IEEE International Conference on Smart Grid Engineering (SEGE'13)

28-30 August, 2013

UOIT, Oshawa, ON (Canada)

Sponsored by IEEE Toronto (NPSS & PES) and MITACS

Tutorial

(30-Aug-2013, 13:30-2:30pm)

XMPP, Big Data, and the Smart Grid

William J. Miller, President, MaCT

Sensei/IoT* XMPP

XMPP, Big Data, and the Smart Grid

ISO/IEC/IEEE P21451-1-4
eXtensible Markup and Presence Protocol Interface Standard for Sensors, Actuators, and Networked Devices for M2M and the Internet of Things (IoT)

WILLIAM J. MILLER
Chairman

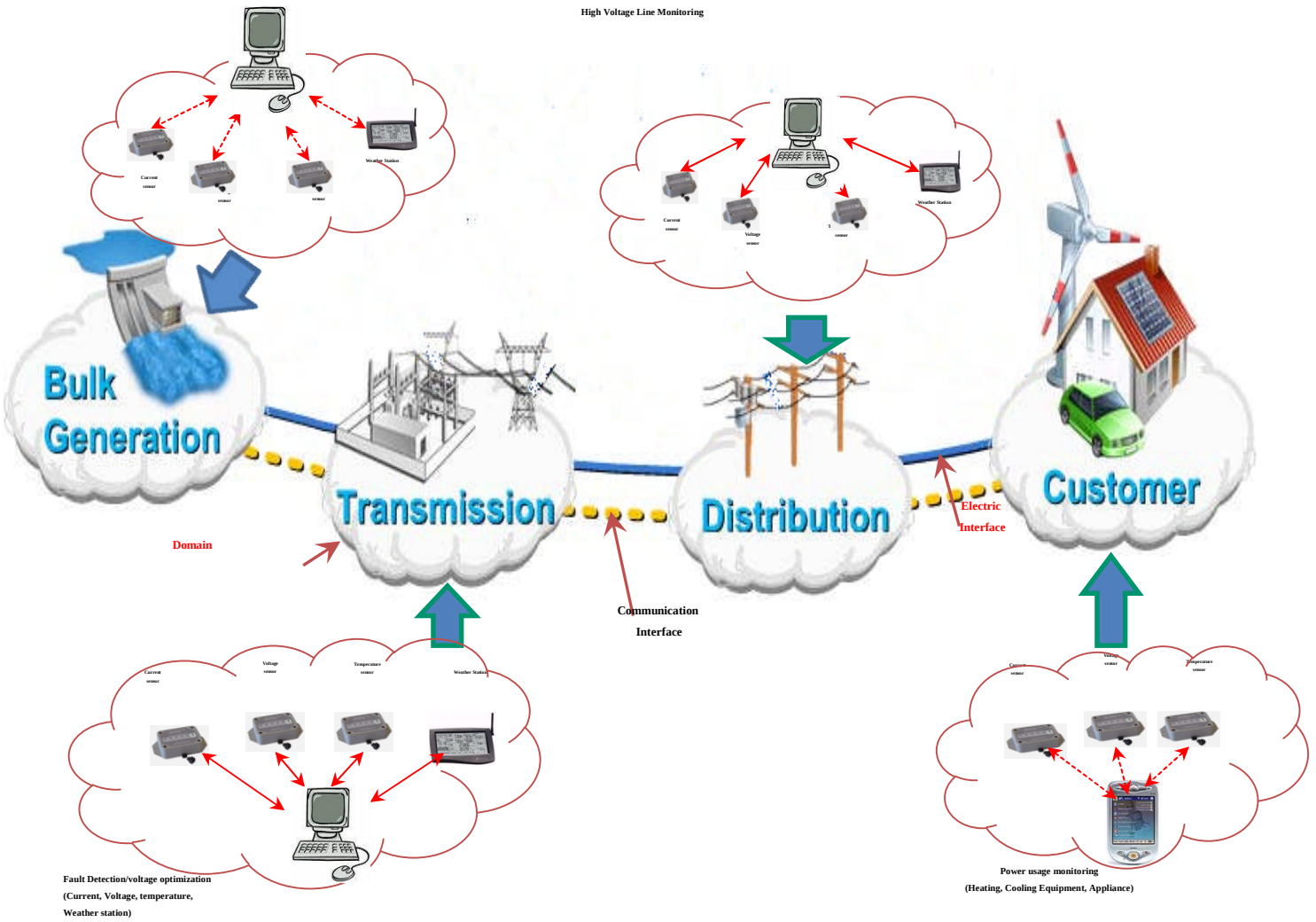
August 28-30, 2013

Agenda

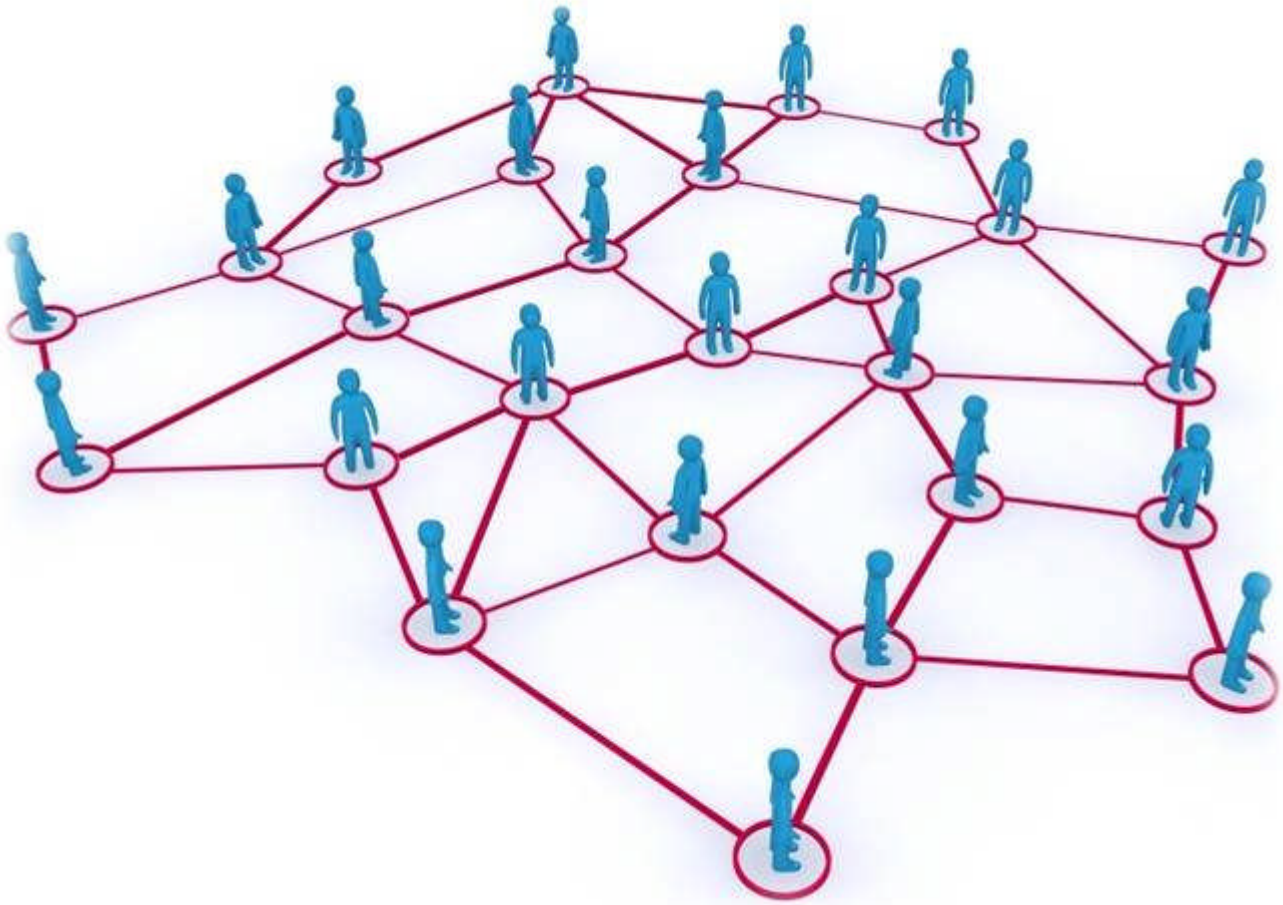
- Internet of Things (IoT)
- ISO/IEC/IEEE P21451-1-4 Sensei/Iot*
- Big Data for the Smart Grid
- Use Cases for the Smart Grid

Internet of Things (IoT)

