Smart Sensor Network and Sensor-RFID Standards for Supply Chain

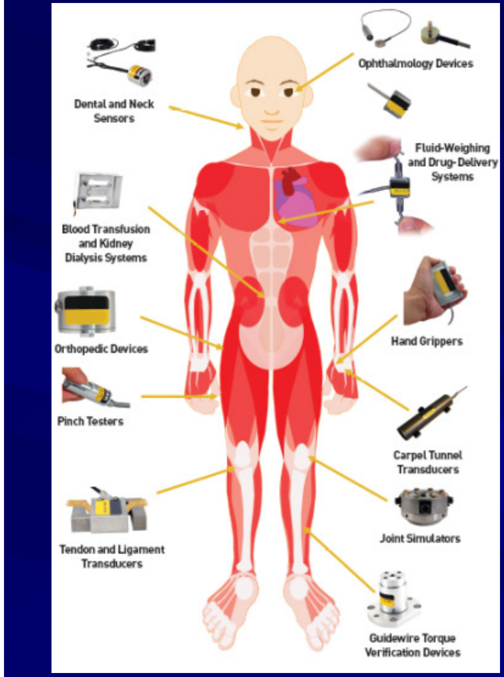
ANSI Homeland Security Standards Panel
9th Annual Plenary Meeting
Arlington, Virginia

November 9-10, 2010

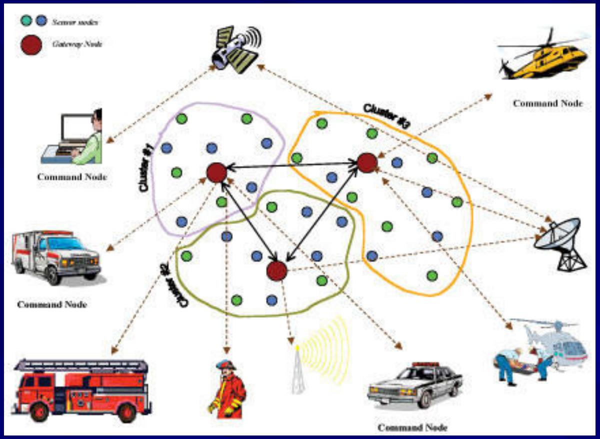
Kang Lee
kang.lee@nist.gov
Intelligent Systems Division
Engineering Laboratory
National Institute of Standards and Technology

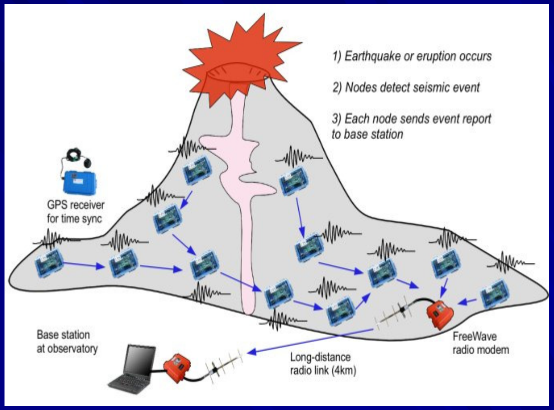
NIST National Institute of Standards and Technology

Sensors are Ubiquitous



Ophthalmology Devices
Dental and Neck Sensors
Fluid-Weighing and Drug-Delivery Systems
Blood Transfusion and Kidney Dialysis Systems
Hand Grippers
Orthopedic Devices
Pinch Testers
Carpel Tunnel Transducers
Joint Simulators
Tendon and Ligament Transducers
Guidewire Torque Verification Devices





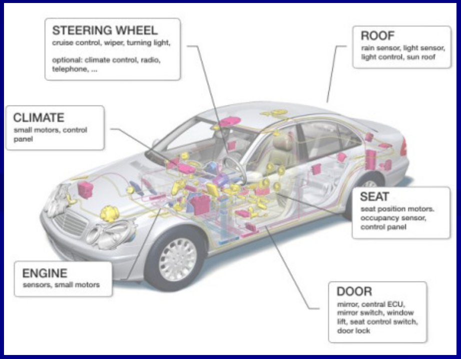
1) Earthquake or eruption occurs
2) Nodes detect seismic event
3) Each node sends event report to base station
GPS receiver for time sync
Base station at observatory
Long-distance radio link (4km)
FreeWave radio modem

Wireless

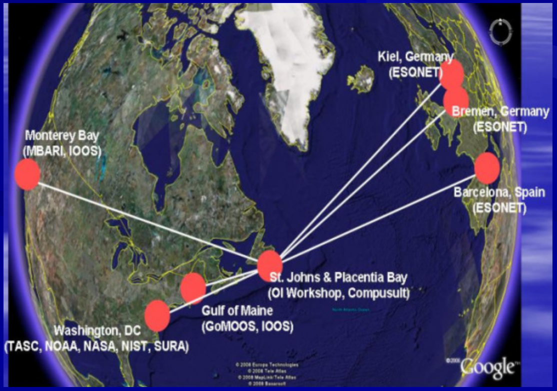
Net-centric

Security

Web access



STEERING WHEEL
cruise control, wiper, turning light,
optional: climate control, radio, telephone, ...
ROOF
rain sensor, light sensor, light control, sun roof
CLIMATE
small motors, control panel
SEAT
seat position motors. occupancy sensor, control panel
ENGINE
sensors, small motors
DOOR
mirror, central ECU, mirror switch, window lift, seat control switch, door lock



Kiel, Germany (ESONET)
Bremen, Germany (ESONET)
Monterey Bay (MBARI, IOOS)
Barcelona, Spain (ESONET)
St. Johns & Placentia Bay (OI Workshop, Compusult)
Gulf of Maine (GoMOOS, IOOS)
Washington, DC (TASC, NOAA, NASA, NIST, SURA)
Google

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

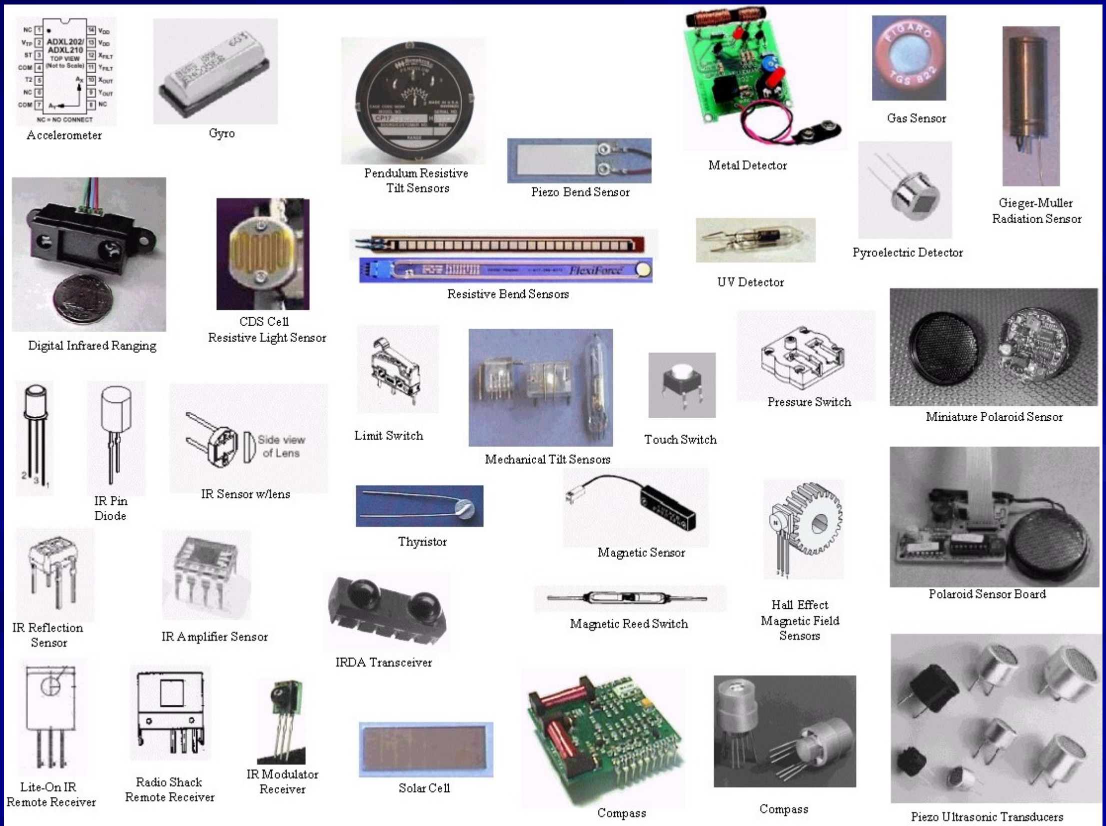
✓Common interfaces from devices to people,

✓lower cost, etc.

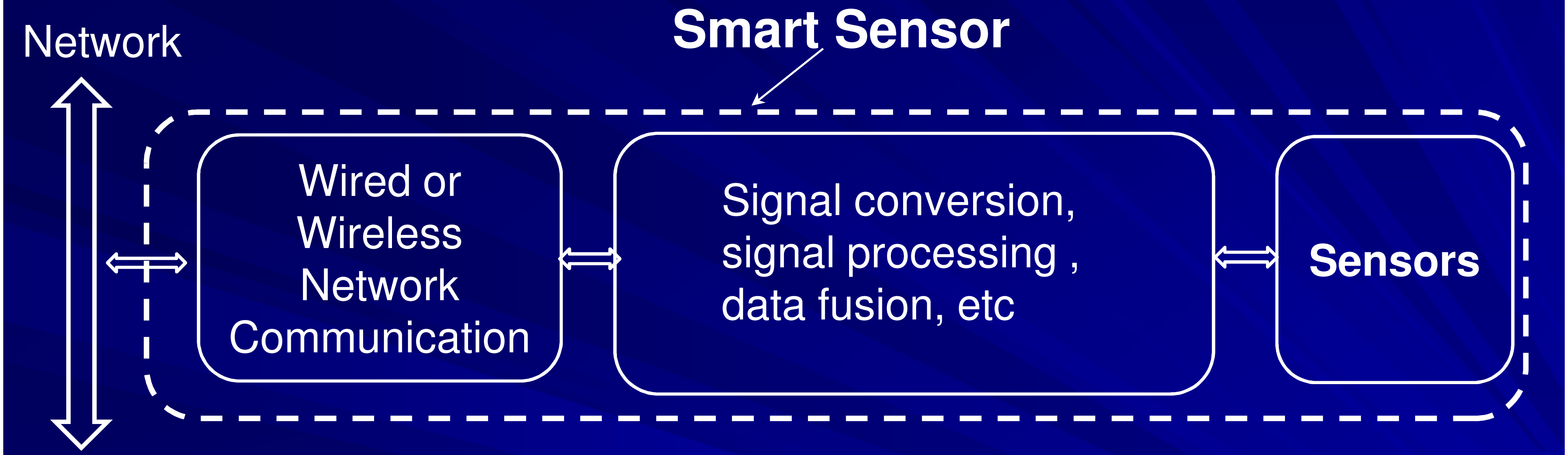
What is a smart sensor?

