

# IEEE International Conference on Smart Grid Engineering (SGE'12)



27-29 August, 2012  
UOIT, Oshawa, Canada



Sponsored by IEEE Toronto (NPSS & PES) and MITACS

## Tutorial (29-Aug-2012, 2:30-3:00pm)

### **XMPP for the Smart Grid**

ISO/IEC/IEEE 21451-1-4

eXtensible Markup and Presence Protocol Interface (XMPP) Standard  
for Sensors, Actuators, and Networked Devices

**WILLIAM .J. MILLER**  
MaCT USA  
Chairman



- A coordinated effort to recognize de facto, market-driven standards and raise the visibility of the principles that drive them launched today. The effort is branded as OpenStand Principles and is backed by global players in the standards arena, including the IEEE (Institute of Electrical and Electronics Engineers).



- "Five leading global organizations—IEEE, Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), Internet Society and World Wide Web Consortium (W3C)—today announced that they have signed a statement affirming the importance of a jointly developed set of principles establishing a modern paradigm for global, open standards.



- "The shared OpenStand Principles—based on the effective and efficient standardization processes that have made the Internet and Web the premiere platforms for innovation and borderless commerce—are proven in their ability to foster competition and cooperation, support innovation and interoperability and drive market success.



- "IEEE, IAB, IETF, Internet Society and W3C invite other standards organizations, governments, corporations and technology innovators globally to endorse the principles..."
- Learn more at:
- <http://open-stand.org/principles/>



IPDX for Android and  
Apple offers XMPP for  
mobile M2M sensor  
networks.

# XMPP for the Smart Grid

**-ISO/IEC/IEEE 21451-1-4  
eXtensible Markup and Presence Protocol Interface (XMPP) Standard  
for Sensors, Actuators, and Networked Devices**

**WILLIAM .J. MILLER  
MaCT USA  
Chairman**

**August 27-29, 2012**

Copyright 2012 - MaCT USA

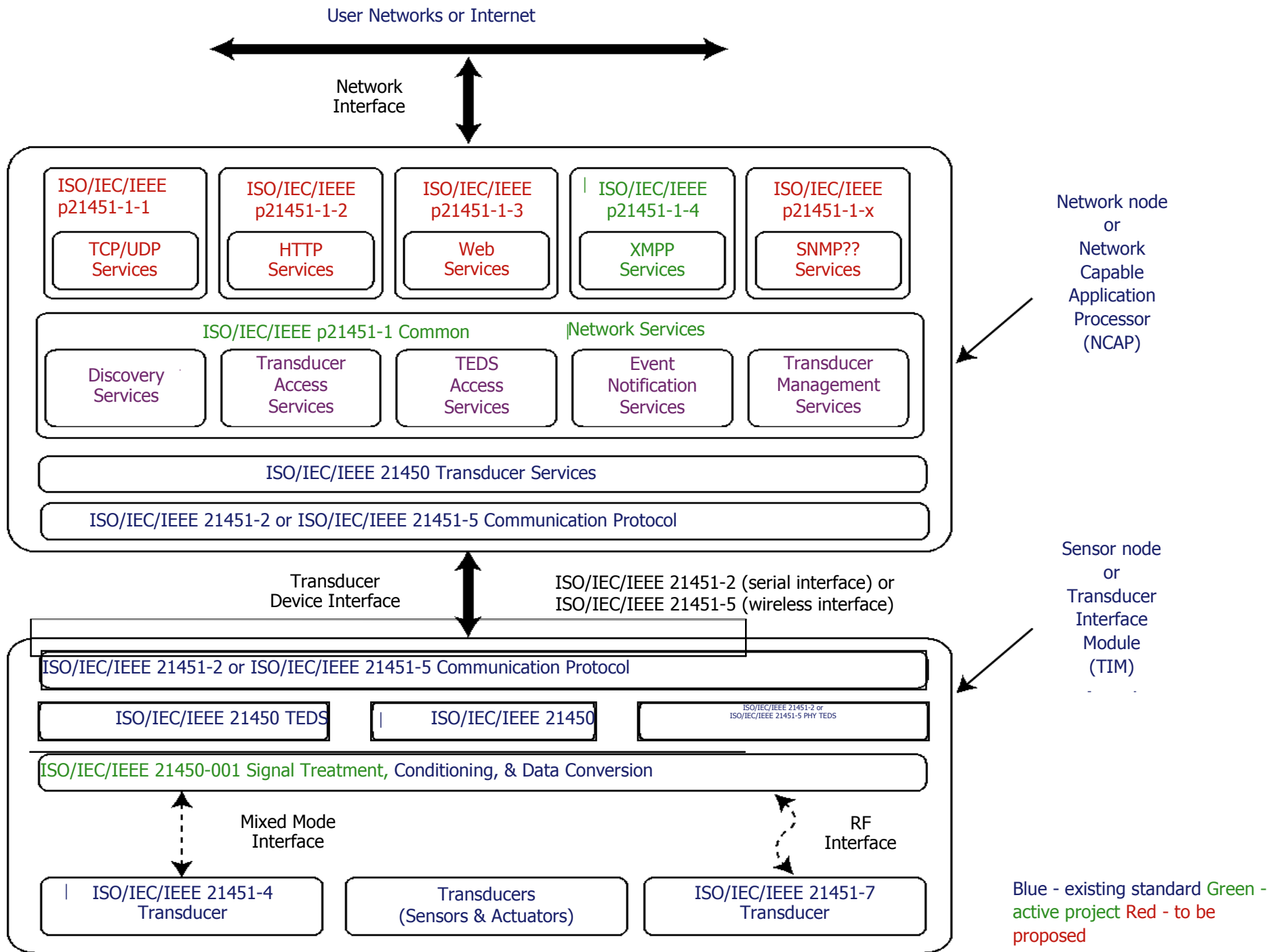
# What is XMPP?

- The eXtensible Messaging and Presence Protocol (XMPP) is an open XML technology for real-time communication, which powers a wide range of applications including instant messaging, presence, media negotiation, white-boarding, collaboration, lightweight middleware, content syndication, and generalized XML routing.
- More formally, XMPP is defined by RFC 3920 and RFC 2921 as published by the IETF in October 2004. Everything we've built on top of those two specifications called "XMPP extensions" or XEP stanzas.
- Learn more at <http://www.xmpp.org>

# ISO/IEC/IEEE 21451-1-4

- ISO/IEC/IEEE 21451-1-4 - eXtensible Messaging and Presence Protocol (XMPP) Standard for Sensors, Actuators, and Networked Device Communications using real-time streaming XML (Extensible Markup Language).
- ISO/IEC/IEEE 21451-1-4 was IEEE P1451.1.4.
- This work is sponsored by Dr. Kang Lee at NIST, chairman of IEEE TC9 Sensor Technology and host of the IEEE 1451 Smart Transducer series of standards
- Learn more at <http://www.ieee.org/development/project/1451.1.4.html>





# New Information

- ISO/IEC/IEEE 21451-1-4 being considered by ISO JTC1 SC31 as a common set of XEP stanzas using XMPP protocol for the ISO Internet of Things (IoT).
- IEEE SA evaluating IoT and overlap with cloud computing, M2M, Smart Grid, etc.
- IEEE SA considering to participate in oneM2M IoT effort and recommend common XEP stanzas