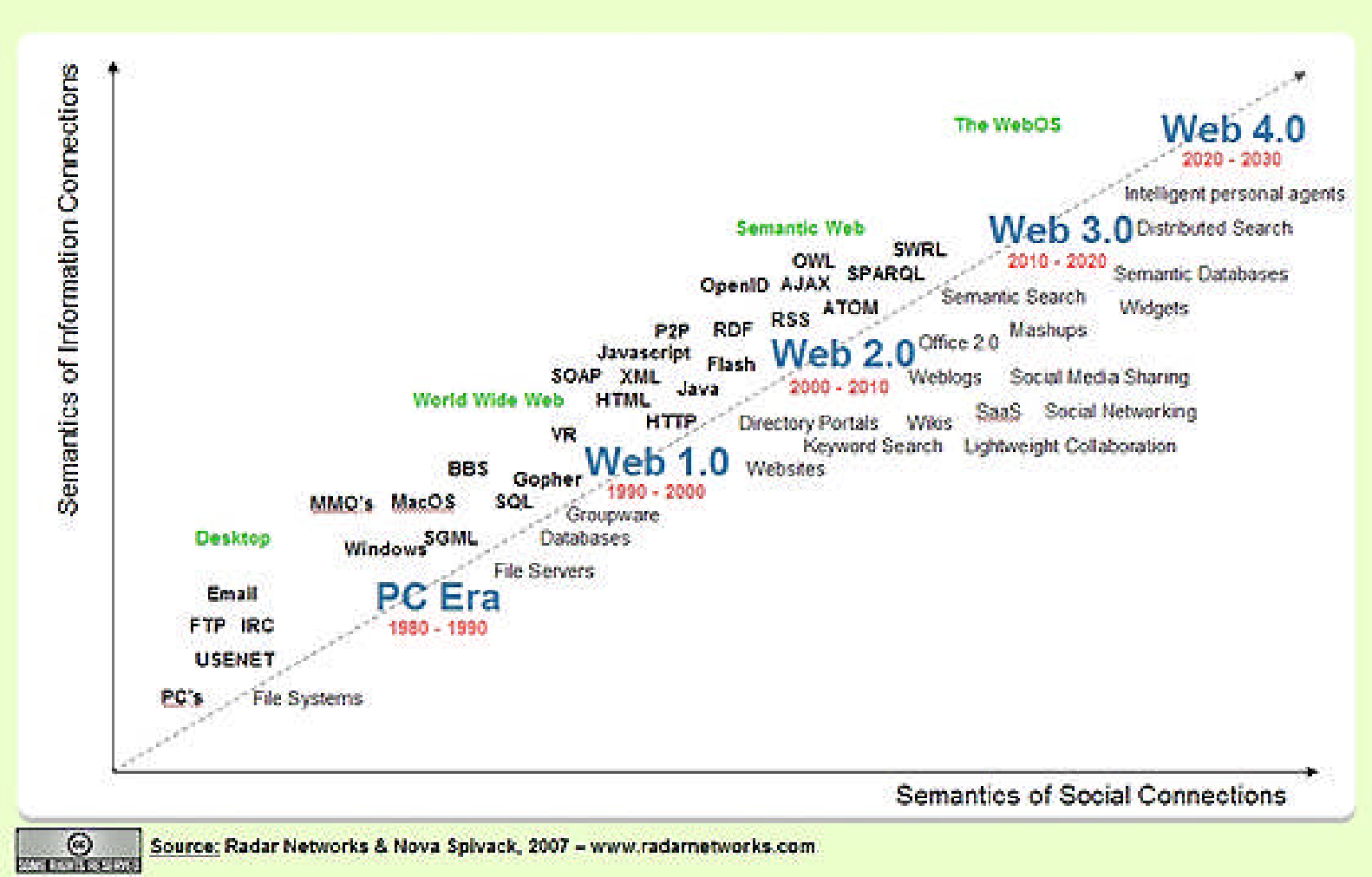
Smart Grid


Structure &
Equipment
Monitoring
High Voltage Line Monitoring
Bulk
Generation
Transmission
Distribution
Customer
Domain
Electric
Interface
Communication
Interface
Fault Detection/voltage optimization
(Current, Voltage, temperature,
Weather station)
Power usage monitoring
(Heating, Cooling Equipment, Appliance)