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

Smart Sensor

Wired or Wireless Network Communication

Signal conversion, signal processing , data fusion, etc

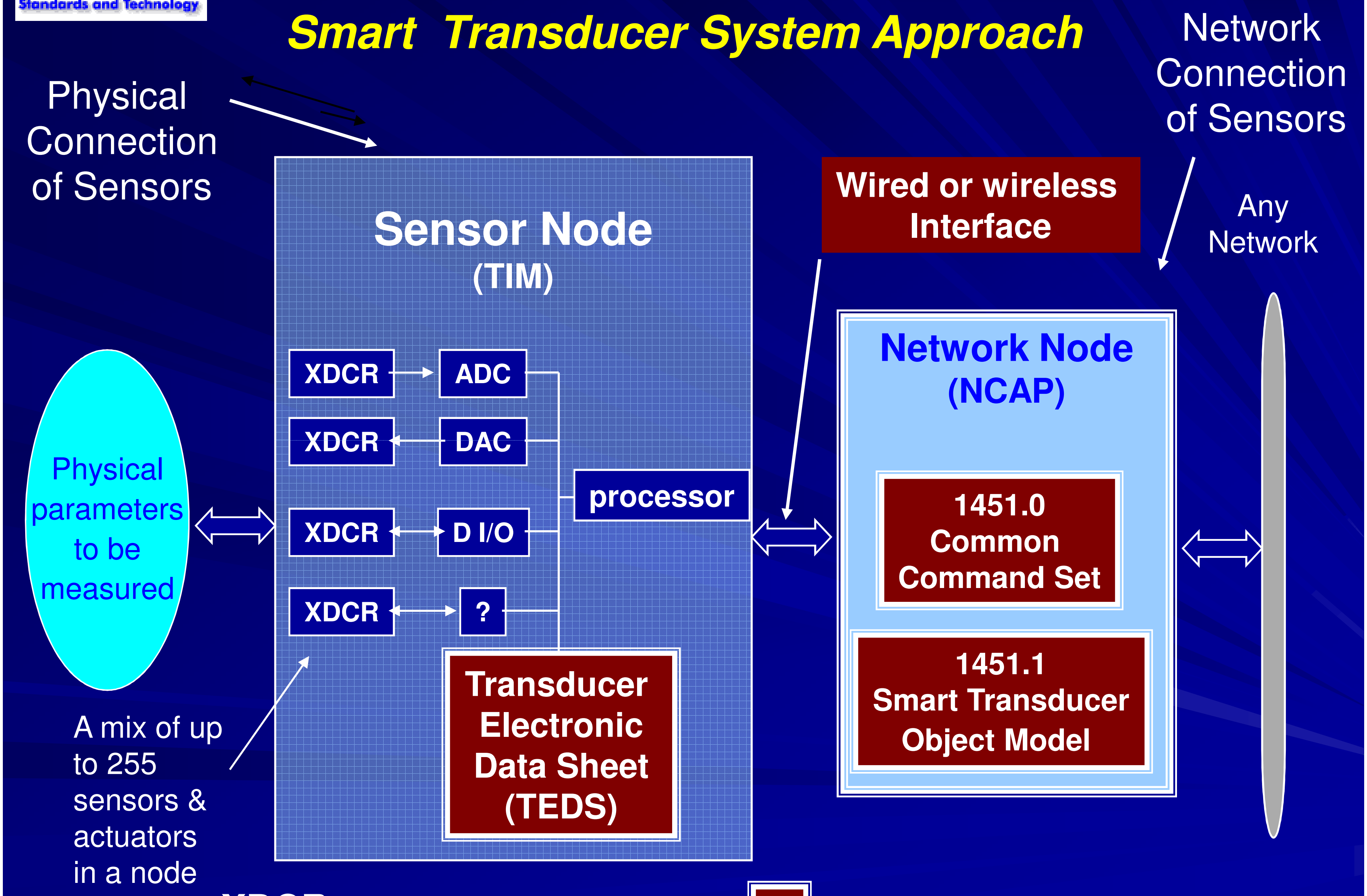
Sensors

NIST
National Institute of
Standards and Technology

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

Network Connection of Sensors

Sensor Node (TIM)

XDCR → ADC

XDCR ← DAC

XDCR ↔ D I/O

XDCR ↔ ?

processor

Transducer Electronic Data Sheet (TEDS)

Wired or wireless Interface

Network Node (NCAP)

1451.0 Common Command Set

1451.1 Smart Transducer Object Model

Any Network

Physical parameters to be measured

A mix of up to 255 sensors & actuators in a node

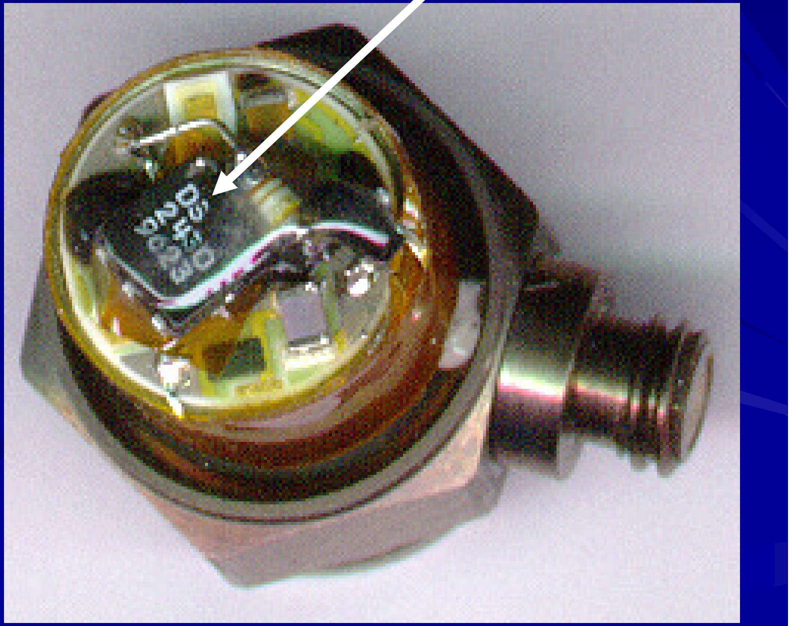
XDCR = sensor or actuator

🟥 **-- 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….



TEDS

Sensor ID (identification)

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

For 1EEE 1451.X Standards (for digital sensors)

24-bit Organization ID

Company ID – OUI-24	Extension Identifier
24 bits	40 bits

36-bit Organization ID

Company ID – OUI-36	Extension Identifier
36 bits	28 bits

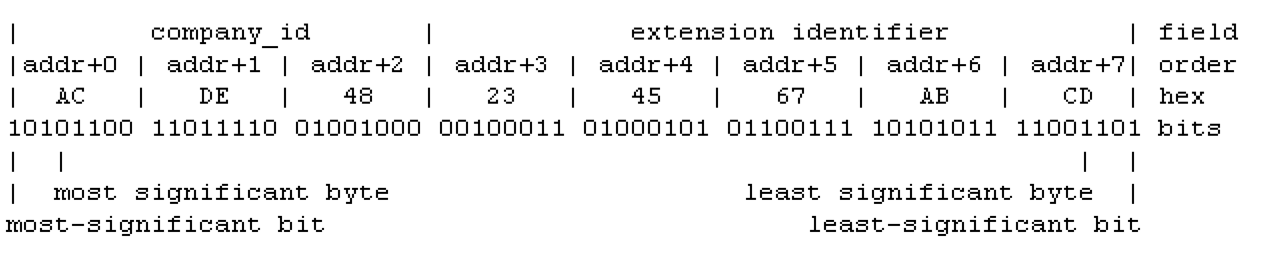
For IEEE 1451.4 Manufacturer ID (for analog sensors)

Manufacturer ID	Model Number	Version Letter	Version Number	Serial Number
14 bits	15 bits	5 bits (A-Z)	6 bits	24 bits

IEEE 64-bit Global Identifier (EUI-64)

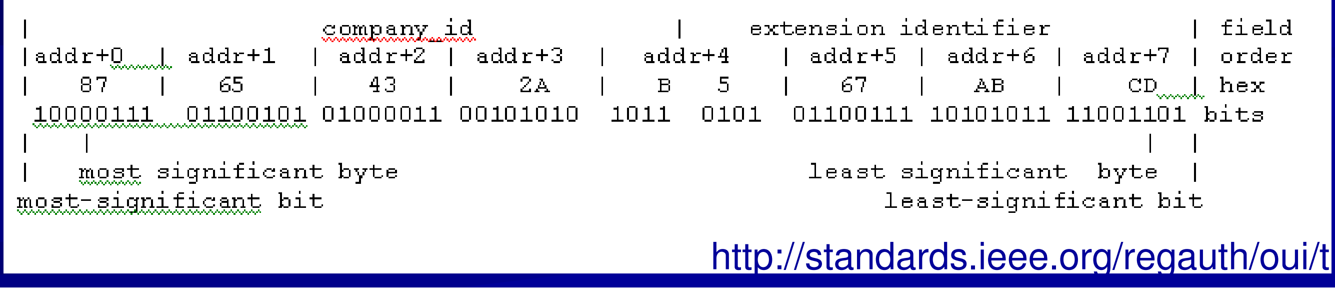
The 64-bit global identifier EUI-64 (extended unique identifier-64) is a combination of a *company_id* and the extended identifier. The *company_id* represented in OUI-24 or OUI-36 (organizational unique identifier) is assigned by the IEEE Registration Authority. The extended identifier is assigned by 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$_{16}$



```
|        company_id       |             extension identifier          | field
|addr+0 | addr+1 | addr+2 | addr+3 | addr+4 | addr+5 | addr+6 | addr+7| order
|  AC   |   DE   |   48   |   23   |   45   |   67   |   AB   |   CD  | hex
10101100 11011110 01001000 00100011 01000101 01100111 10101011 11001101 bits
|  |                                                                |  |
|  most significant byte                          least significant byte  |
most-significant bit                                       least-significant bit
```