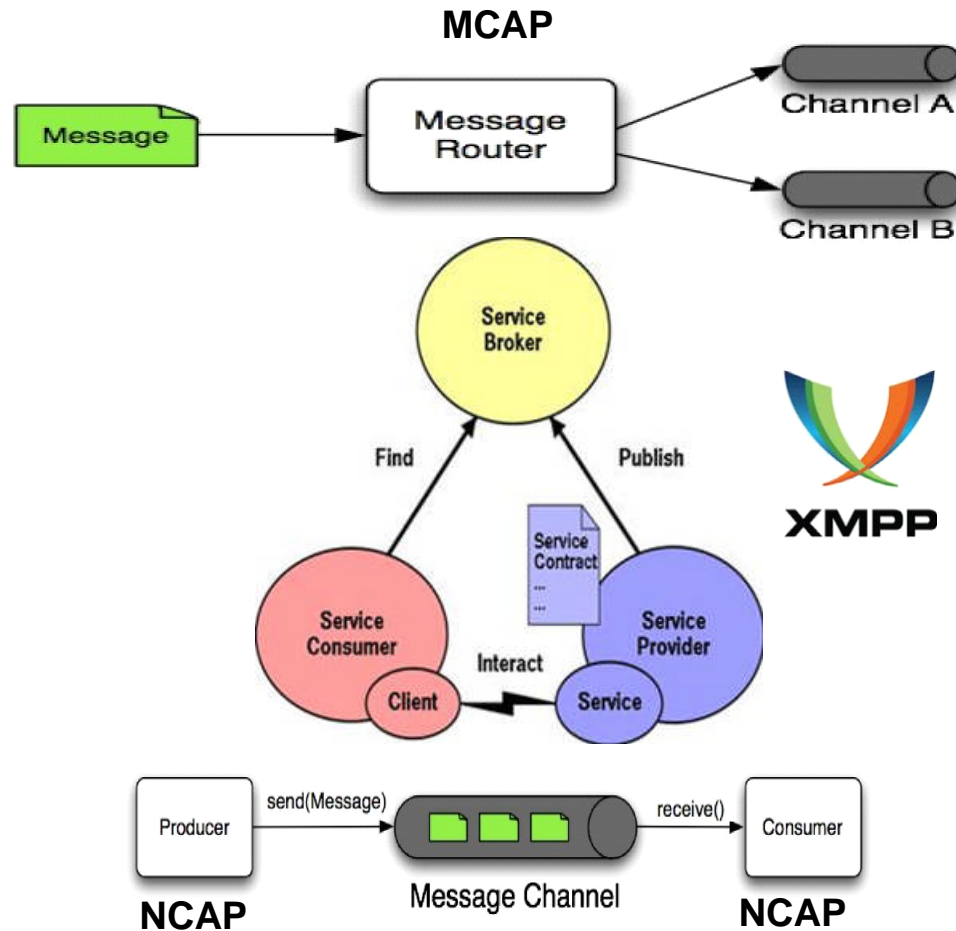
# IETF XMPP

- IETF XMPP Working Group has already produced a number of documents:
- RFC 3920 – XMPP: Core, which describes client-server messaging using two open-ended XML streams. A connection is authenticated with Simple Authentication and Security Layer (SASL) and encrypted with Transport Layer Security (TLS).
- RFC 3921 – XMPP: Instant Messaging and Presence.
- RFC 3922 – Mapping the XMPP to Common Presence and Instant Messaging
- RFC 3923 – End-to-End Signing and Object Encryption for XMPP.
- <http://www.xmpp.org/about-xmpp/xsf>

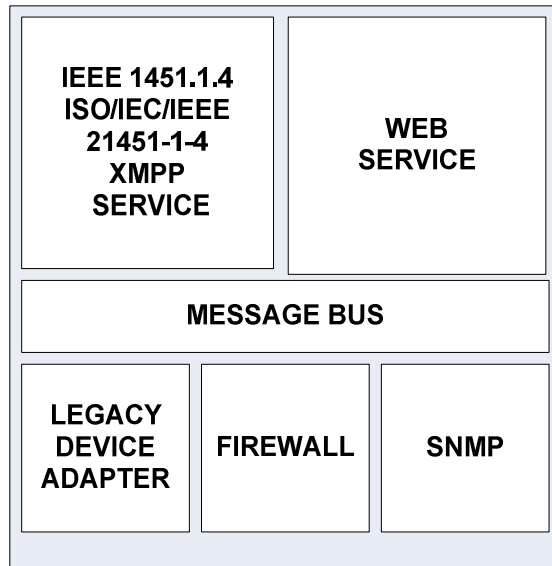
# IPDX™

- IPDX is the first to offer capabilities based upon the use of XMPP to offer an event driven messaging system for enterprise integration of large scale heterogeneous sensor networks.
- IPDX offers a distributed decentralized client-server architecture which includes registration, policy administration and management including directory services, data sharing, and security.
- IPDX provides a reference model for the ISO/IEC/IEEE 21451-1-4 standard.
- <http://www.mact-usa.com>

# Integration Concept



# IPDX



IPDX for Android and Apple offers XMPP for mobile M2M sensor networks.

# IPDX App

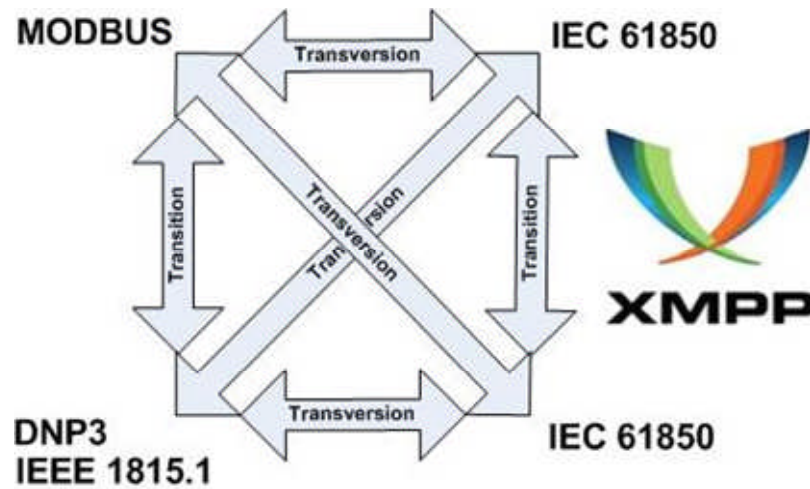
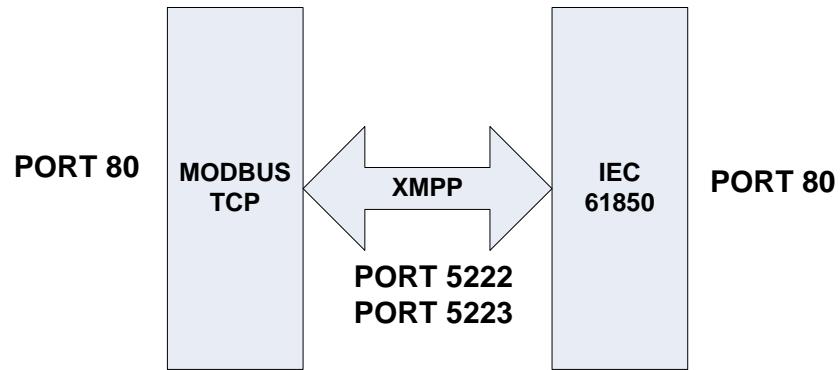


