
<td>Sensor capability</td>
</tr>
<tr>
<td>7</td>
<td>Scale Factor Exponent</td>
<td>6 bits</td>
<td>Sensor capability</td>
</tr>
<tr>
<td>8</td>
<td>Scale Offset Significand</td>
<td>11 bits</td>
<td>Sensor capability</td>
</tr>
<tr>
<td>9</td>
<td>Scale Offset Exponent</td>
<td>6 bits</td>
<td>Sensor capability</td>
</tr>
<tr>
<td>10</td>
<td>Data uncertainty</td>
<td>3 bits</td>
<td>Sensor capability</td>
</tr>
<tr>
<td>11</td>
<td>Sensor Reconfiguration Capability</td>
<td>1 bit</td>
<td>0 = NO 1 = YES</td>
</tr>
<tr>
<td>12</td>
<td>Memory Rollover Capability</td>
<td>1 bit</td>
<td>0 = NO 1 = YES</td>
</tr>
<tr>
<td>13</td>
<td>Air Interface Security Capability Code</td>
<td>3 bits</td>
<td>See Table 5 for details.</td>
</tr>
<tr>
<td>14</td>
<td>Sensor Security Capability Code (Note 1)</td>
<td>3 bits</td>
<td>See Table 5 for details.</td>
</tr>
</tbody>
</table>

#### Note 1:
If the air interface and sensor security systems are both supported and if Security Function Codes based on the capability codes are programmed to different levels, then the more secure mode shall apply to how the sensor processes commands.
<table>
<thead>
<tr>
<th>Field</th>
<th>Name</th>
<th>Size</th>
<th>Example/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Sensor Authentication Encryption Capability Map</td>
<td>7 bits</td>
<td>Choices of encryption algorithms for authentication that the sensor supports. If all zeroes then encrypted authentication is not supported.</td>
</tr>
<tr>
<td>16</td>
<td>Sensor Data Encryption Capability Map</td>
<td>7 bits</td>
<td>Choices of encryption algorithms for data that the sensor supports. If all bits are zero then data encryption is not supported. If data encryption is supported, the directions supported are detailed in the Data Encryption Capability field of this table.</td>
</tr>
<tr>
<td>17</td>
<td>Sensor Authentication Password/Key Size (Note 2)</td>
<td>3 bits</td>
<td>000_2=16 bits, 001_2=32 bits, 010_2=64 bits, 011_2=128 bits, 100_2~111_2 = RFU</td>
</tr>
<tr>
<td>18</td>
<td>Sensor Data Encryption Key Size (See Note 3)</td>
<td>3 bits</td>
<td>000_2=16 bits, 001_2=32 bits, 010_2=64 bits, 011_2=128 bits, 100_2~111_2 = RFU</td>
</tr>
<tr>
<td>19</td>
<td>Random Number Sizes Supported (See Note 4)</td>
<td>3 bits</td>
<td>000_2 = 16 bits, 001_2 = 16 &amp; 32 bits, 010_2 = 16, 32 &amp; 64 bits, 011_2 = 16, 32, 64, &amp; 128 bits, 100_2~111_2 = RFU</td>
</tr>
</tbody>
</table>

**Note 2:** For sensor authentication the term “password/key” is used instead of simply “key” because this field functions as a key if the sensor has authentication encryption but as a password if it does not. Though sensor authentication password/key sizes are 16 bits and greater, if Sensor Security Capability Code is 000, then there is no password or key and this overrides the password/key length field. It is possible via the Sensor Authentication Encryption Capability Map to select a standardized encryption algorithm with a key length that overrides the key length field. The key length field is to allow algorithms that support multiple key lengths to specify the particular length the tag uses. For example, AES can have key lengths of 128, 192, and 256 bits (though only 128 is specified for this standard version).

**Note 3:** Though sensor data encryption key sizes are 16 bits and greater, if Sensor Security Capability Code is 000, then there is no key and this overrides the key length field. It is possible via the Sensor Data Encryption Capability Map to select a standardized encryption algorithm with a key length that overrides the key length field.

**Note 4:** A random number generator is needed to support authentication, which it does by providing a continuously changing number to encrypt into a security token that proves the key is possessed. The supported random number sizes in this version are all or a subset of 16, 32, 64, and 128. Though the random number size is 16 bits and greater, if Sensor Encryption Capability Code is 000, then there is no random number generator and this overrides the Random Number Size field. The actual random number sizes to be used by each side of the link are provided by the Challenge command for the initial authentication, and by the Reader-Authenticate command for Continuing Authentication. See next comment.
### Field 20
**Continuing Authentication Capability field** (See Note 5)
- **Size**: 2 bit
- **Example/Note**: See Table 9 for details.

### Field 21
**Data Encryption Capability field**
- **Size**: 2 bit
- **Example/Note**: Table 10 for details.

### Field 22
**Clock Accuracy** (See Note 6)
- **Size**: 3 bits
- **Example**:
  - 00: >10%
  - 001: 10%
  - 010: 5%
  - 011: 2%
  - 100: 1%
  - 101: 300 ppm
  - 110: 100 ppm
  - 111: <100 ppm

**Note 5**: Continuing Authentication is an optional ability to authenticate all commands and responses individually, as opposed to a single authentication where it is assumed that following authentication commands are not subject to hostile action.

**Note 6**: Clock accuracy applies to logged data, and if supported then also to the Secure Session Timer of Table 16. The range of values shown are suitable for the two main classes of reference sources, which are free running relaxation (RC) oscillators (trimmed and untrimmed) and low cost low power crystal timers (such as standard 32.768 kHz watch crystal based Real Time Clocks). The manufacturer shall permanently lock the Primary Sensor Characteristics TEDS.
Enabling Technology for Web-based Online Sensor Monitoring, Diagnostic, and Control.