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$_{16}$.



```
|                   company_id              |    extension identifier         | field
|addr+0   | addr+1    | addr+2 | addr+3    |    addr+4     | addr+5 | addr+6 | addr+7 | order
|   87    |   65      |   43   |     2A    |   B    5      |   67   |   AB   |    CD  | hex
 10000111  01100101 01000011 00101010  1011  0101  01100111 10101011 11001101 bits
|    |                                                                       |   |
|    most significant byte                               least significant  byte  |
most-significant bit                                          least-significant bit
```

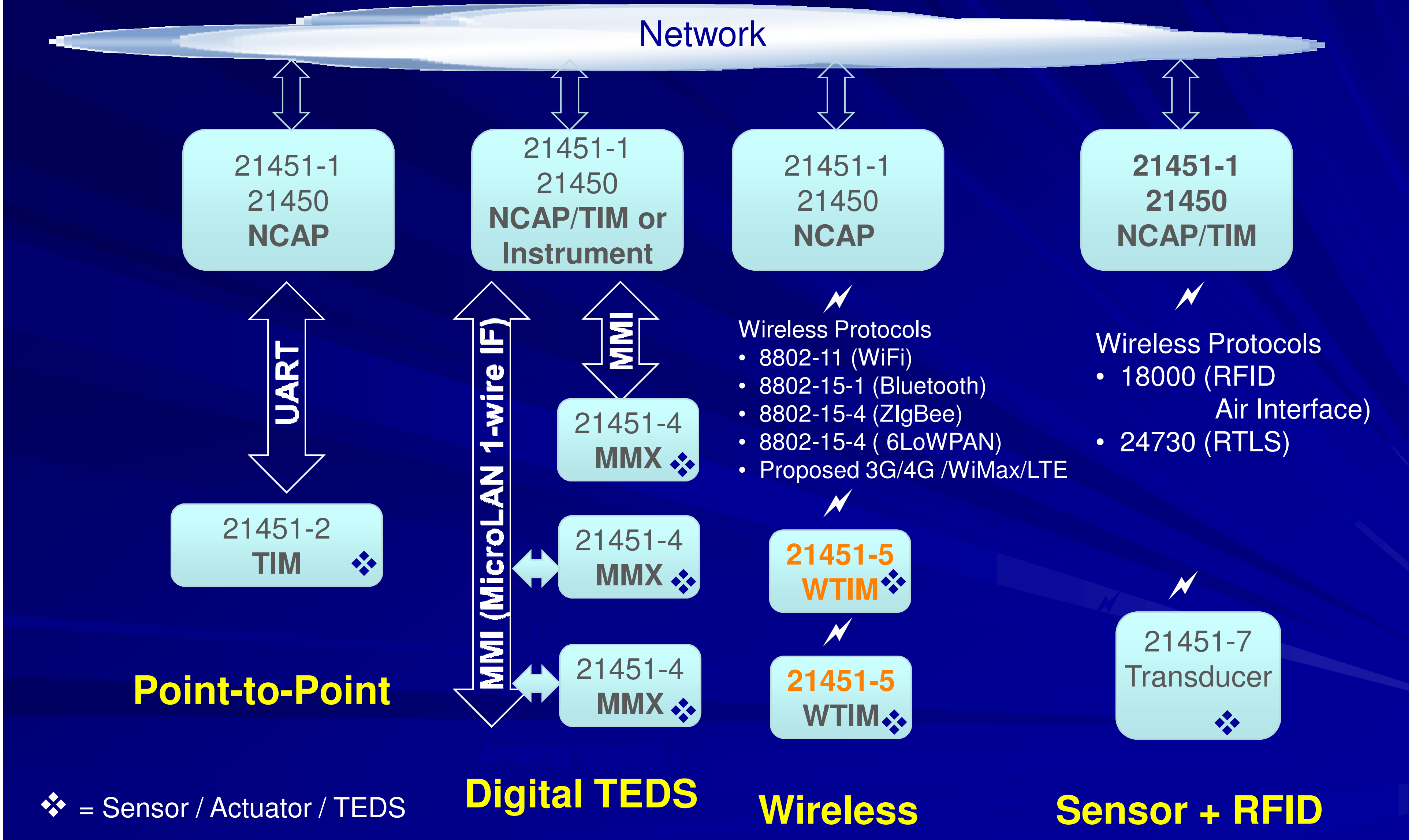
http://standards.ieee.org/regauth/oui/t

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 21451-2
  - ISO/IEC/IEEE 21451-4
  - ISO/IEC/IEEE 21451-5
  - ISO/IEC/IEEE 21451-7

NIST National Institute of Standards and Technology

ISO/IEC/IEEE Sensor Standards



Network

21451-1
21450
NCAP

UART

21451-2
TIM ❖

Point-to-Point

21451-1
21450
NCAP/TIM or
Instrument

MMI (MicroLAN 1-wire IF)