**IPDX for Apple  
brings XMPP power  
for mobile M2M  
sensor networks.**



**IPDX for Android  
brings XMPP power  
for mobile M2M  
sensor networks.**

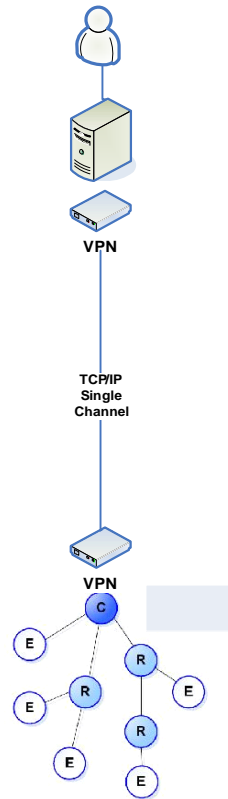
# TRANSVERSION



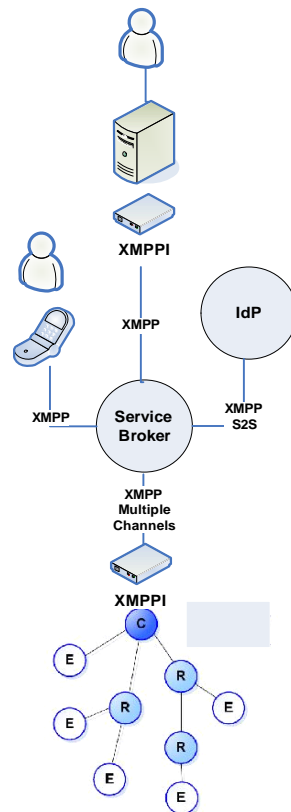


# Cloud Services

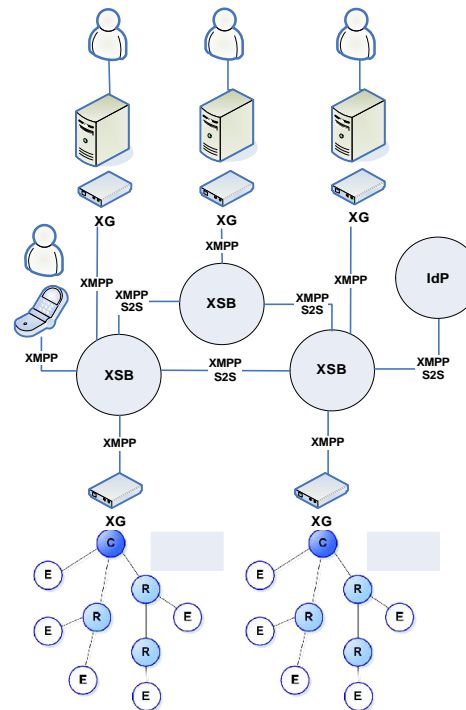
VPN SERVICE



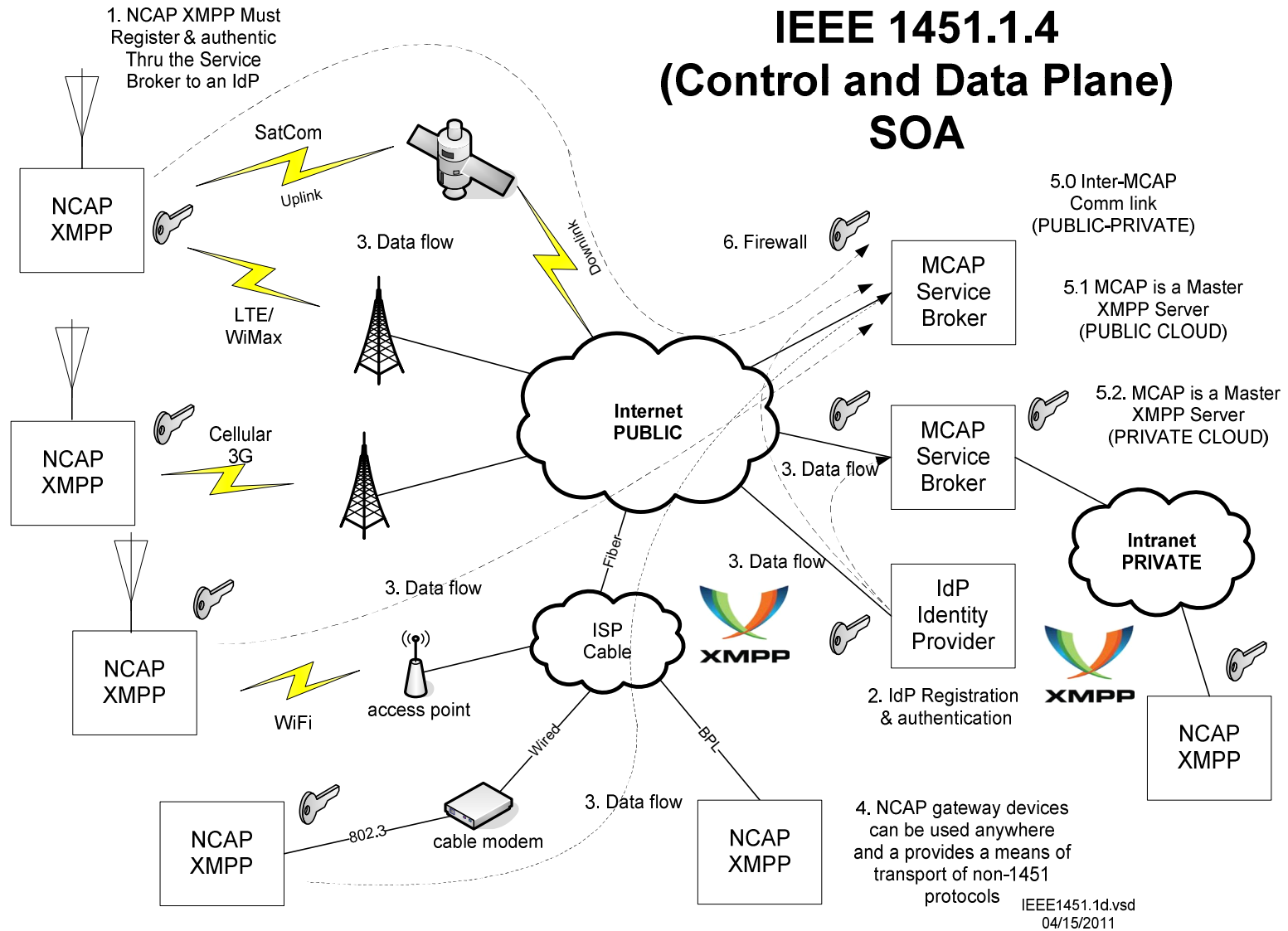
XMPP SERVICE



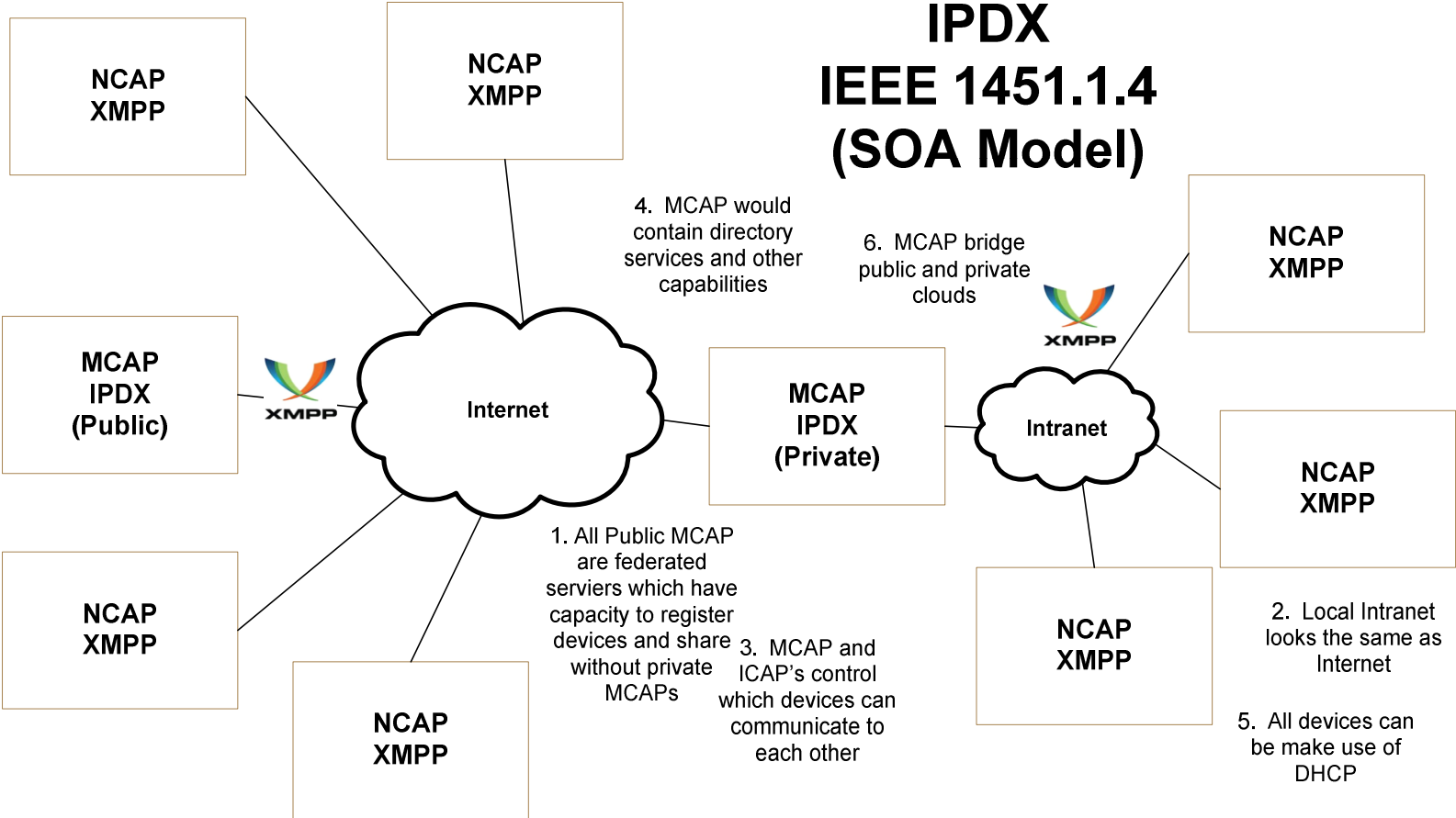
XMPP FEDERATED CLOUD SERVICE

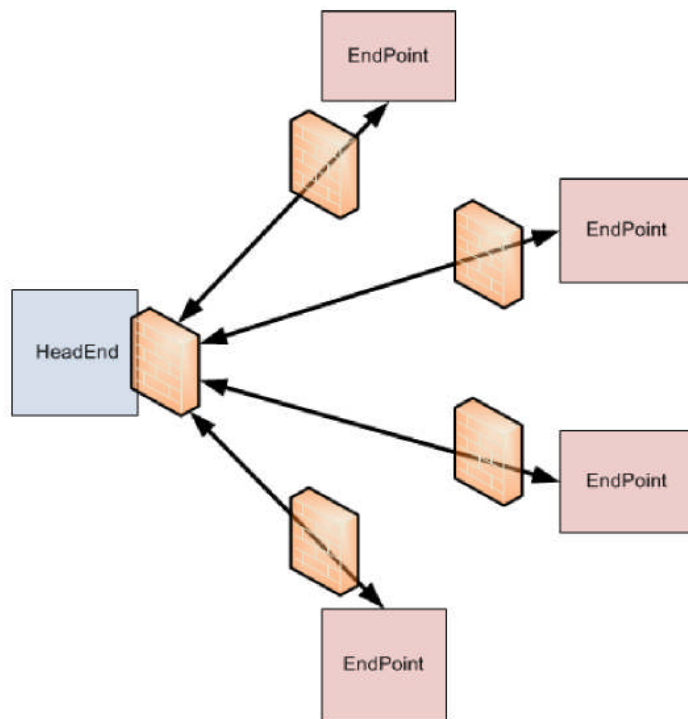


# IEEE 1451.1.4 (Control and Data Plane) SOA

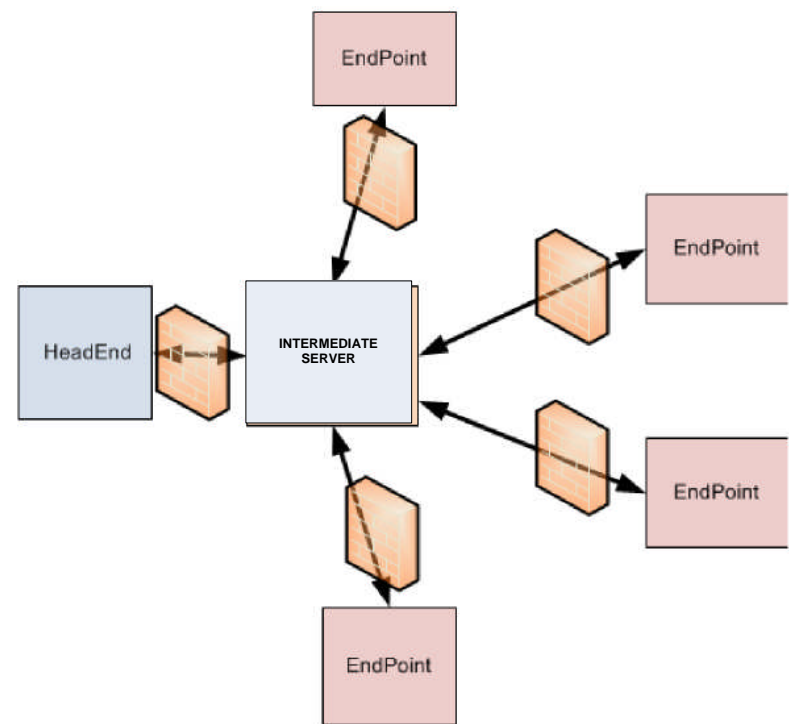


# IPDX IEEE 1451.1.4 (SOA Model)





**CENTRALIZED APPROACH** – The end points need to send their information to a central server and all functions must be handled by the root device. Data sharing must be from the headend. All end point devices are single thread permitting only one connection at a time.



**DECENTRALIZED APPROACH** includes a Server Broker between the end points using XMPP it will offer presence, registration, data sharing, etc. All nodes only have to contact a single root node but can fail-over to a secondary root node if it is available.

# Objective

- ISO/IEC/IEEE 21451-1-4 standard demonstrates assured interoperability, scalability, and security utilizing a common extensible protocol (XMPP) .

# Characteristic Requirements

1. Provide an ability to view remote sensors and control of actuators over any technology and provide maximum assurance of interoperability with built-in security
2. Provide registration of devices to recognize if a devices configuration has changed
