"Net-Ready" CBRN Sensors – A Way Forward…

Presented to: 2005 Chemical and Biological Information Systems (CBIS) Science and Technology (S&T) Conference

Chuck Datte
619.794.7099
cdatte@spawar.navy.mil

Ritesh Patel
619.553.4509
ritesh.patel@navy.mil

David W. Godso
703.989.0779
godso@spawar.navy.mil

Outline

- What is “net-ready”?
  - To the Warfighter…
  - To the Policy / Requirements / Program Professionals…
  - To the Engineers…
  - To the “10 year old”…
- Common Information Technology (IT) Platform for Sensors
- Desired Capabilities
  - General
  - Data and Service Standards
  - Reusable Host Platform
  - Modular Components
  - Security
- Conclusion

What is “Net-Ready”?

Net-Centricity* is a transformation enabler that empowers all users with the ability to easily discover, access, integrate, correlate and fuse data/information that support their mission objectives.

Systems exchange common data through a set of common services and interfaces which allow for flexible and dynamic specification of data producers and consumers and data routing (i.e.: Scales easily)*

* JFCOM/J8 – Joint Interoperability & Integration / C2 FCB

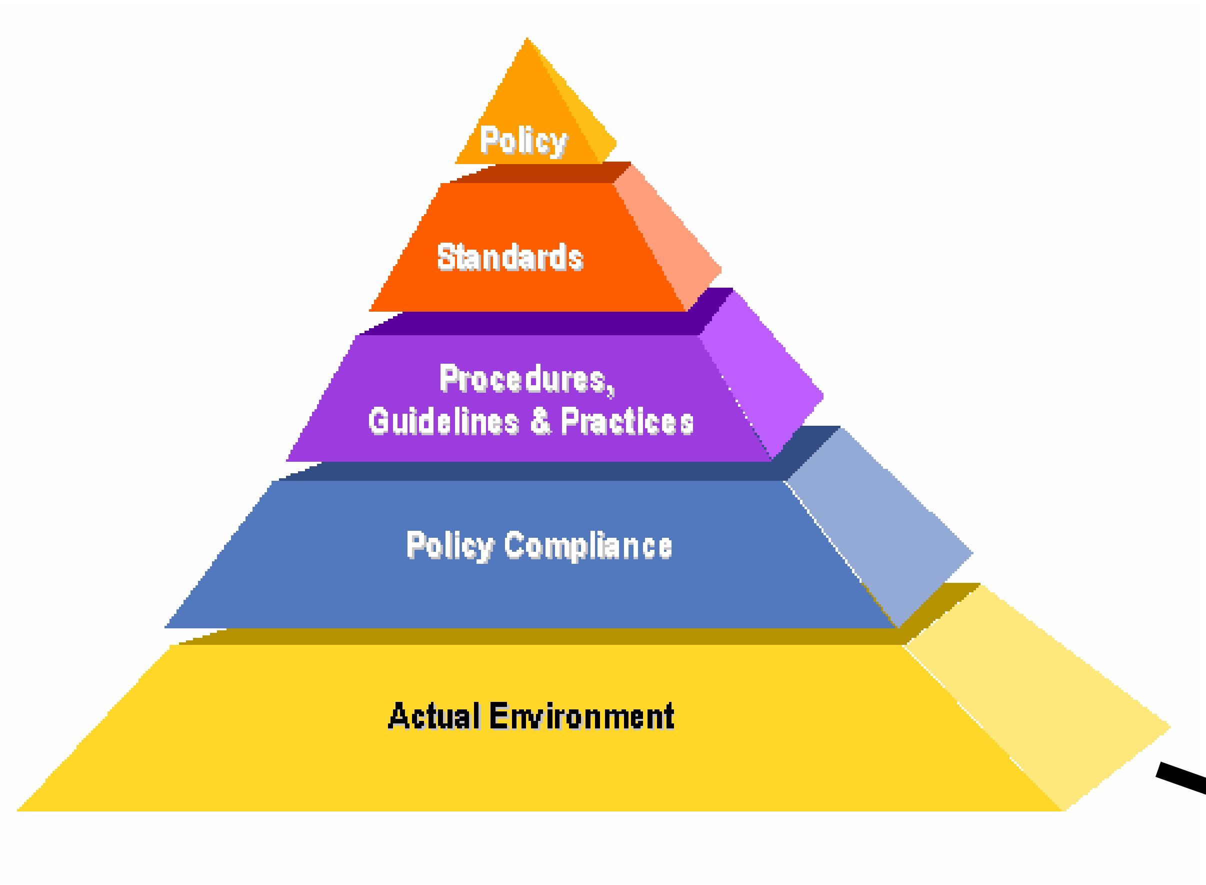
What is "Net-Ready"?
To the Warfighter…

To the Warfighter…

- Easily find, access, update, and share information resources relevant to their Area of Responsibility (AOR) and tasking
- Quickly deploy assets that have an information component to them with minimal setup and configuration expertise required
- Easily access wired / wireless connected sensors