MMI

21451-4
MMX ❖

21451-4
MMX ❖

21451-4
MMX ❖

Digital TEDS

21451-1
21450
NCAP

Wireless Protocols

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

21451-5
WTIM ❖

21451-5
WTIM ❖

Wireless

21451-1
21450
NCAP/TIM

Wireless Protocols

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

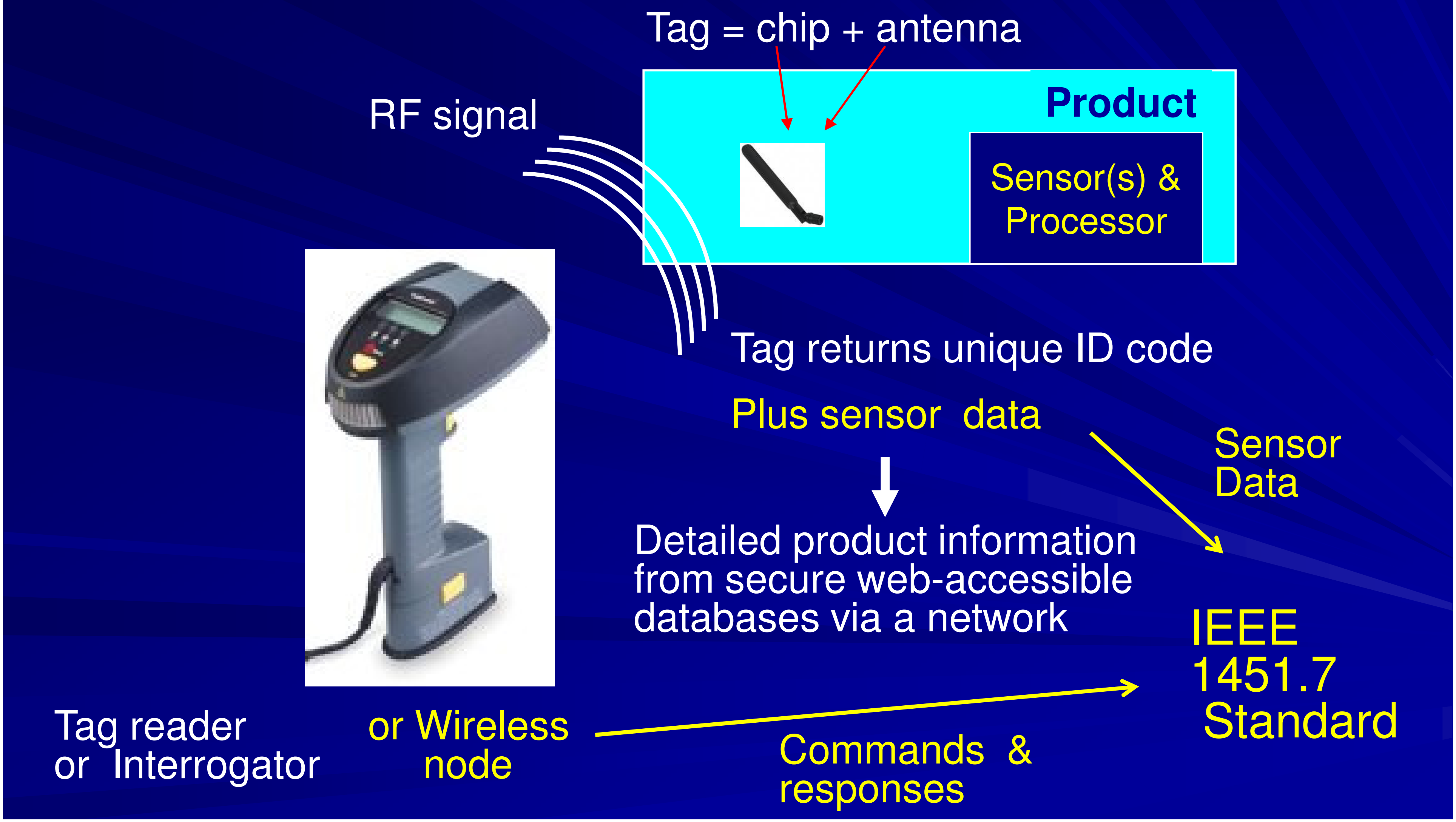
21451-7
Transducer
❖

Sensor + RFID

❖ = Sensor / Actuator / TEDS

A Basic RFID System

Consisting of Tags, Readers, and IT infrastructure



Tag = chip + antenna

RF signal

Product

Sensor(s) & Processor

Tag returns unique ID code

Plus sensor data

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

Sensor Data

IEEE 1451.7 Standard

Tag reader or Interrogator

or Wireless node

Commands & responses

NIST
National Institute of Standards and Technology

Integration of Sensors and RFID Creates Unique Business Opportunities

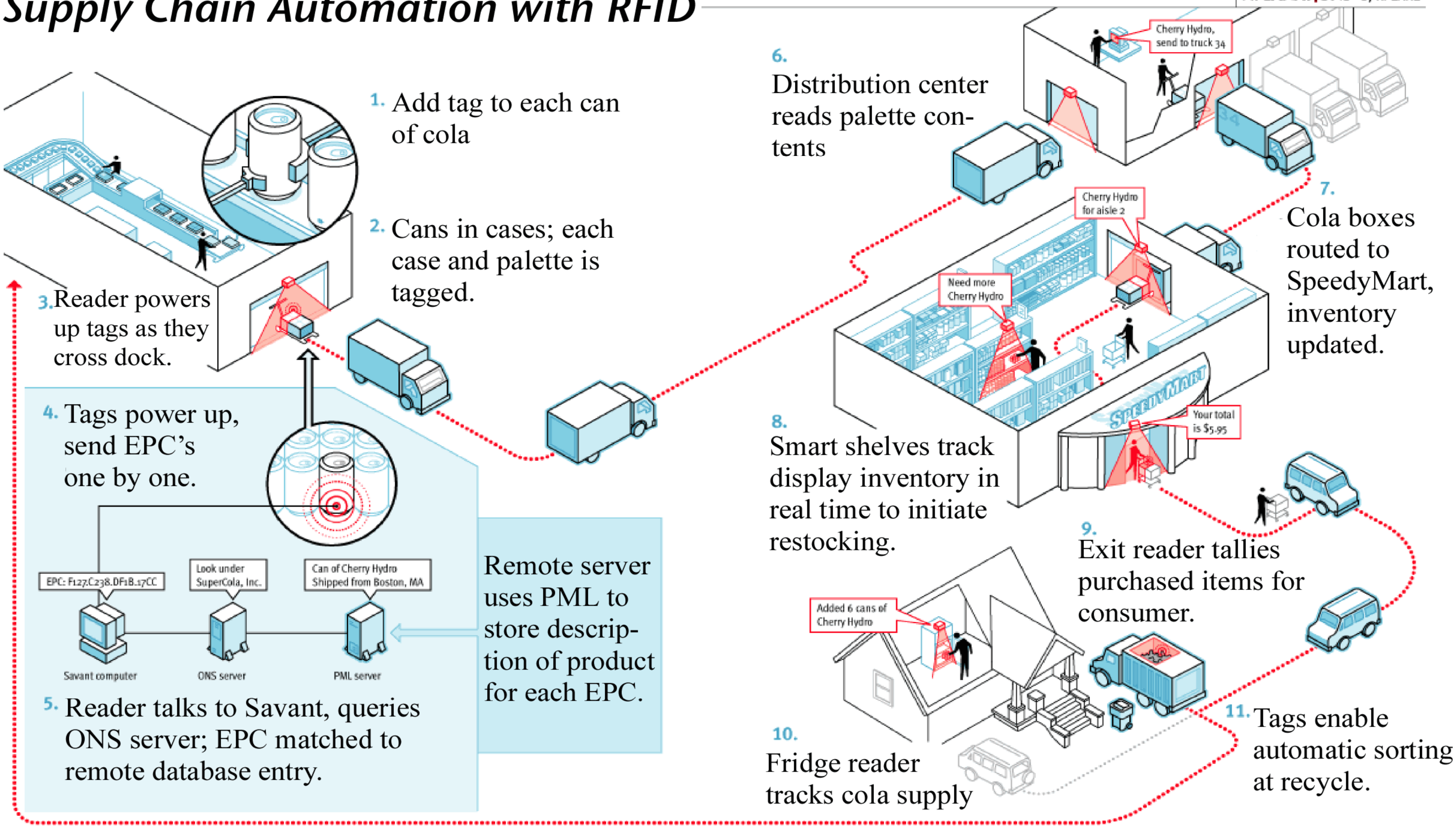
Rationale: In manufacturing, production, and supply chain systems,

- 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.

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

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.

9. Exit reader tallies purchased items for consumer.

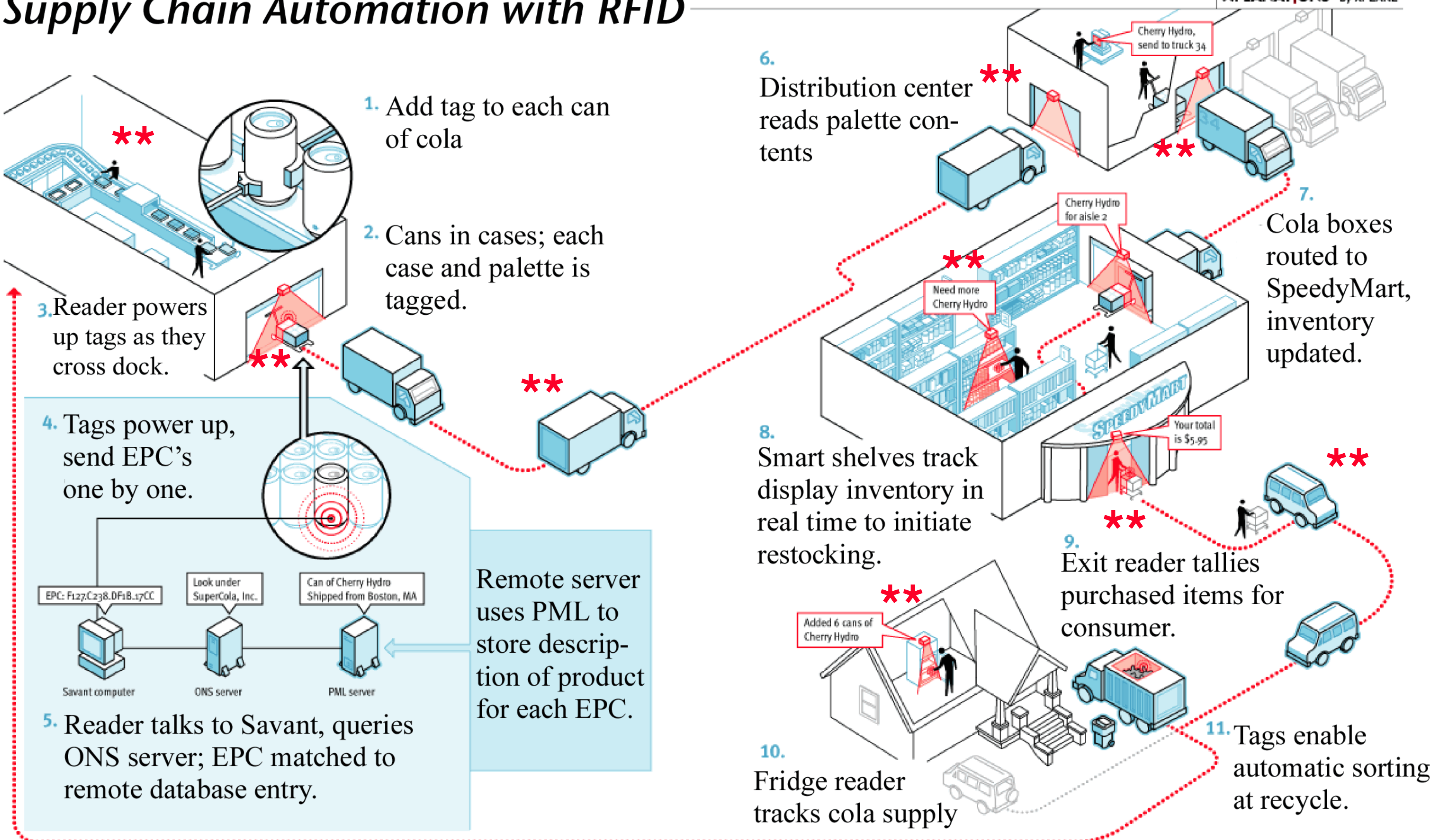
10. Fridge reader tracks cola supply

11. Tags enable automatic sorting at recycle.

Source: EPCglobal

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

Supply Chain Automation with RFID



XPLANATIONS by XPLANE

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.

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

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.

9. Exit reader tallies purchased items for consumer.

10. Fridge reader tracks cola supply

11. Tags enable automatic sorting at recycle.

Source: EPCglobal

** Add sensors to RFID with Standardized sensor interfaces

ISO/IEC/IEEE 21451.7 Standard on Security

- **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)

Field	Name	Size	Example/Note
1	TEDS type	3 bits	001_2
2	Sensor Type	7 bits	0001110_2 = Relative Humidity
3	Units extension	5 bits	Sub-type, e.g., for chemical sensors
4	Sensor map	16 bits	
5	Data resolution	5 bits	Sensor capability
6	Scale Factor Significand	11 bits	Sensor capability
7	Scale Factor Exponent	6 bits	Sensor capability
8	Scale Offset Significand	11 bits	Sensor capability
9	Scale Offset Exponent	6 bits	Sensor capability
10	Data uncertainty	3 bits	Sensor capability
11	Sensor Reconfiguration Capability	1 bit	0 = NO 1 = YES
12	Memory Rollover Capability	1 bit	0 = NO 1 = YES
13	Air Interface Security Capability Code (Note 1)	3 bits	See Table 5 for details.
14	Sensor Security Capability Code (See Note 1)	3 bits	000_2=No Direct Sensor Security. If greater than zero then at least one-way password security is supported. If greater than zero and at least one authentication encryption algorithm is supported, then two-way initial encrypted authentication is also supported. See Continuing Authentication Capability field of this table for directions supported when continuing to authenticate each command. See Table 6 for Sensor Security Capability Code assignments.

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.

21451.7 Prim. Sensor Characteristics - Continued

Field	Name	Size	Example/Note
15	Sensor Authentication Encryption Capability Map	7 bits	Choices of encryption algorithms for authentication that the sensor supports. If all zeroes then encrypted authentication is not supported.
16	Sensor Data Encryption Capability Map	7 bits	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.
17	Sensor Authentication Password/Key Size (Note 2)	3 bits	000_2=16 bits, 001_2=32 bits, 010_2=64 bits, 011_2=128 bits, 100_2~111_2 = RFU
18	Sensor Data Encryption Key Size (See Note 3)	3 bits	000_2=16 bits, 001_2=32 bits, 010_2=64 bits, 011_2=128 bits, 100_2~111_2 = RFU
19	Random Number Sizes Supported (See Note 4)	3 bits	000_2 = 16 bits, 001_2 = 16 & 32 bits, 010_2 = 16, 32 & 64 bits, 011_2= 16, 32, 64, & 128 bits, 100_2~111_2 = RFU

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

21451.7 Prim. Sensor Characteristics - Continued

Field	Name	Size	Example/Note
20	Continuing Authentication Capability field (See Note 5)	2 bit	See Table 9 for details.
21	Data Encryption Capability field	2 bit	Table 10 for details.
22	Clock Accuracy (See Note 6)	3 bits	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.