3. Ensure that all data is encrypted between end points.
4. Provide presence capability to know that a device is available for use.
5. End device shall have the ability to instantly change an incoming protocol to XML
  - The XML shall be able to be mapped to any protocol
  - The XML may be used as the primary protocol
6. End devices are viewable by a web browser and can be viewed on mobile devices
7. There shall be a intermediary brokerage (Service Broker) between the end-point
8. Firewalls shall exist at all end-points
9. There shall be a profile that can identify the end devices
10. The interface shall be able to operate over any wired or wireless connection

# Advantages

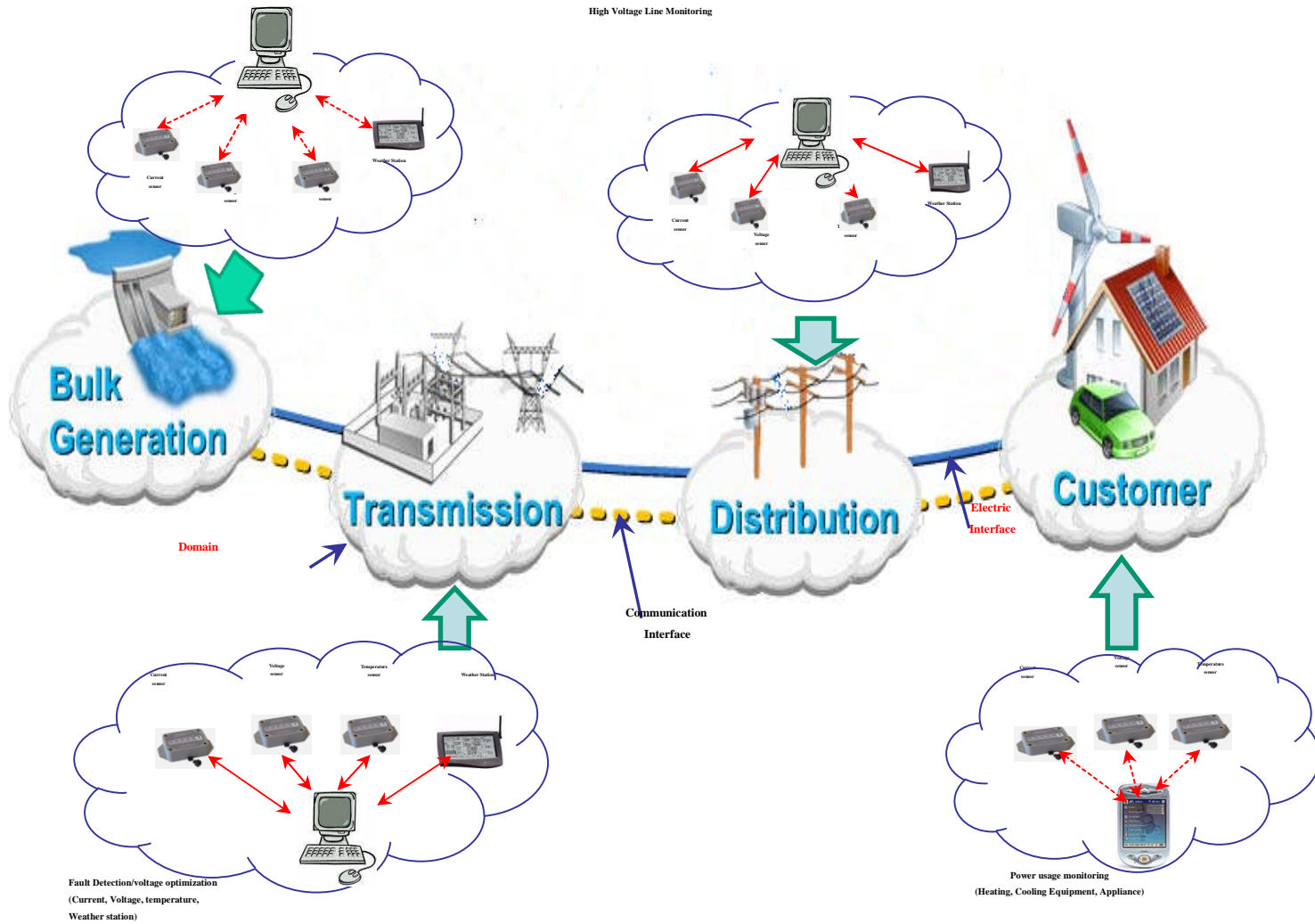
1. The brokerage isolates any end-point including devices, users, or applications.
2. All packets are checked at the end-point to defend against cyber-attack
3. Policy administration allow restriction of packet actions
4. Directory services can be offered including indication of presence
5. Provides a common way to manage devices that are registered
6. Integration of mobile devices and trusted data sharing

# Benefits

1. Applications, end-points, and users are not exposed to cyber-attack
2. All devices must be registered and can only talk to the Service Broker
3. End devices can be viewed by mobile devices such as Android
4. Packets are inspected during the transversion process
5. The device identity and use must be specified in a transducer profile
6. All devices, applications and users have an agreed trust relationship
7. The brokerage provides virtually unlimited scalability.