- Dismount and carry forward handheld sensors that remain connected to the network (wirelessly)
- Sensor data seamlessly integrates with my C2 platform
- Plug and Play (PnP) sensors into the network

"Even my 10 year old knows what net-centric is…" and practices it…!!!

What is “Net-Ready”?
To the Policy / Requirements / Program Professionals…



To the Policy / Requirements / Program Professionals…

- **DoD Policies:**
  - **CJSCI/M 3170.01 Joint Capability Integration and Development System (JCIDS)**
  - **CJCSI 6212.01C Interoperability and Supportability of Information Technology and National Security Systems**
  - **DOD Architecture Framework (DODAF)**
    - **Provides a process and representation framework for developing and sharing architectures**
  - **Global Information Grid (GIG) and Net-Centric Operations Warfare Reference Model (NCOW)**
    - **Provides pervasive network connectivity to DoD Systems**
  - **GIG Network Centric Enterprise Services (NCES)**
    - **Provides Core Enterprise Services to DoD Systems beyond 06**
    - **Facilitates Community of Interest (COI) shared services**
  - **Net Ready KPP**
    - **Partially based on LISI and Inspeqtor tool**

To the Policy / Requirements / Program Professionals…

- **Compliance - measure Overall Degree to Which a Systems Makes its Services Net Accessible – Net-Ready KPP**

  – ***Compliance with the Net-Centric Operations and Warfare Reference Model***

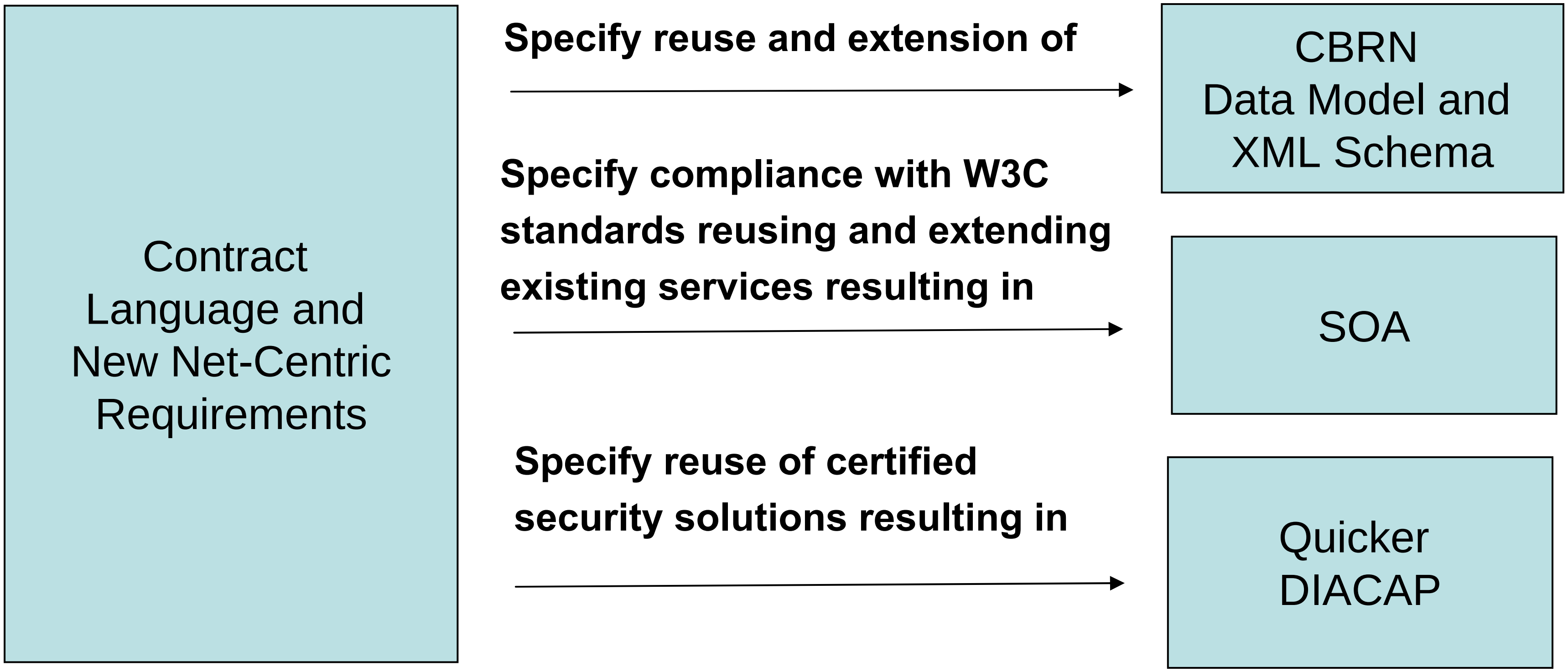
  – ***Compliance with applicable Global Information Grid Key Interface Profiles***