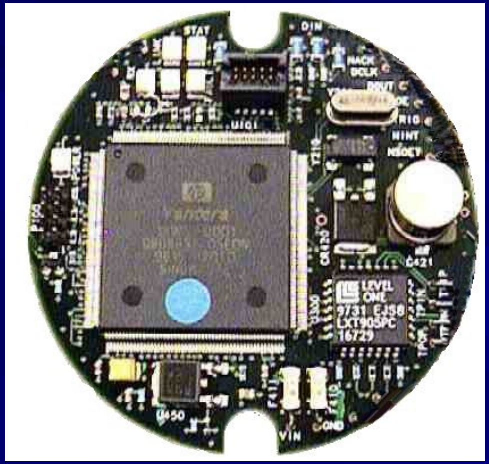
Note 6: Clock accuracy applies to logged data, and if supported then also to the Secure Session Timer of Table 16. The range of values shown are suitable for the two main classes of reference sources, which are free running relaxation (RC) oscillators (trimmed and untrimmed) and low cost low power crystal timers (such as standard 32.768 kHz watch crystal based Real Time Clocks).

The manufacturer shall permanently lock the Primary Sensor Characteristics TEDS.

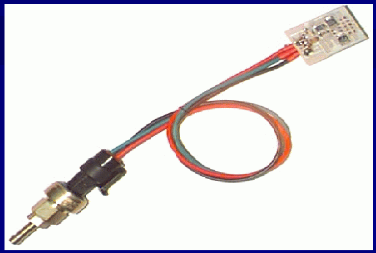
NIST
National Institute of Standards and Technology

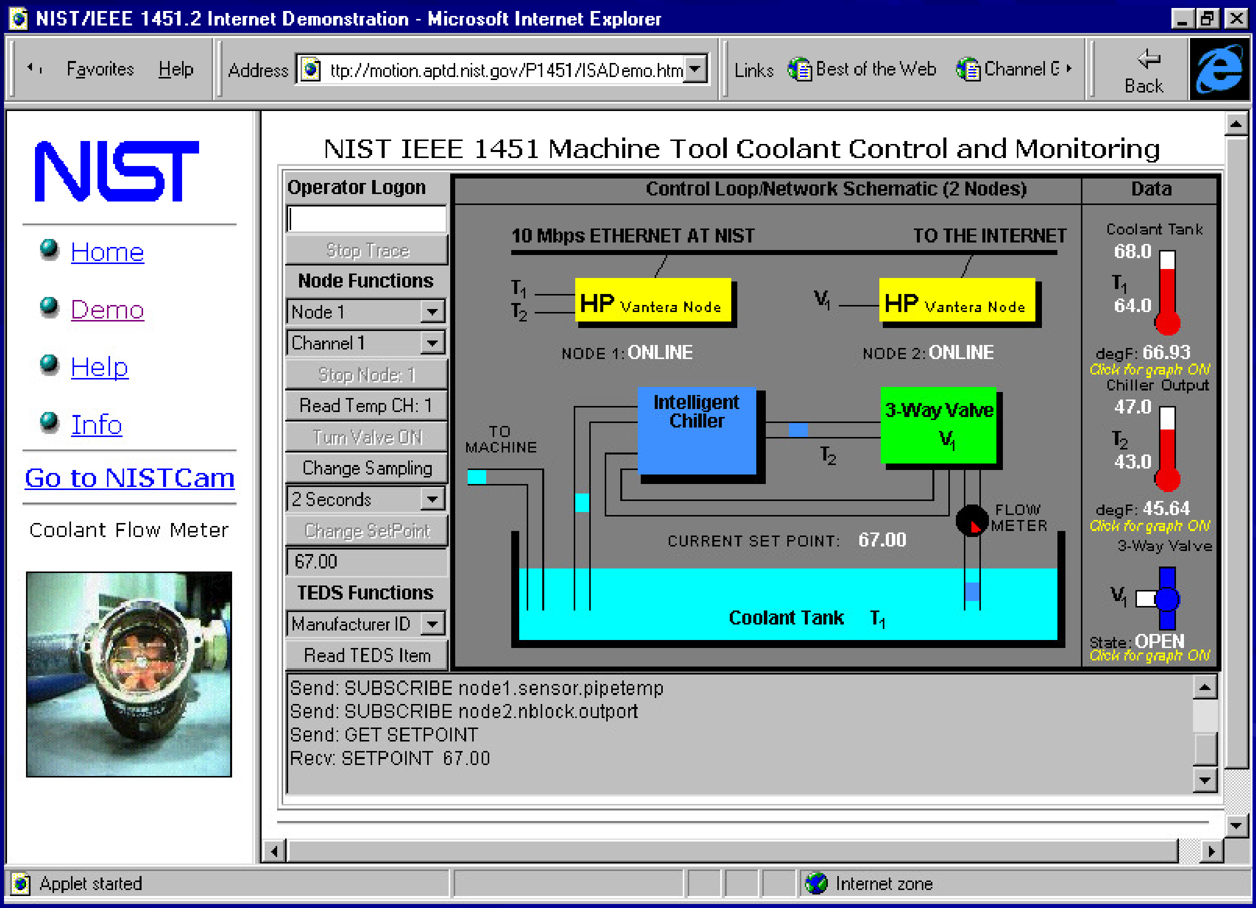
Enabling Technology for Web-based Online Sensor Monitoring, Diagnostic, and Control.

Ethernet node + web server



Sensor with 1451 Interface





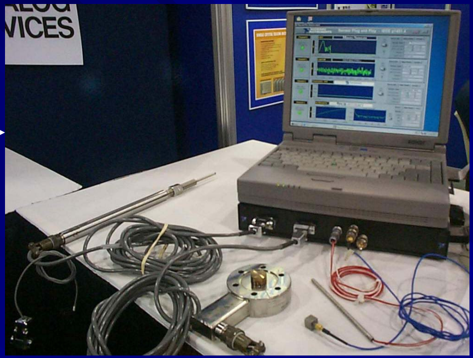
```
Send: SUBSCRIBE node1.sensor.pipetemp
Send: SUBSCRIBE node2.nblock.outport
Send: GET SETPOINT
Recv: SETPOINT  67.00
```

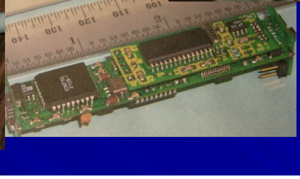
The Java-based remote monitoring and control applet

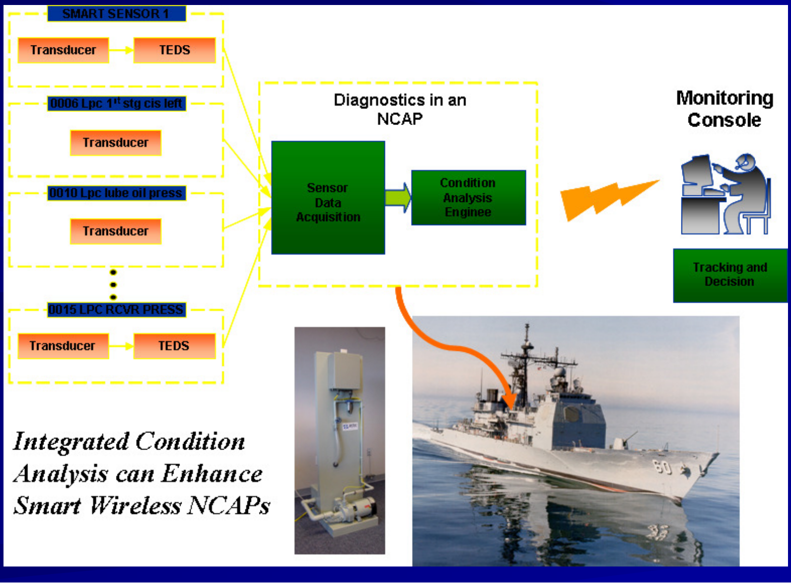
NIST
National Institute of Standards and Technology

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 SensorNet.
- IEEE 1451 in naval vessels for CBM.





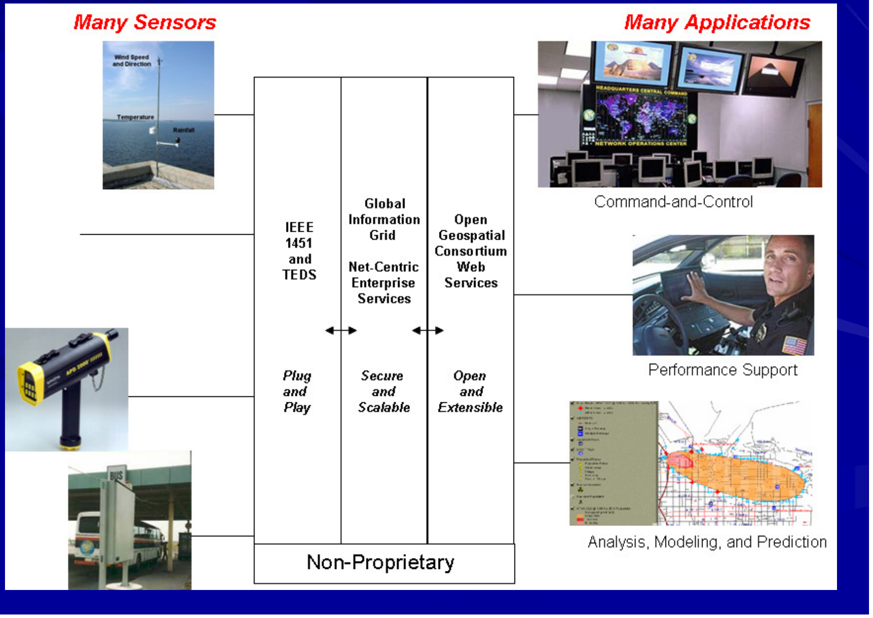


SMART SENSOR 1
Transducer → TEDS
0006 Lpc 1st stg cis left
Transducer
0010 Lpc lube oil press
Transducer
0015 LPC RCVR PRESS
Transducer → TEDS