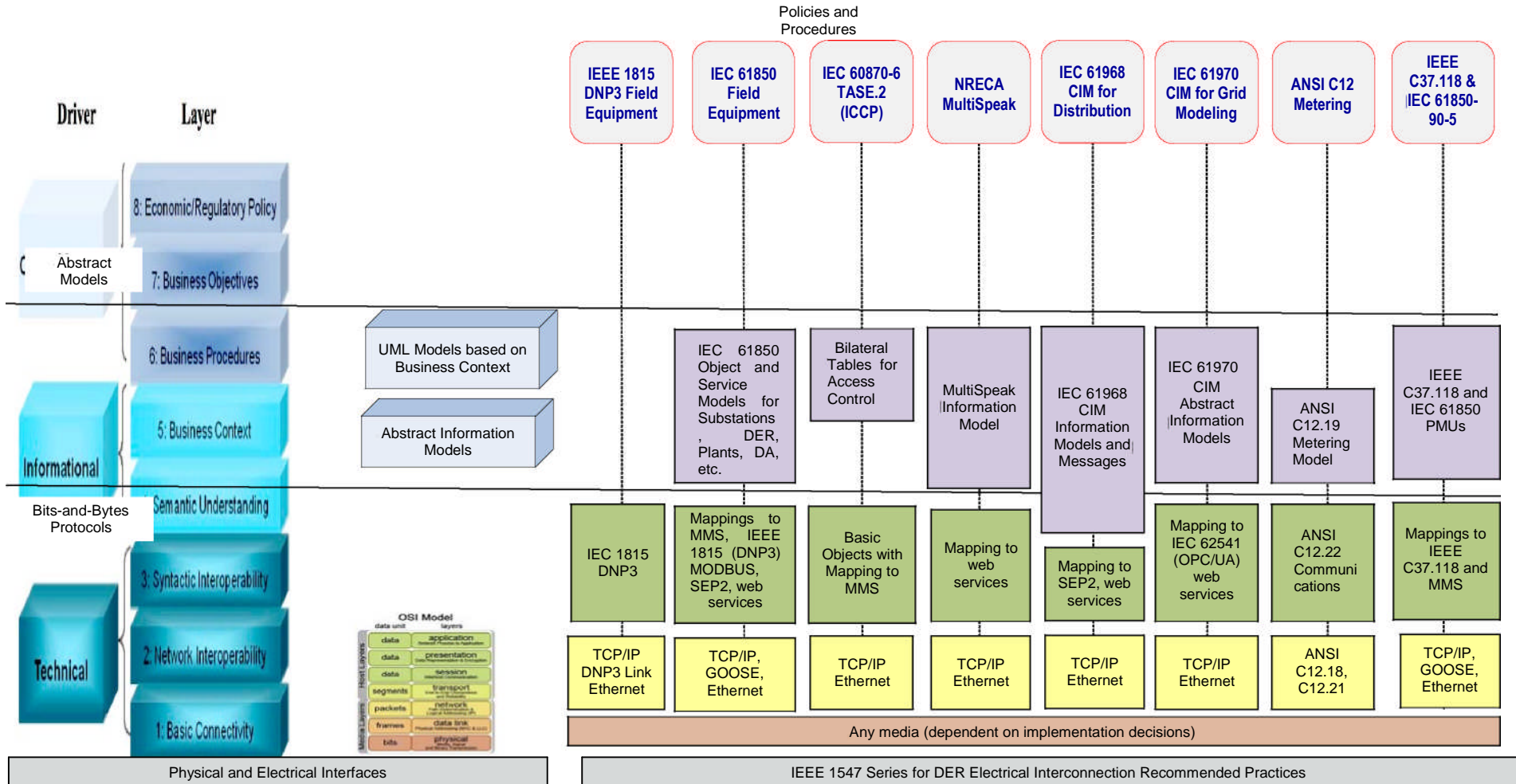


# Smart Grid



# Core Smart Grid Standards for Utilities

## GWAC Stack Core Smart Grid Standards for Utilities



Copyright 2012 - MaCT USA

# Areas of Concern

- Bulk Generation – renewable energy and storage systems
- Generation – data sharing increasing complexity including energy usage, fuel cost, & environmental compliance
- Transmission – line fault detection
- Distribution – Microgrid integration and tie-in of legacy substation controls
- Consumer – EMS, Smart Metering, and local generation/storage capabilities

# Key Technical Challenges

- New IEC standards such as 61850 will require high speed connections using fiber optic links, and 4G cellular.
- Legacy systems will take time to transition.
- Internet is not used effectively due to cyber-security concerns.

# Internet M2M

- Public networks like the Internet offer a point of entry for prospective cyber attacks and represents a burden on asset owners to manage the progressively complex paths of incoming and outgoing information.
- VPNs are used to provide Point-2-Point wired or wireless connections. However, the Smart Grid needs Point-2-Multipoint bi-directional communications and data sharing

# **XMPP: SG Use Cases**

- Power Line Fault Detection
- IEEE 1815.1 mapping to IEC 61850
- Renewable Energy
- Common Network Management
- Embedded Applications
- UCIDS CIM Integration