  – ***Compliance with DoD Information Assurance requirements***

  – ***Production of DoDAF products***

NR-KPP: Degree to Which a System Makes Data and Services Net Accessible

To the Policy / Requirements / Program Professionals…
JPEO-CBD SSA Activities



Contract Language and New Net-Centric Requirements

Specify reuse and extension of → CBRN Data Model and XML Schema

Specify compliance with W3C standards reusing and extending existing services resulting in → SOA

Specify reuse of certified security solutions resulting in → Quicker DIACAP

Translate the vision into specific guidance to JPEO-CBD developers – S&T should start with a common reusable “net-centric” IT platform and Test Community must develop robust test strategies to verify.

To the Policy / Requirements / Program Professionals…
Acquisition Goals

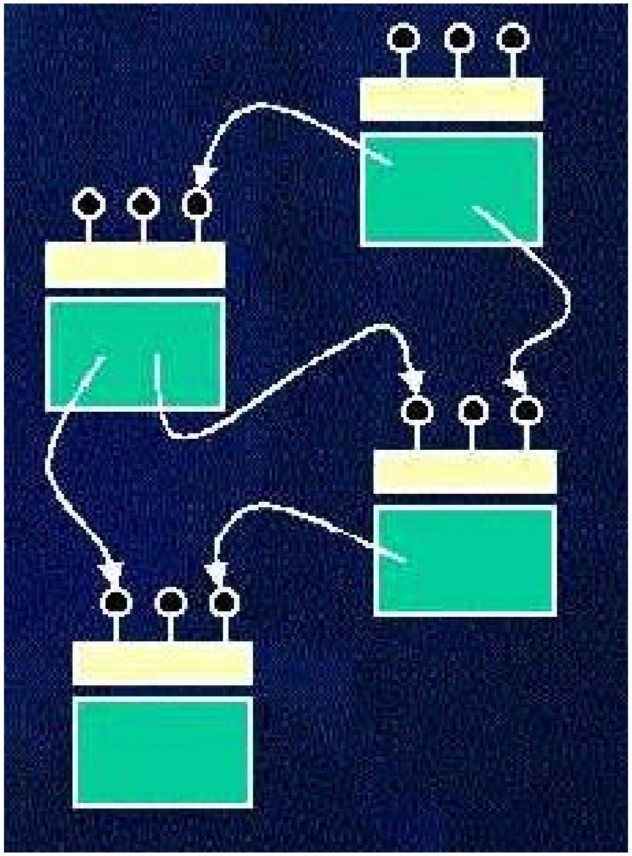
- **QUICKER fielding and LOWER procurement and sustainability costs through standardization**
  - **Common software and hardware platforms**
  - **No LSI's to "integrate" sensors into host/C4ISR systems…**
  - **PnP easily configurable common components**
  - **Reduced cost of operation and maintenance**
  - **Reduces deployment costs (with little or no integration costs)**
  - **Open standard interfaces**
    - **focus more on what to do with the data than how to decipher N different sources (no stovepipe solutions)**

What is “Net-Ready”?
To the Engineers…

To the Engineers…

Best Practices

- Common software services that are based on a common data model, common schema, and common protocol
  - Sensor data is already in the format expected and can be readily stored in my host database and/or pushed to decision support systems
  - Data Integration becomes translation between schemas, vice programming
- Modular, reusable, domain independent software components
  - Common software driver reused for all new sensors for sending / receiving sensor data
  - More configuration and less new development