Diagnostics in an NCAP
Sensor Data Acquisition → Condition Analysis Enginee

Monitoring Console
Tracking and Decision

Integrated Condition Analysis can Enhance Smart Wireless NCAPs



Many Sensors

Many Applications

IEEE 1451 and TEDS

Global Information Grid

Net-Centric Enterprise Services

Open Geospatial Consortium Web Services

Plug and Play

Secure and Scalable

Open and Extensible

Non-Proprietary

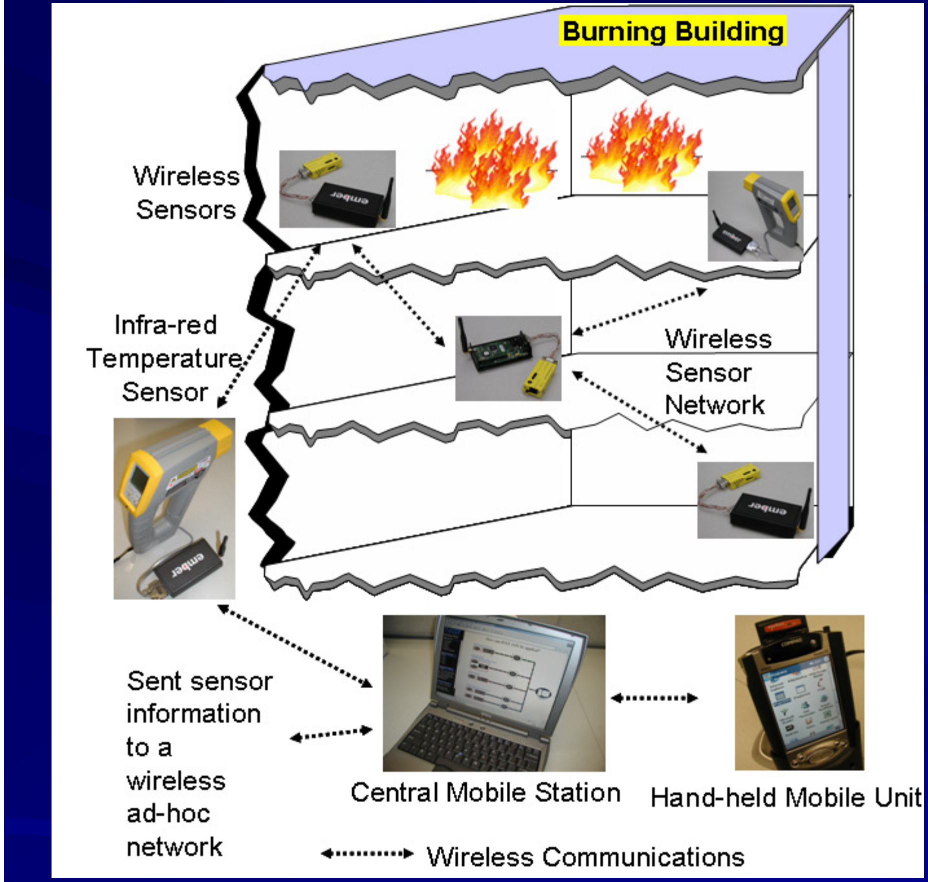
Command-and-Control

Performance Support

Analysis, Modeling, and Prediction

NIST National Institute of Standards and Technology

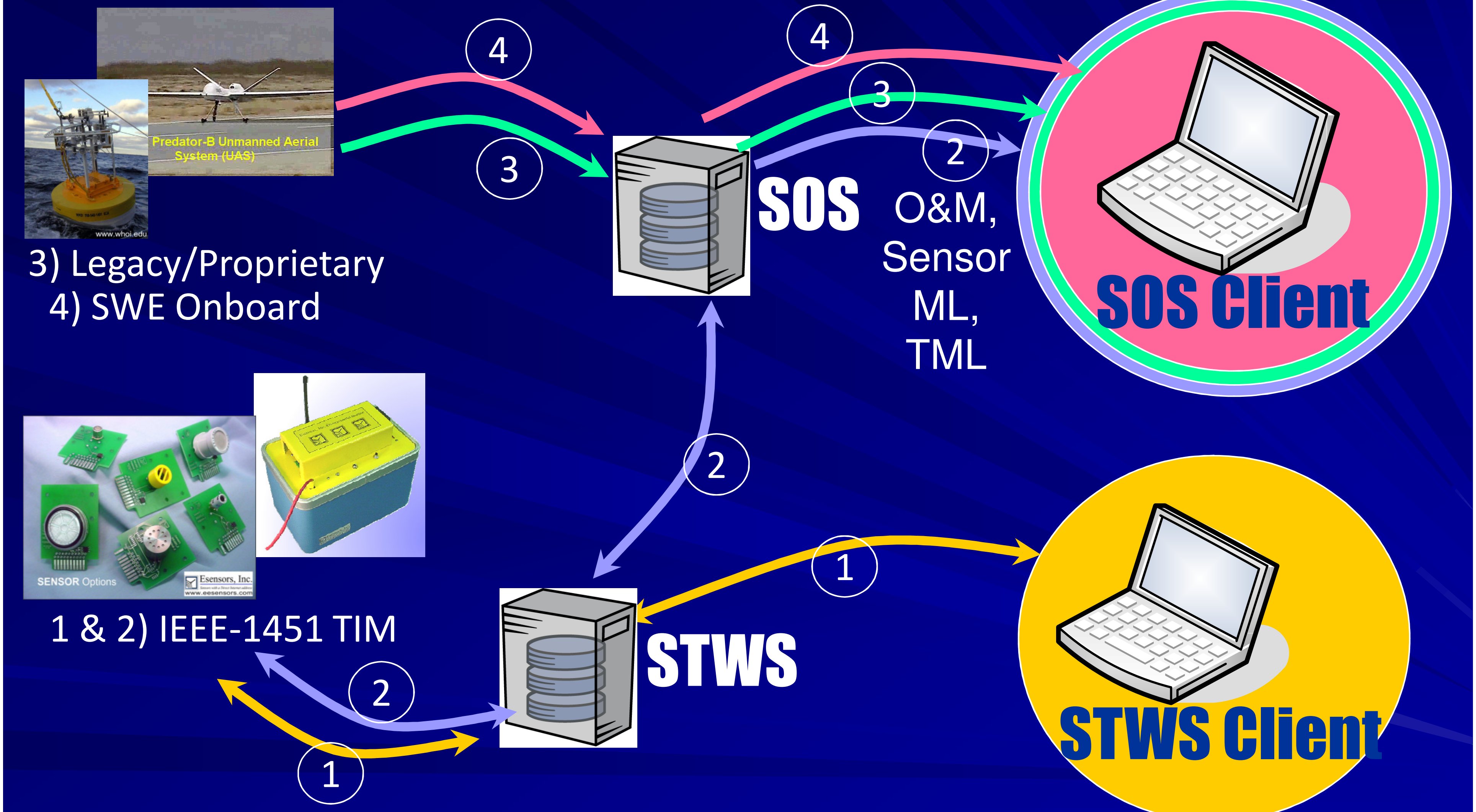
Sensor and RFID Standards for:



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

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.

IEEE 1451 & OGC-SWE Integration



3) Legacy/Proprietary
4) SWE Onboard

SOS

O&M,
Sensor
ML,
TML

SOS Client

1 & 2) IEEE-1451 TIM

STWS

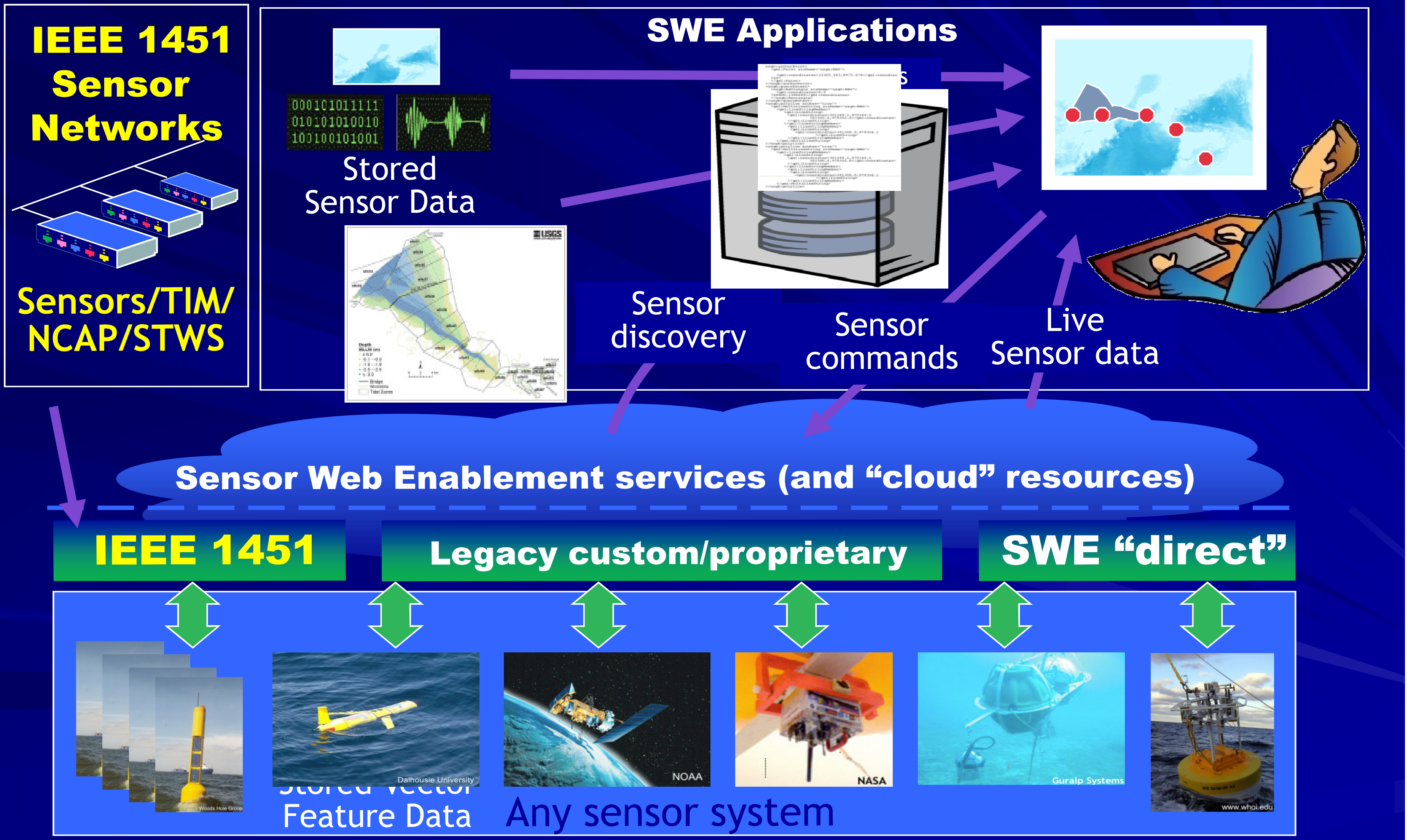
STWS Client

OGC Data Specifications: O&M, SensorML, TML

Courtesy Open Geospatial Consortium

OGC SWE & IEEE 1451 Converged in Ocean Applications

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



IEEE 1451 Sensor Networks

Sensors/TIM/ NCAP/STWS

SWE Applications

Stored Sensor Data

Sensor discovery

Sensor commands

Live Sensor data

Sensor Web Enablement services (and “cloud” resources)