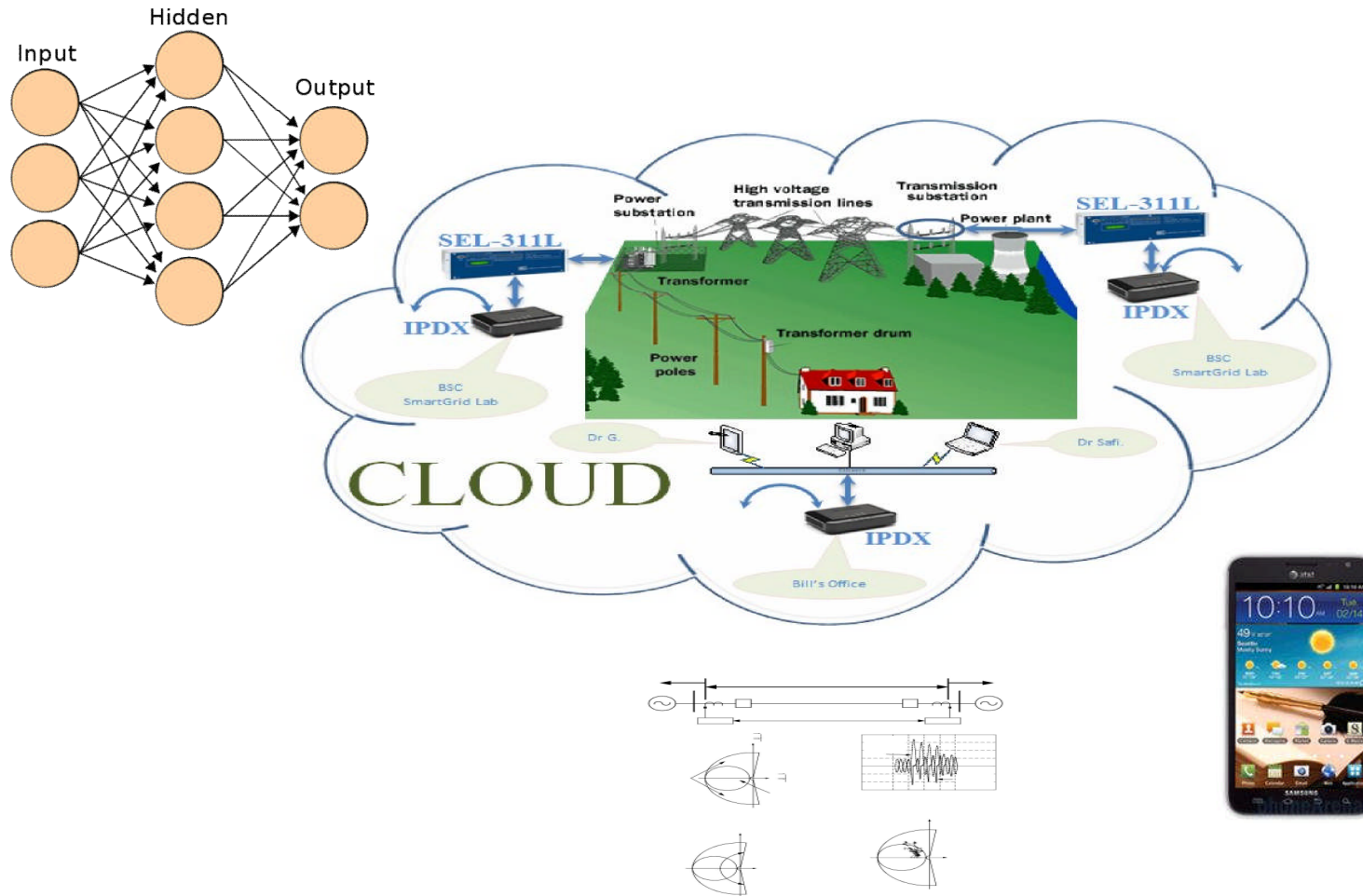
# **ARTIFICIAL NEURAL NETWORK (ANN) POWER LINE FAULT DETECTION**

Schneider Electric SEL-311L

University of Buffalo

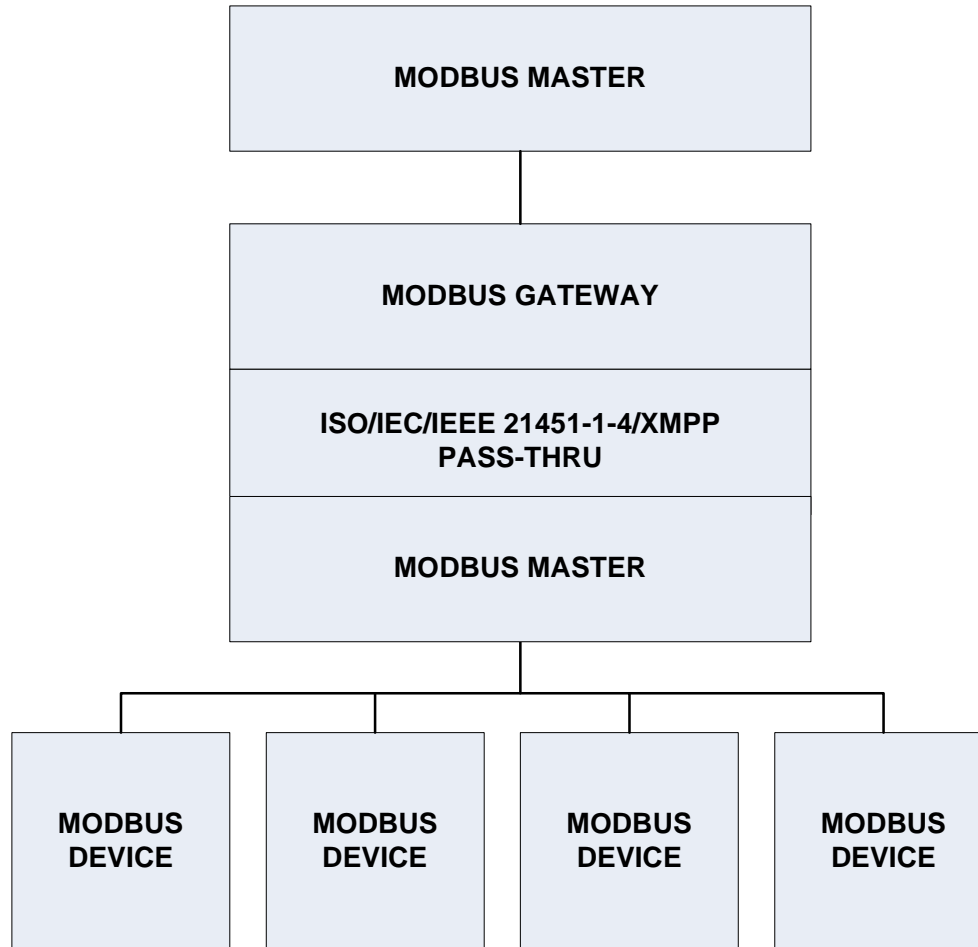
Buffalo State College

# Artificial Neural Network (ANN) Power Line Fault Detection



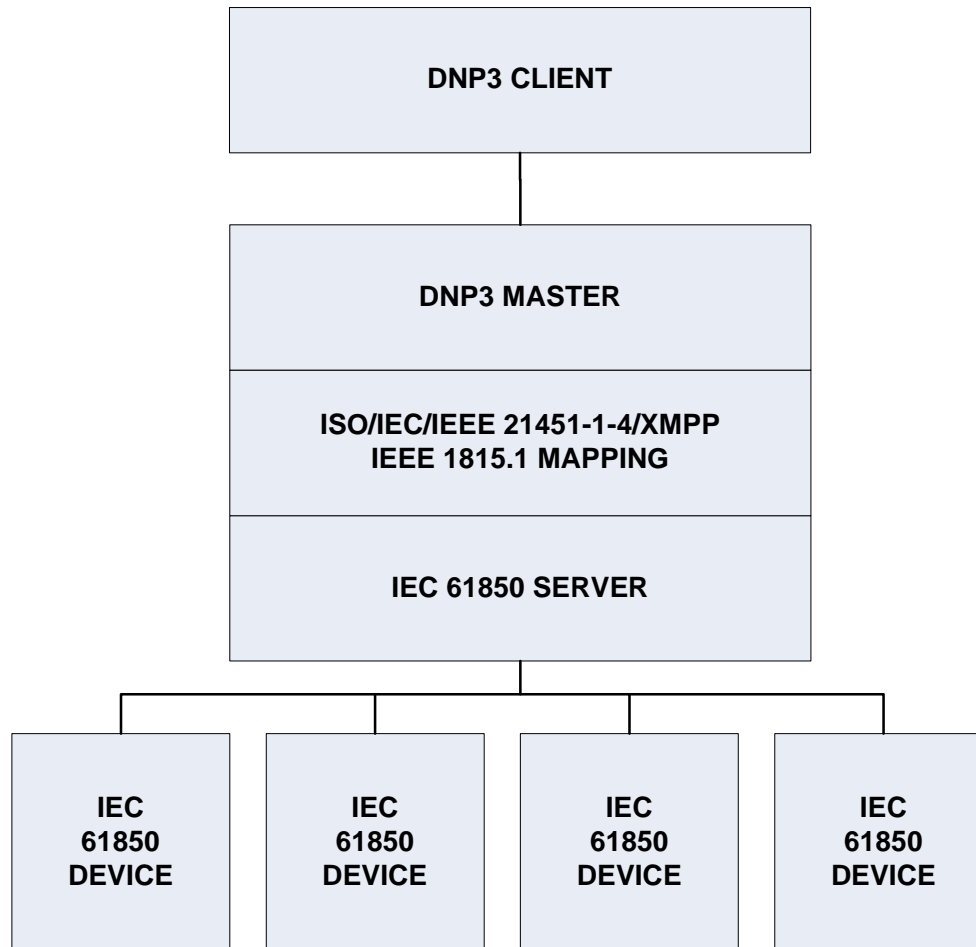


# MODBUS-XMPP-MODBUS

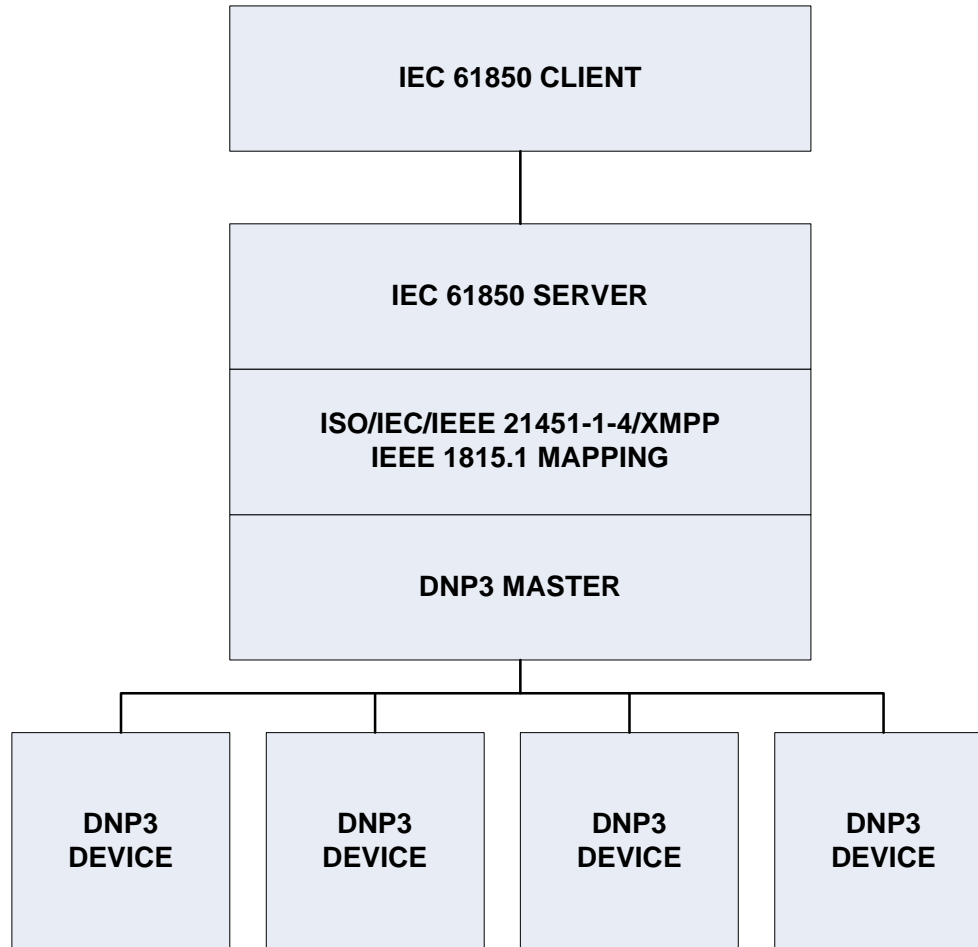


**IEEE 1815.1 (DNP3)  
MAPPING TO IEC 61850  
DEMAND RESPONSE**

# DNP3-XMPP-IEC 61850



# IEC 61850-XMPP-DNP3



# **RENEWABLE ENERGY**

## The Power Chain

Copyright 2012 - MaCT USA

# RENEWABLE ENERGY



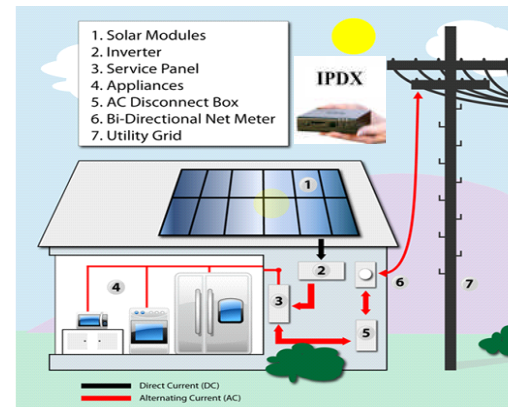
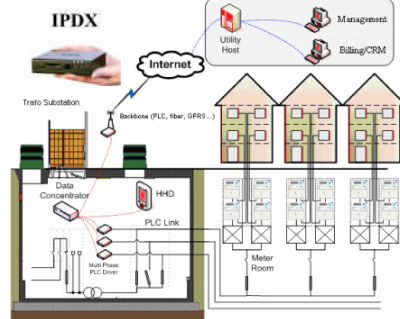
LARGE SCALE RENEWABLE ENERGY