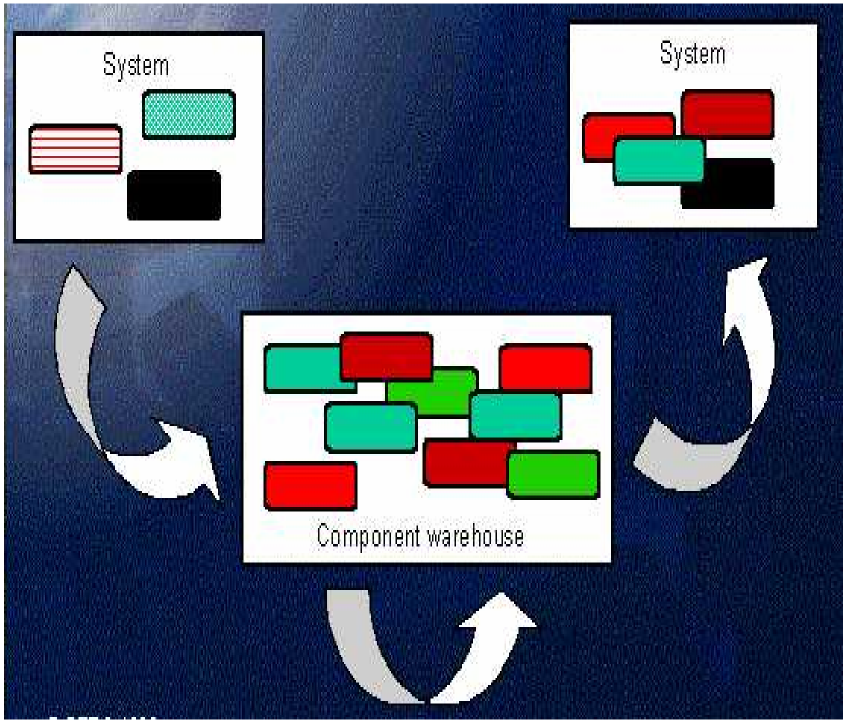
***More** upgrade, configuration, and component provisioning…*

***Less** new development… **Modularity** and **Reuse** are key.*

To the Engineers…

Facilitation of Net-Centric Operations

- Component configuration and deployment and dynamic software load in-the-field provisioning to well defined interfaces:
  - Component upgrade and component level integration
  - PnP components provisioned based on environment (e.g. wired, wireless, bandwidth restrictions (specification of common binary compression/decompression techniques), modifiable encryption/decryption, operational vice service/maintenance)…



Late binding… distributed interaction… assembly vice development…

To the Engineers…
Developer Guidance

- Systems and technical views of DoDAF architectures that specify technology standards, explain how systems communicate, data passed, and how data are represented
- Supports the W3C WS-I (Web Services Interoperability) Basic Profile (e.g. XML, SOAP, WSDL, UDDI, HTTP(S))
- Configuration controlled components and artifacts:
  - E.g. Architecture and Data Models, Engineering Reference Model Specifications, Technical Specifications, Common Software Services, and Common Hardware platforms
  - CBRN Data Model must be maintained and up-to-date and in sync with the sensor-interfaces
  - Modularity to enhance compatibility across versions
  - *Joint CBRN (JCBRN) Architecture Working Group, Data Working Group, and Configuration Management Plan Established…*

Ensuring interoperability and portability starts with the specifications…

To the Engineers…

Testers Guidance

- Implies redefinition of system vice “service” boundaries when testing a net-centric service vice a SoS or FoS composition thereof
- Encapsulate testing of the “IT” component vice “CBRN” testing
- Common IT services => common test strategies and facilitates the automation of testing IT services

New requirements imply new test cases and testing strategies… however, as we develop common services, testing should become easier, not harder.