IEEE 1451

Legacy custom/proprietary

SWE “direct”

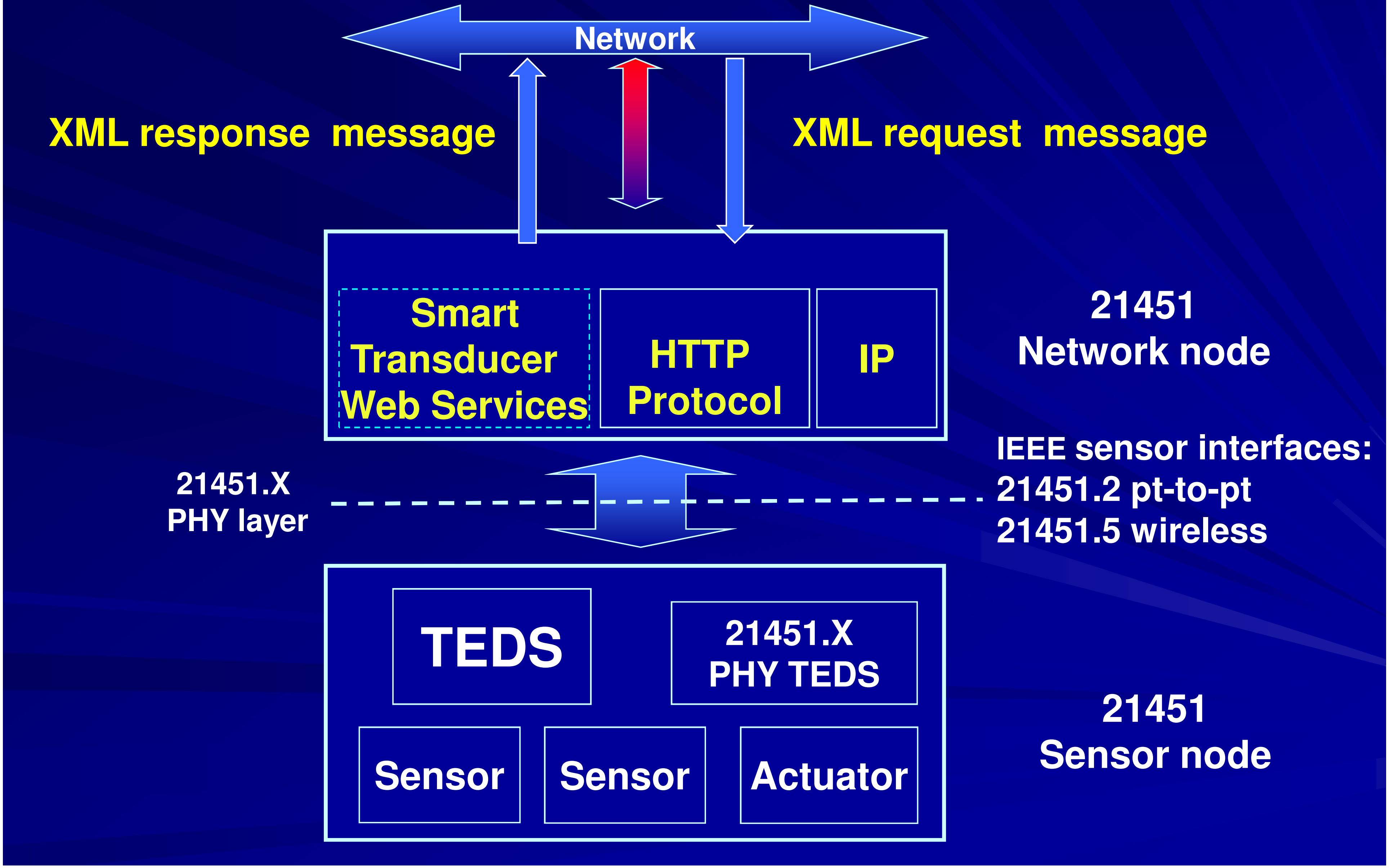
Stored Vector Feature Data

Any sensor system

Courtesy Open Geospatial Consortium

NIST
National Institute of Standards and Technology

Network and Internet Access of ISO/IEC/IEEE 21451 Sensors



Network

XML response message

XML request message

Smart Transducer Web Services

HTTP Protocol

IP

21451 Network node

21451.X PHY layer

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

TEDS

21451.X PHY TEDS

Sensor

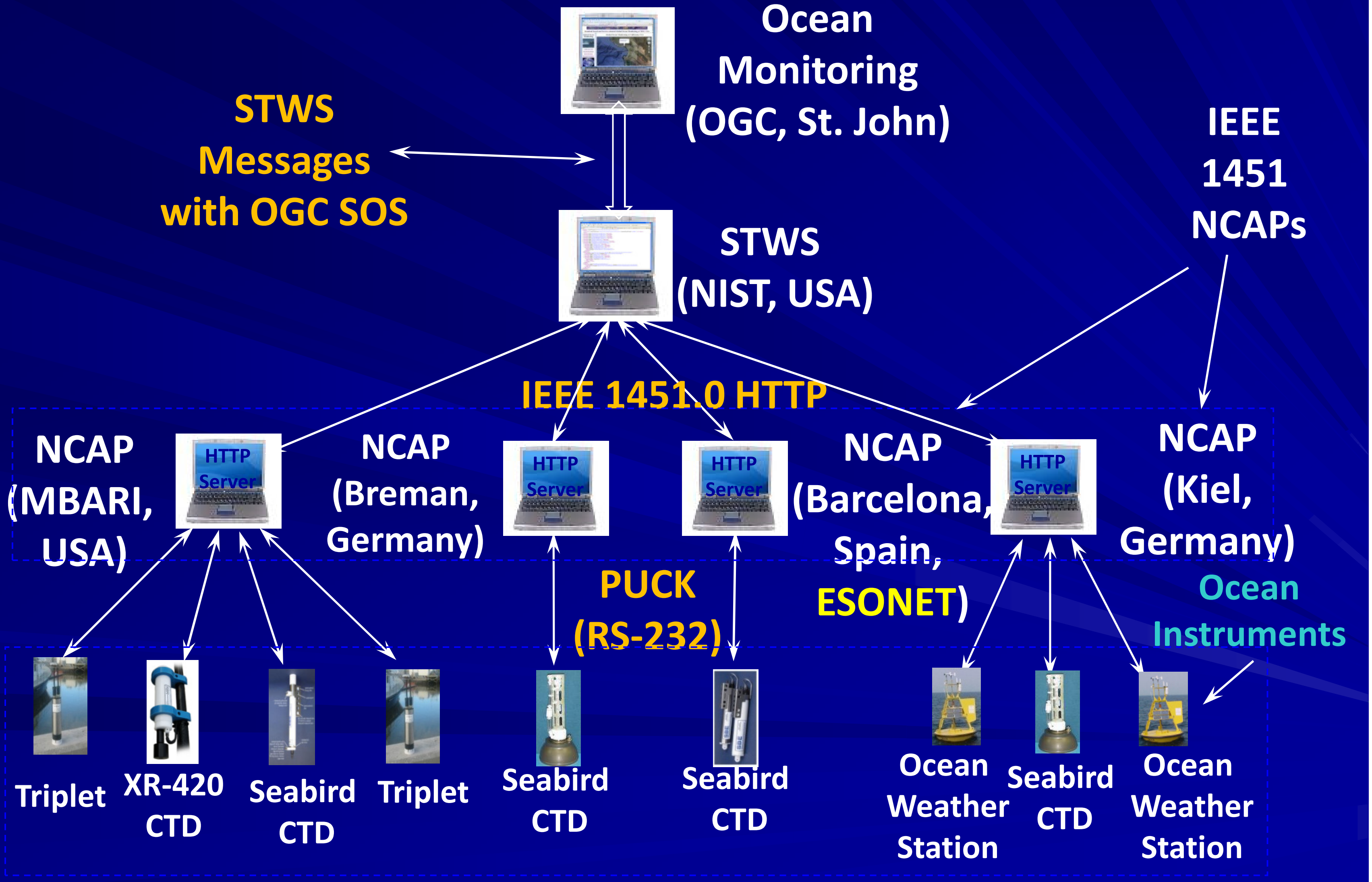
Sensor

Actuator

21451 Sensor node

Ocean Application Demo Setup

Common interfaces were used for connectivity



Ocean Monitoring (OGC, St. John)

STWS Messages with OGC SOS

STWS (NIST, USA)

IEEE 1451 NCAPs

IEEE 1451.0 HTTP

NCAP (MBARI, USA)

NCAP (Breman, Germany)

NCAP (Barcelona, Spain, ESONET)

NCAP (Kiel, Germany)

PUCK (RS-232)