MICROGRID AND SUBSTATIONS



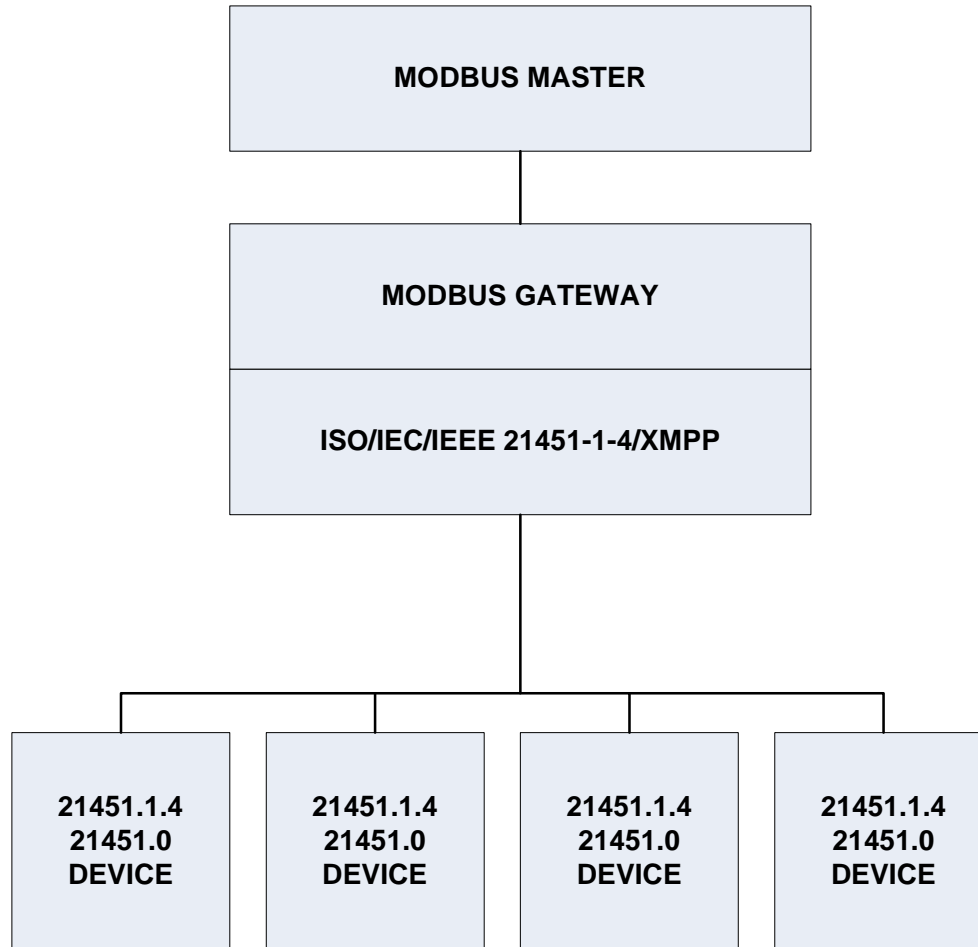
## Microgrid Automation Broadband over Power Lines (BPL)