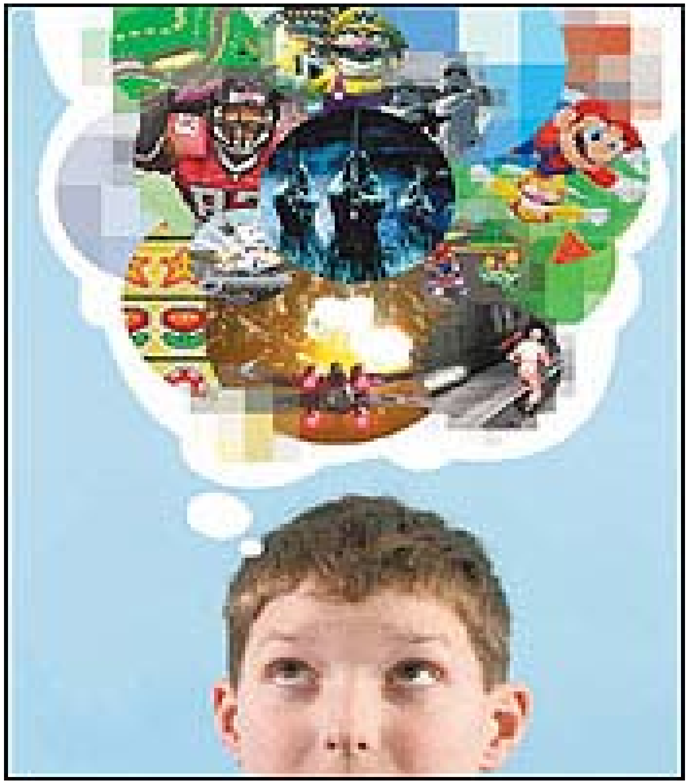
Plug-n-Play on-the-go!

What is "Net-Ready"?

To the "10 Year Old"…

"Google" Anything I Want!!!

On Line Gaming!



Play With My Friends Anywhere / Anytime - Online!

To the "10 Year Old"…

- Discover who is on line… chat with my friends… share information with my friends – use their toys and let them use mine… all on-line…
  - *Robust inexpensive real-time distributed collaboration and resource sharing…*
- Online gaming – discover game servers and other gamers and start seeing them and their actions/status on my display and have them see my actions/status on theirs…
  - *Distributed situational awareness engagement applications…*
- Wireless on the go is a way of life now – my cell phone, my PDA, my IPOD (look, I'm "Podcasting"!) and dock it when I'm at home
  - *Same components used on the move or docked at home*
- PnP peripherals – I want to connect something new so I buy it and plug it in and use it
  - *Plug it in, load the driver, configure the device, get the data…*

Tomorrow's Warfighters already live in a net-centric world!

Net-Ready Sensors…

Net-Ready Sensors

- **Common CBRN Sensor Platform** – *the fully encapsulated net-centric reusable software service that communicates securely via the CBRN XML Schema using a common protocol…*
- All CBRN sensor data that can be transmitted, received, and stored will use the CBRN Data Model as the basis for data representation!
  - *Specification of sensor data entities and attributes in the CBRN Data Model is underway NOW, being lead by JPM IS Data Team.. Other specifications will follow…*

Standardization of the interfaces across all CBRN sensors/devices!

Key Assertions

Common IT Platform for Sensors

- Common IT platform for sensors:
  - **Sensor data format** and **protocol** that exists between a sensor and the host/user platform…
  - IT components associated with making a device “net-ready” are completely independent of the domain-space in which that device will be deployed…
  - NOT addressing data fusion

- No new radical development here –
  - Bringing CBRN Sensors into the 21st century…
  - Leveraging commercial and leading-edge DoD agency efforts
  - The “S&T” is really education, socialization, and miniaturized integration of existing components into CBRN sensors…

Starting with common open standards in S&T makes it much easier to evaluate new technology and transition it into programs of record.