Ocean Instruments

Triplet

XR-420 CTD

Seabird CTD

Triplet

Seabird CTD

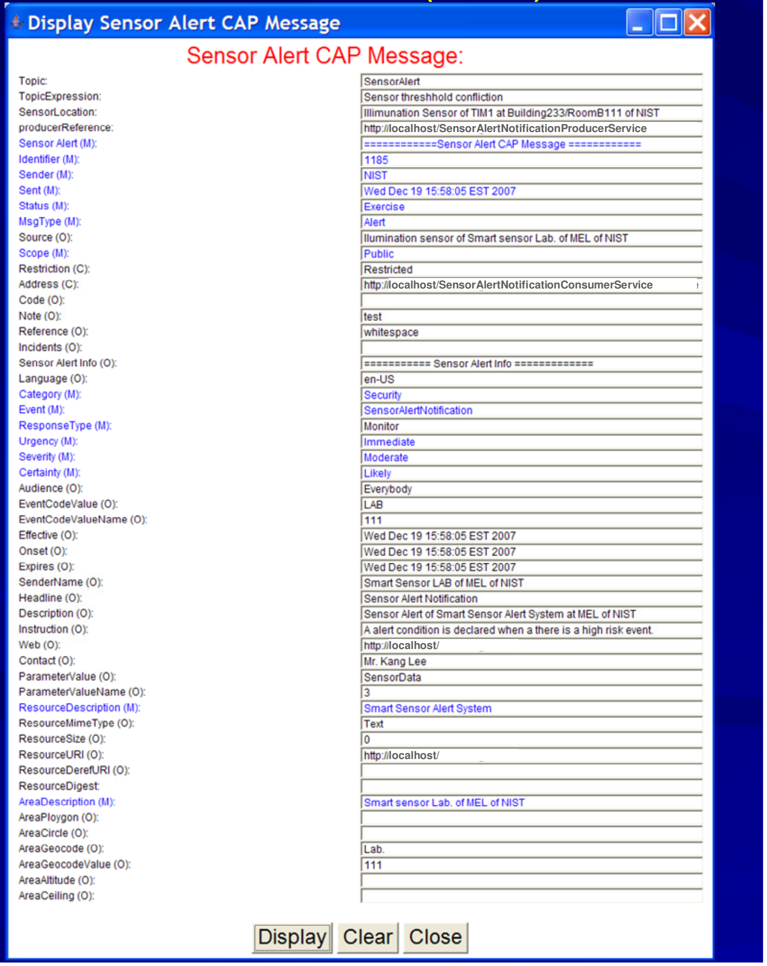
Seabird CTD

Ocean Weather Station

Seabird CTD

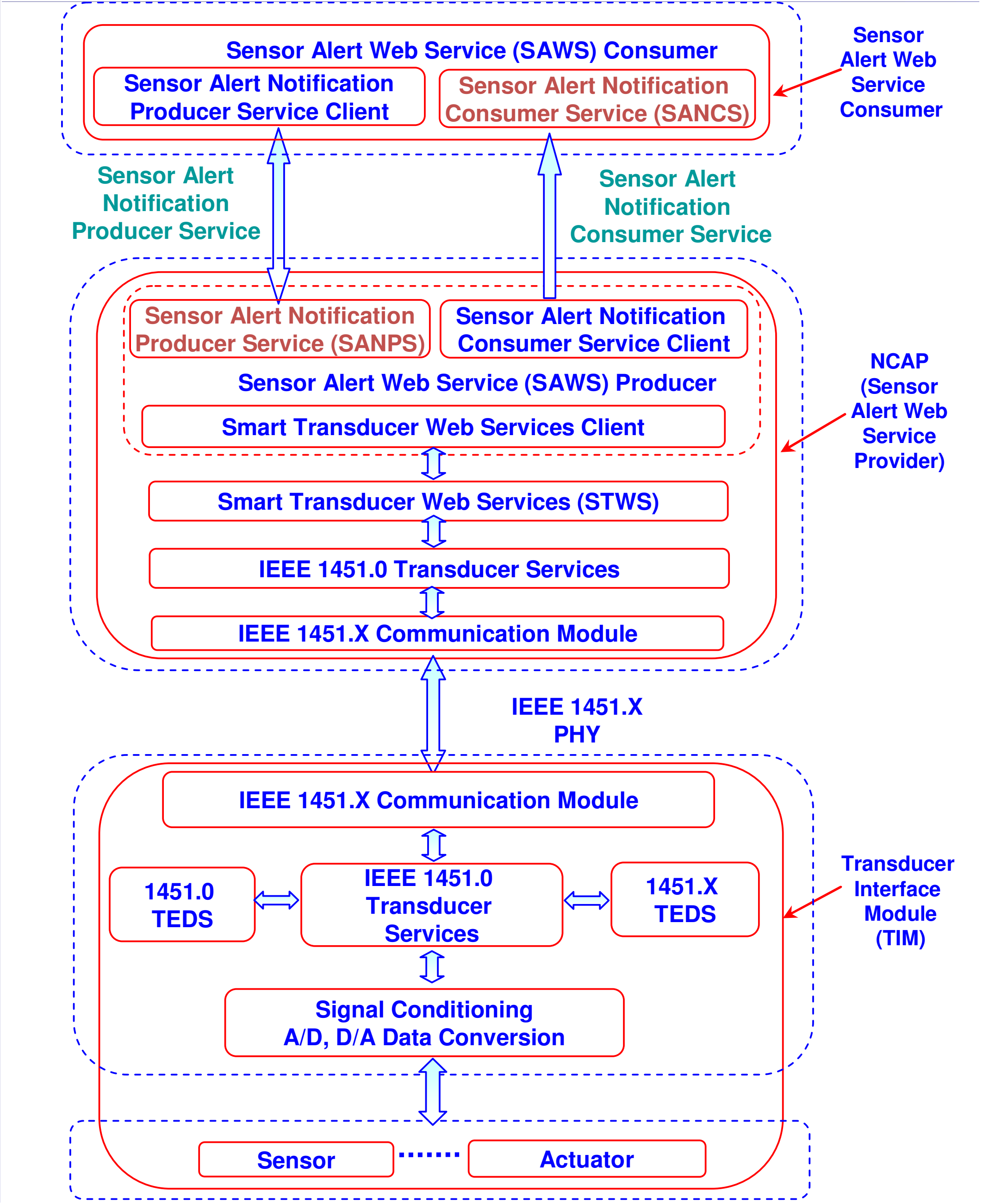
Ocean Weather Station

Architecture of Sensor Alert Web Service for IEEE 1451-based sensor networks and its implementation with OASIS Common Alert Protocol (CAP)



Sensor Alert CAP Message:

Topic:	SensorAlert
TopicExpression:	Sensor threshhold confliction
SensorLocation:	Illimunation Sensor of TIM1 at Building233/RoomB111 of NIST
producerReference:	http://localhost/SensorAlertNotificationProducerService
Sensor Alert (M):	============Sensor Alert CAP Message ============
Identifier (M):	1185
Sender (M):	NIST
Sent (M):	Wed Dec 19 15:58:05 EST 2007
Status (M):	Exercise
MsgType (M):	Alert
Source (O):	Ilumination sensor of Smart sensor Lab. of MEL of NIST
Scope (M):	Public
Restriction (C):	Restricted
Address (C):	http://localhost/SensorAlertNotificationConsumerService
Code (O):	
Note (O):	test
Reference (O):	whitespace
Incidents (O):	
Sensor Alert Info (O):	=========== Sensor Alert Info =============
Language (O):	en-US
Category (M):	Security
Event (M):	SensorAlertNotification
ResponseType (M):	Monitor
Urgency (M):	Immediate
Severity (M):	Moderate
Certainty (M):	Likely
Audience (O):	Everybody
EventCodeValue (O):	LAB
EventCodeValueName (O):	111
Effective (O):	Wed Dec 19 15:58:05 EST 2007
Onset (O):	Wed Dec 19 15:58:05 EST 2007
Expires (O):	Wed Dec 19 15:58:05 EST 2007
SenderName (O):	Smart Sensor LAB of MEL of NIST
Headline (O):	Sensor Alert Notification
Description (O):	Sensor Alert of Smart Sensor Alert System at MEL of NIST
Instruction (O):	A alert condition is declared when a there is a high risk event.
Web (O):	http://localhost/
Contact (O):	Mr. Kang Lee
ParameterValue (O):	SensorData
ParameterValueName (O):	3
ResourceDescription (M):	Smart Sensor Alert System
ResourceMimeType (O):	Text
ResourceSize (O):	0
ResourceURI (O):	http://localhost/
ResourceDerefURI (O):	
ResourceDigest:	
AreaDescription (M):	Smart sensor Lab. of MEL of NIST
AreaPloygon (O):	
AreaCircle (O):	
AreaGeocode (O):	Lab.
AreaGeocodeValue (O):	111
AreaAltitude (O):	
AreaCeiling (O):	


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

National Institute of Standards and Technology

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 adopts or harmonizes 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

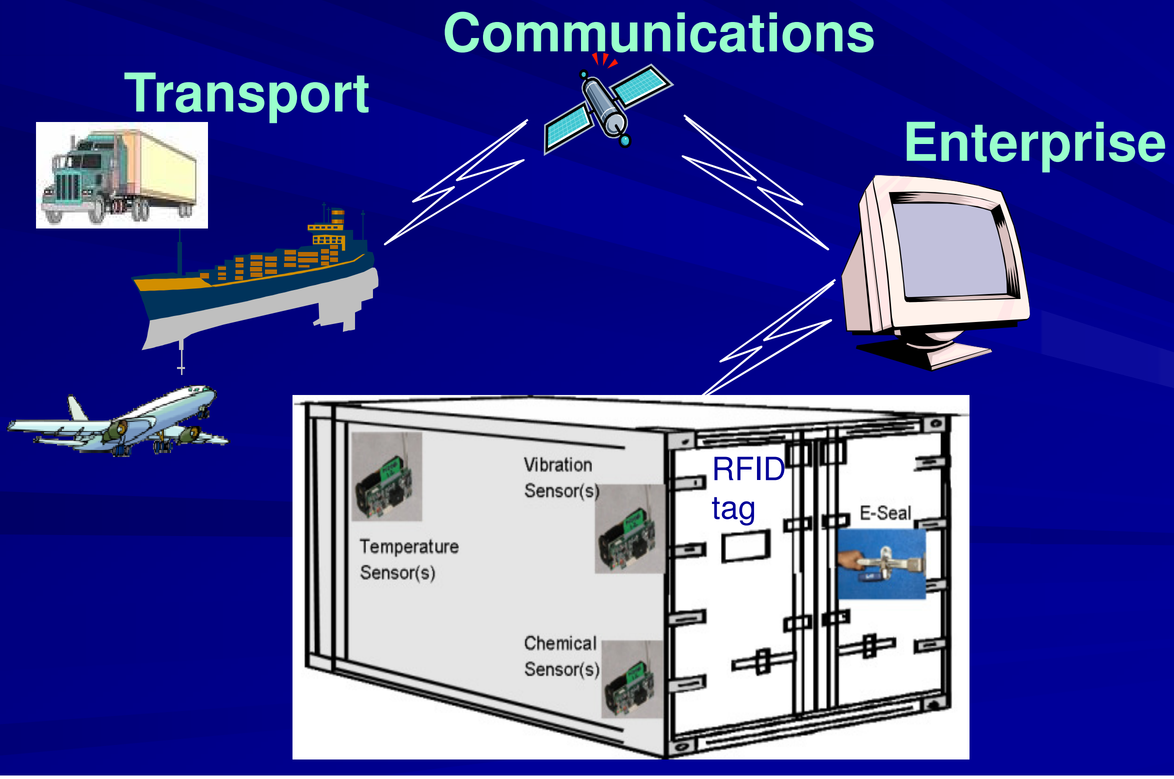
Objectives of SSHWG

- 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



Communications

Transport

Enterprise

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?