# **EMBEDDED APPLICATIONS**

**IEEE 1451 DEVICES**  
**Internet of Things (IoT)**

# MODBUS-XMPP-IEC 21451

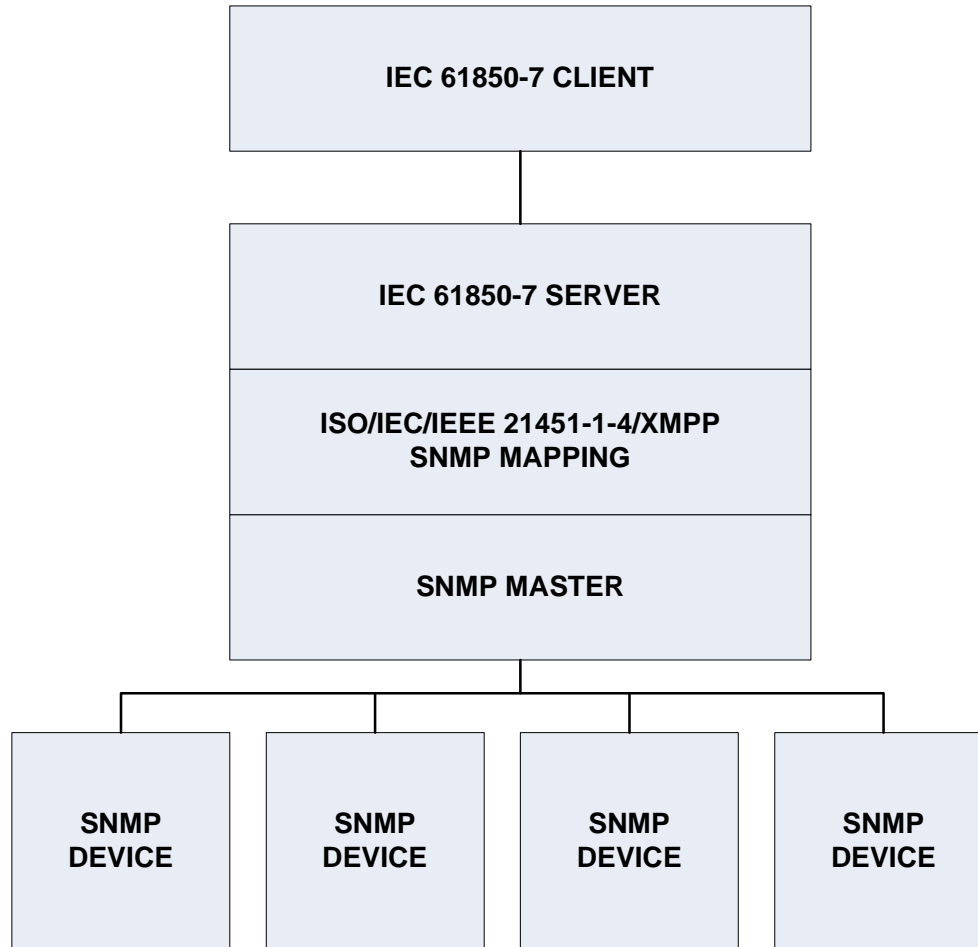




# **COMMON NETWORK MANAGEMENT**

IEC 61850-7  
SNMP over XMPP

# (IEC 61850-7)-XMPP-SNMP



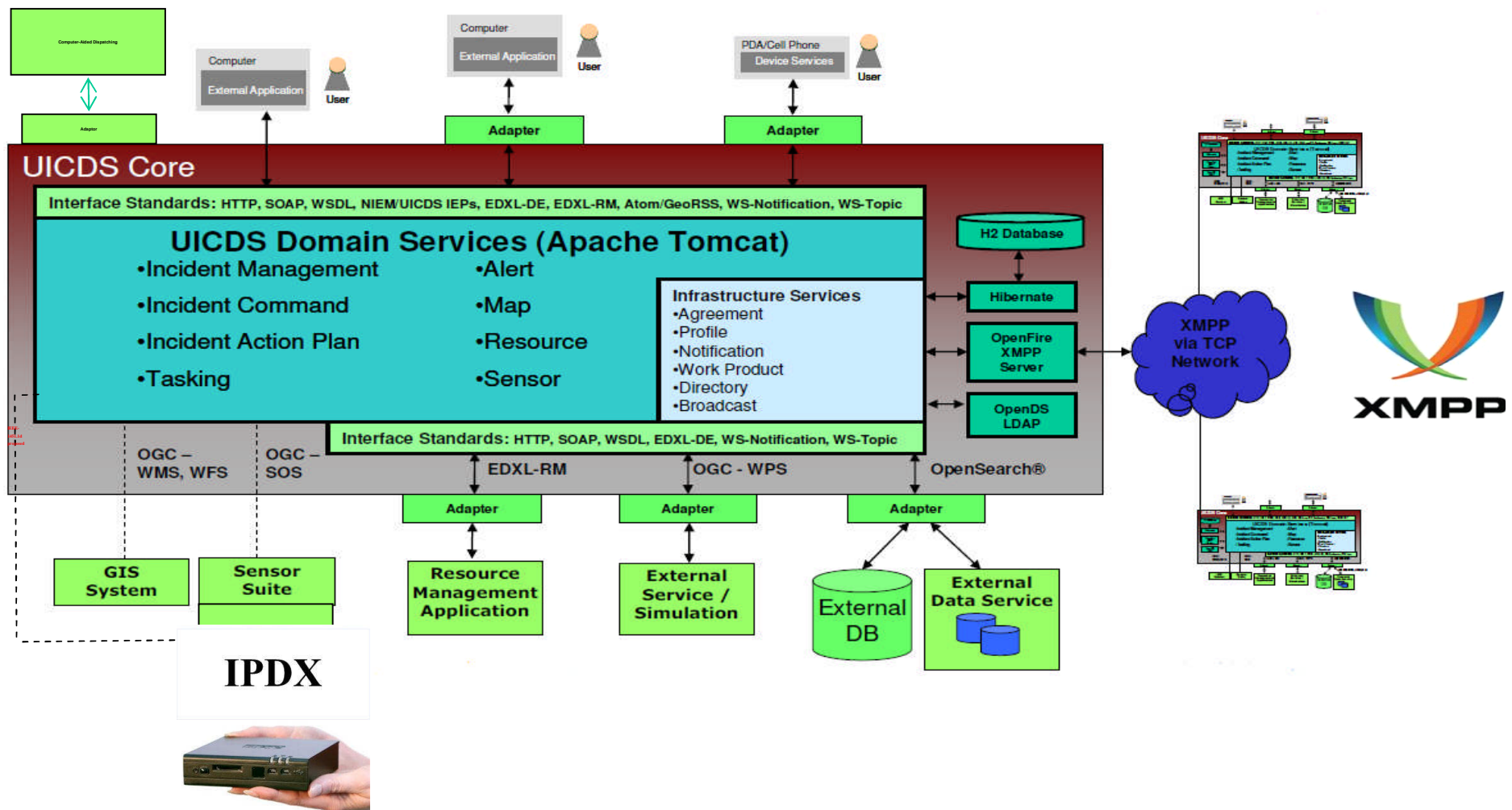
# **UICDS CIM Integration**

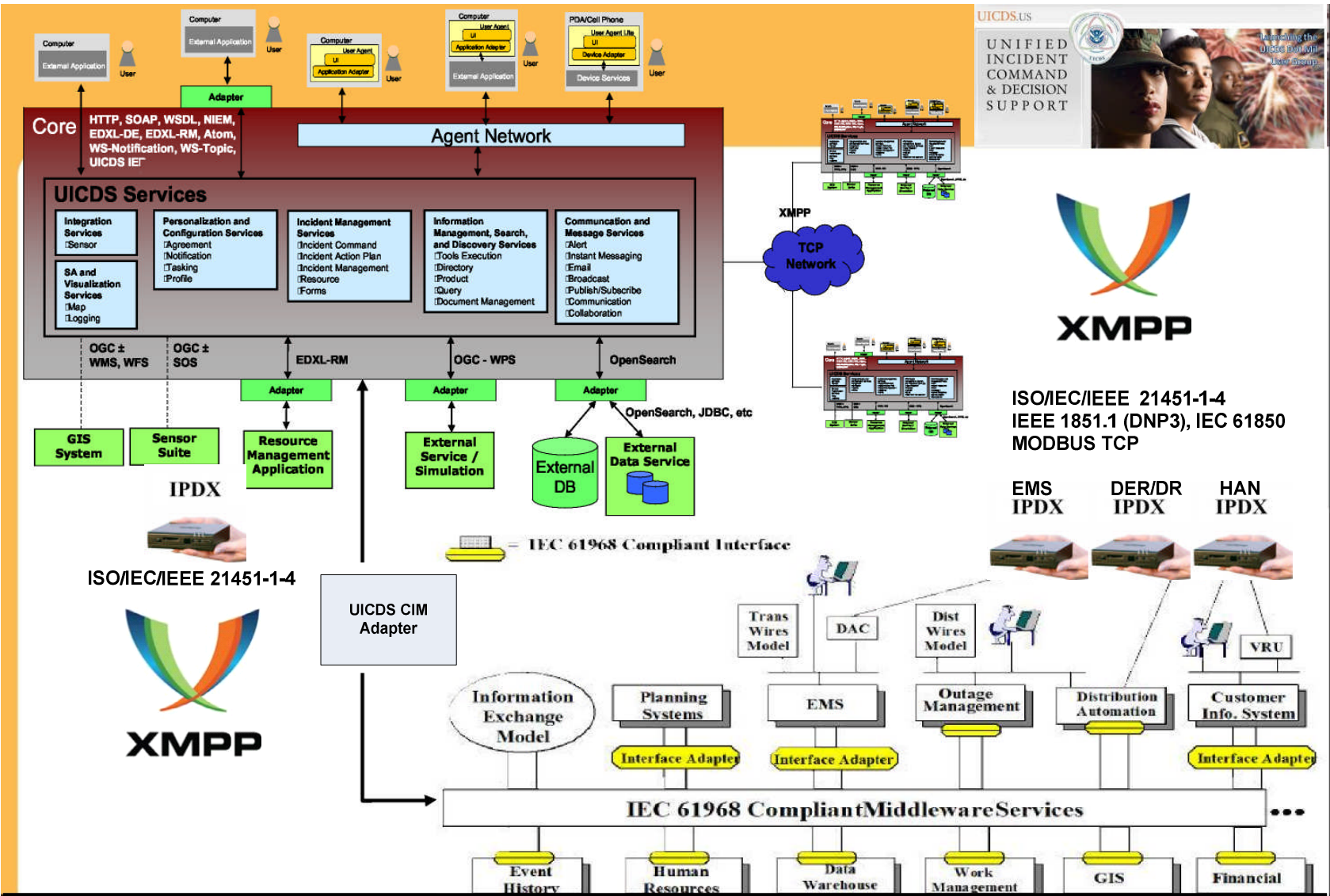
**Data Sharing**

**Learn more at**

**<http://www.uicds.us>**

# Unified Incident Command and Decision Support (UICDS) with IPDX Sensor Suite Integration





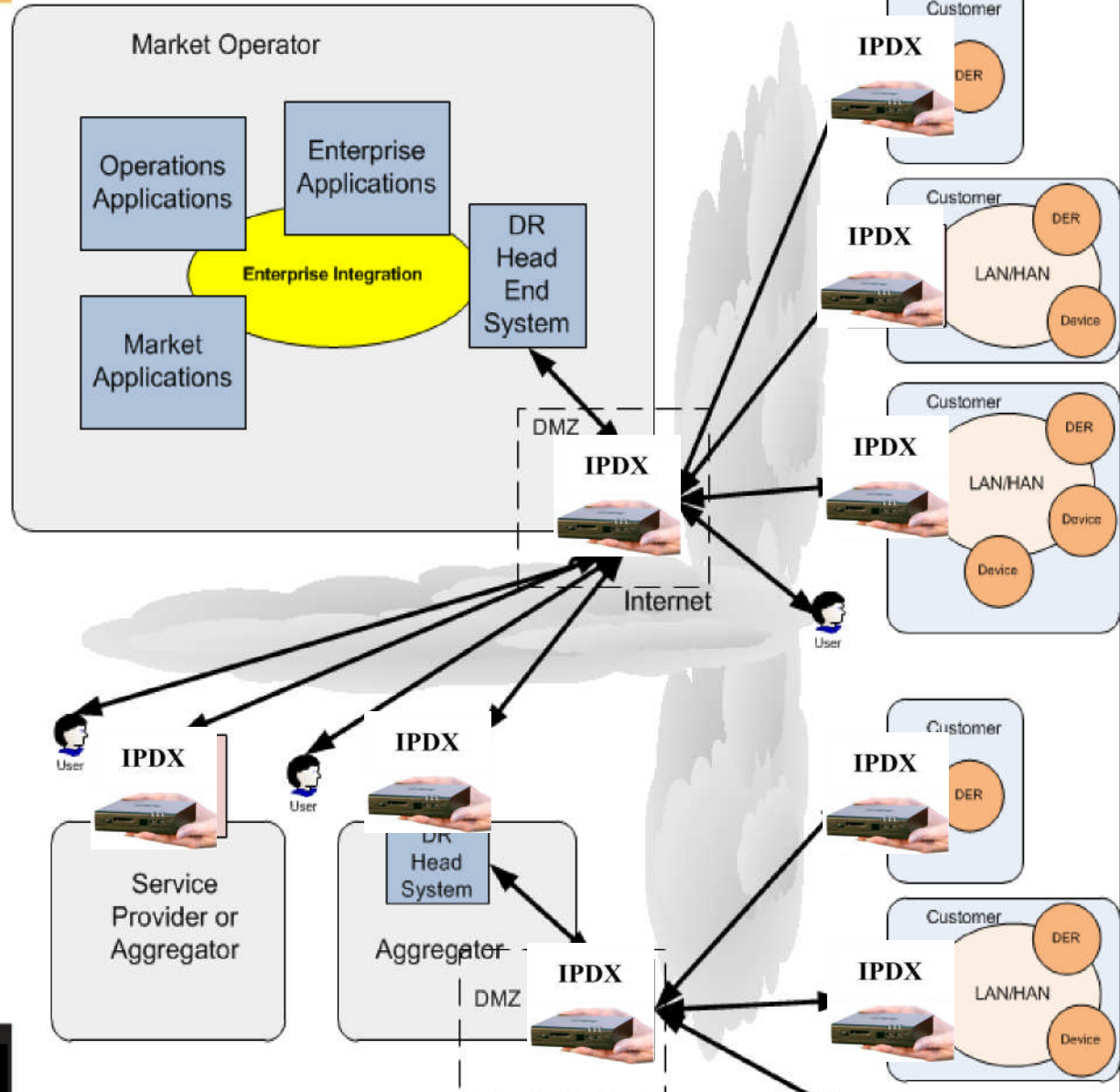
SG Educational Series Webinar  
July 16, 2012

Copyright 2012 - MaCT USA



ISO/IEC/IEEE  
21451-1-4

### CIM USE CASE



# Summary

- XMPP can be used at any level of the Smart Grid and is a key enabler as a common extensible protocol to harmonize operation between new and legacy protocols.
- XMPP is technology agnostic and protocol independent greatly reducing the complexity and cost.
- XMPP can leverage use of legacy devices and facilitate a transition to new IEC standards.
- XMPP offers messaging that can be trusted.
- XMPP is easy using dynamic addressing, built-in cyber protection without the complexity and cost yet using standards available today.
- XMPP can provide assured interoperability, scalability, and security.

**IPDX.NET**

Federated cloud sensor service  
based on use of XMPP

Coming Soon!



# IPDX UNIVERSE

## Collaborative Research Network

- ISO/IEC/IEEE 21451-1-4 is to provide session initiation and protocol transport for sensors, actuators, and devices. The standard addresses issues of security, scalability, and interoperability. This standard can provide significant cost savings and reduce complexity, leveraging current instrumentation and devices used in industry.



**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce



IPDX for Android  
brings XMPP power  
for mobile M2M  
sensor networks.

# Thank You

Questions?

Learn more at

<http://www.mact-usa.com>

Copyright 2012 - MaCT USA