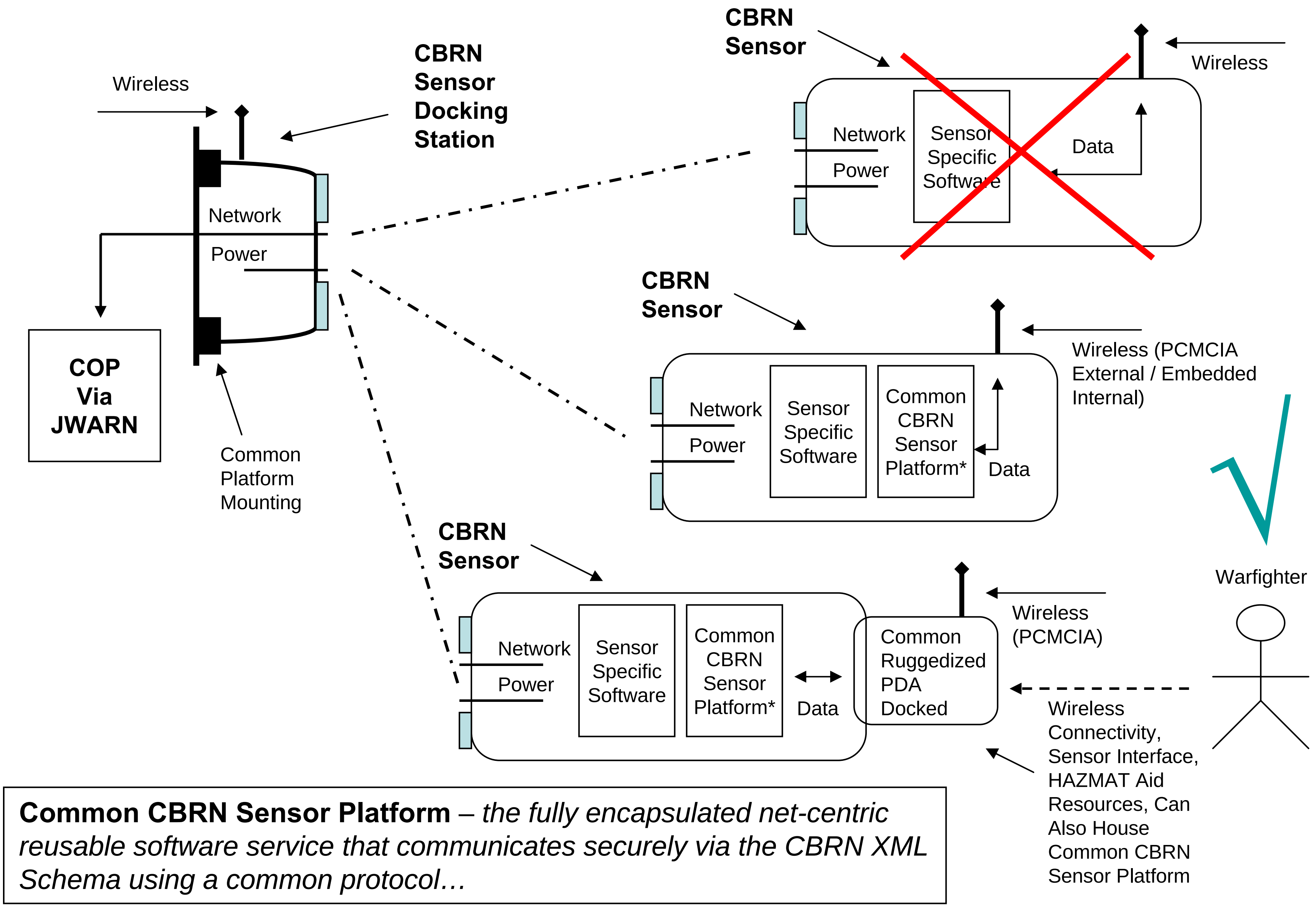
Key Assertions

Sensors in a Service Oriented Architecture

- For net-centric sensors to be successful, the interface standards must be widely accepted. To enable such wide acceptance, the standards used for these services and the technologies that implement those standards should meet the following criteria:*
  - A sensor should be able to service requests from any client regardless of the platform on which the client is implemented*
  - A client should be able to find and use any sensor regardless of the service's implementation details or the platform on which it runs*

** Derived from Designing Web Services with the J2EE 1.4 Platform - Overview of Web Service Standards.*

Desired Capabilities - General


Wireless
CBRN Sensor Docking Station
Network
Power
COP Via JWARN
Common Platform Mounting
CBRN Sensor
Network
Power
Sensor Specific Software
Data
Wireless
CBRN Sensor
Network
Power
Sensor Specific Software
Common CBRN Sensor Platform*
Data
Wireless (PCMCIA External / Embedded Internal)
√
CBRN Sensor
Network
Power
Sensor Specific Software
Common CBRN Sensor Platform*
Data
Common Ruggedized PDA Docked
Wireless (PCMCIA)
Warfighter
Wireless Connectivity, Sensor Interface, HAZMAT Aid Resources, Can Also House Common CBRN Sensor Platform

Common CBRN Sensor Platform – *the fully encapsulated net-centric reusable software service that communicates securely via the CBRN XML Schema using a common protocol…*