Ethernet node + web server

Sensor with 1451 Interface

The Java-based remote monitoring and control applet
IEEE 1451 Applications

- IEEE 1451.4 “Plug and Play” interface built into LabView.
- IEEE 1451.2 in health monitoring of oil pipeline.
- IEEE 1451 in naval vessels for CBM.
Sensor and RFID Standards for:

A fire chief can use handheld PDA or remote mobile station based on IEEE 1451 wired and wireless sensor networks to monitor the condition of the first responders and their operating environment to help make decision ensuring the safety of the fire fighters.

Port authority can monitor the condition of the shipping containers with smart sensors based on IEEE 1451 smart sensor standards and technologies. (smart containers)
IEEE 1451 & OGC-SWE Integration

SOS Client

SOS O&M, Sensor ML, TML

STWS Client

STWS

OGC Data Specifications: O&M, SensorML, TML

1 & 2) IEEE-1451 TIM

3) Legacy/Proprietary

4) SWE Onboard

O&M, Sensor ML, TML

STWS

Courtesy Open Geospatial Consortium
Diverse sensors, some in IEEE 1451 configurations, are discoverable and Web-accessible via SWE interfaces, in diverse architectures and applications, with geospatial context.

**OGC SWE & IEEE 1451 Converged in Ocean Applications**

Sensor Web Enablement services (and “cloud” resources)

**IEEE 1451**
- IEEE 1451 Sensor Networks
- Sensors/TIM/NCAP/STWS

**Legacy custom/proprietary**

**SWE “direct”**

- Stored Vector Feature Data
- Any sensor system

Ongoing efforts are to harmonize and converge OGC SWE and IEEE 1451 as highlighted in several ongoing testbeds (including the Ocean and Earth assets)

**Courtesy Open Geospatial Consortium**
Network and Internet Access of ISO/IEC/IEEE 21451 Sensors

XML response message

XML request message

Smart Transducer
Web Services

HTTP Protocol
IP

21451 Network node

IEEE sensor interfaces:
21451.2 pt-to-pt
21451.5 wireless

21451.X PHY layer

TEDS

21451.X PHY TEDS

Sensor

Sensor

Actuator

21451 Sensor node
Ocean Application Demo Setup

Common interfaces were used for connectivity

STWS Messages with OGC SOS

Ocean Monitoring (OGC, St. John)

STWS (NIST, USA)

IEEE 1451 NCAPs

NCAP (MBARI, USA)

HTTP Server

IEEE 1451.0 HTTP

NCAP (Breman, Germany)

HTTP Server

NCAP (Barcelona, Spain, ESONET)

HTTP Server

NCAP (Kiel, Germany)

Ocean Instruments

HTTP Server

Ocean Weather Station

Seabird CTD

Triplet

XR-420 CTD

Seabird CTD

Triplet

Seabird CTD

Seabird CTD

Ocean Weather Station

Ocean Weather Station

- Sensor Alert Web Service (SAWS) Consumer
  - Sensor Alert Notification Consumer Service (SANCS)
  - Sensor Alert Notification Producer Service Client
- Sensor Alert Web Service (SAWS) Producer
  - Sensor Alert Notification Producer Service (SANPS)
  - Sensor Alert Notification Consumer Service Client
- Smart Transducer Web Services Client
- Smart Transducer Web Services (STWS)
- IEEE 1451.0 Transducer Services
  - IEEE 1451.X Communication Module
- IEEE 1451.X PHY
  - IEEE 1451.X Transducer Services
  - 1451.0 TEDS
  - 1451.X TEDS
- Signal Conditioning
  - A/D, D/A Data Conversion
- Sensor Alert Web Service Consumer
  - NCAP (Sensor Alert Web Service Provider)
- Transducer Interface Module (TIM)
Other Sensor Standards Activities

- ISO/IEC /JTC1/WG7, Working Group on Sensor Networks was created. It focuses on sensor network application aspects. It plans to adopt or harmonize existing and relevant sensor network standards, and create standards to fill the gaps.

- ISO TC122/WG10 develops standards for supply chain and RFID communication tags.

- ISO TC104/SC4/WG2 develops standard for shipping container communication tags.

- Sensor Standards Harmonization Working Group (SSHWG) facilitated by NIST for DHS S&T Standards Office.
Objectives of SSHWG

- Provide a forum for industry, academia, and government to exchange information and improve understanding of the various sensor-related standards programs being advanced by various standards development organizations (SDO).
- Identify opportunities to frame the harmonization of sensor-related standards to meet the need of the community,
  - Standards Harmonization will enable the standards to work together to promote multi-level sensor data, information, and application interoperability.
- Provide opportunities for collaborative demonstration of standards implementation.
- Make recommendation of sensor standards to DHS to help achieve sensor devices, data, and information interoperability.
Cargo Container Security

Enabling Standards

- TC 204 - ISO 26683 - Freight conveyance content identification & comm.
- TC 104 - ISO 18186 - RFID cargo shipment tag system
- TC 122
  - ISO 17363 – Supply chain applications of RFID – Freight containers
  - ISO 21451 – Sensor / RFID Standards
In Summary

- Smart and wireless sensor networks will change the ways sensors are used worldwide.
- Standardized sensor network interfaces are needed and exist to facilitate interoperability.
- Smart and wireless sensor and sensor integrated RFID standards can benefit:
  - Cargo container security
  - Supply chain security, e.g. cold chain
- Need to continue the harmonization of national and international sensor and related standards to foster worldwide interoperability and information sharing.
THANK YOU FOR YOUR ATTENTION

Questions?