Desired Capabilities - General

- Software defined sensor platform that exploits network connectivity to perform its mission in support of diverse Warfighter needs
- Directly supports and encapsulates the DoD net-centric strategy … bring “net-centricity” to sensors via common reusable IT components
- Scaleable PnP architecture securely operable over the Internet
- Immediate integration into system and common operational picture by the Warfighter via JWARN, not a developer / integrator
- Mounts on vehicles and plugs into existing network… dismounts and forward deploys, remaining wirelessly connected – common embedded IT platform and common docking platform across all DoD CBRN sensors

Desired Capabilities - Data and Service Standards

- Out of the box, the sensor should be seen on the network as a discoverable web-enabled service
  - Light weight web-server available via HTTP(S)
  - Over-the-net administration, maintenance, analysis and in-the-field reconfiguration
  - URL / network configuration for streaming data or WSDL exposed for applications to pull data
  - Configuration of xmit of any/all available data fields and period of transmission
  - Repurposing of sensor data and software
  - Configuration (just like most $30 routers) such that email address(es) can be specified for log dumps, providing notification / request for service, or quality of service issues, or denial of service attacks

Desired Capabilities - Data and Service Standards

- Non-proprietary interface that accepts and generates XML to a well-formed schema
  - For JPEO-CBD developed sensors, this is the CBRN XML Schema
  - For commercial developers:
    - If the commercial sensor interface supplies a schema, then we write an XSLT (at a minimum) to map data from sensor vendor schema to CBRN XML Schema (ability to download an XSLT to the sensor preferred)
    - If the commercial sensor interface does not support a well-formed schema, then we will have to write a driver to their vendor supplied interface and then convert that data into a CBRN XML Schema representation *(this is the case we want to avoid at all costs and is a last resort… it's where we are today)*

Starting with common standards in S&T makes it much easier to evaluate new technology and transition it into programs of record.

Desired Capabilities - Reusable Host Platform

- Handheld CBRN sensors built to a common physical hardware docking specification
  - For power/recharge and wired network access when docked
  - Sensor remains wirelessly connected undocked and battery powered
- For those familiar with the JWARN JCID… we want “JCID on a chip”, embedded into all future CBRN sensors…
  - Seeking common small, cheap, proven, low-power hardware platforms (system on a chip or similar) that can be embedded in every sensor to host the desired software capabilities
  - Embed a smart network interface component into sensors
  - Same IT platform can be shared across CBRN sensors

Desired Capabilities - Modular Components

- Completely abstract the “GIG” interface component from the rest of the sensor platform
  - Reuse the infrastructure (software, embedded network cards, etc.)
  - Sensor vendors focus on CBRN “sensing” (detection and identification) and reuse components that provide data availability, sensor services, and security models
- Common open standard software drivers to communicate with devices and code/decode their data to/from the extensions that would be made to the CBRN COI XML Schema
- Performance - ability to “plug-in” compression / decompression on a data stream. Hooks available that allow us to download new modules that can change how that compression / decompression is performed (or not) based on bandwidth / environment

Desired Capabilities - Security

- Ability to “plug-in” encryption / decryption on a byte stream (XML). Hooks available that allow us to download new modules that can change how that encryption / decryption is performed (or not) based on bandwidth / environment
- Ability to “plug-in” future “XML Software Based Guards” into the sensor – hooks available to send / receive data cross-domain
- Encapsulates embedded information assurance framework that contains critical security related software that can be leveraged by all platforms without each of them having to worry about the IA details (abstracted security layer between the software and all ports, protocols, registry settings, network access)
- XML (tagging) of data to support a progression toward Multi-Level Security (MLS) and attribute level discrimination

Encapsulate and reuse accredited IA modules!

Conclusion - Example

- Adding a CBRN Sensor to the Network Should be NO HARDER THAN adding a wireless network printer:
  - Buy printer
  - Power on printer
  - Put CD in my computer
  - Load printer driver
  - Automatically discover new printer
  - Start printing… in less than 15 minutes after opening the box!
- Printer status and control automatically integrate into my host platform printer service manager
- From any where I have access to the network, I can get printer status, print, reconfigure the printer, and update software on that printer that provides new capabilities…

The "network components" are cheap, small, flexible, and available… and, they need to be reused and encapsulated in CBRN sensors!

Conclusion

An average 10-year old should be able to connect / configure / use CBRN sensors… and the steps for connecting to the network and “going mobile” should be identical across CBRN sensors!