Social Networking Driving the Evolution of the Internet

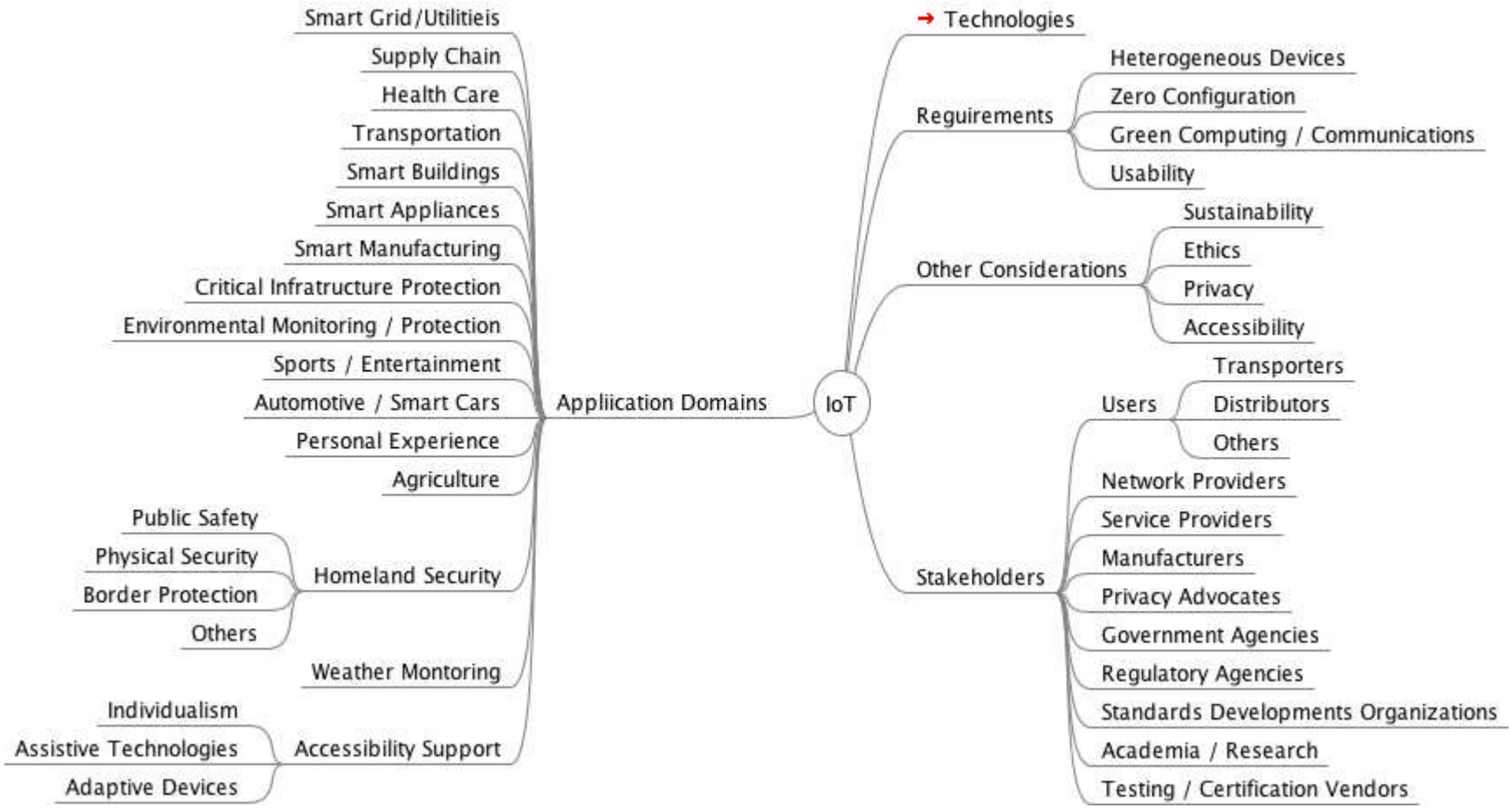


Semantic Web 3.0



Source: Radar Networks & Nova Spivack, 2007 – www.radarnetworks.com

IoT Mindmap


IoT
Technologies
Reguirements
Heterogeneous Devices
Zero Configuration
Green Computing / Communications
Usability
Other Considerations
Sustainability
Ethics
Privacy
Accessibility
Stakeholders
Users
Transporters
Distributors
Others
Network Providers
Service Providers
Manufacturers
Privacy Advocates
Government Agencies
Regulatory Agencies
Standards Developments Organizations
Academia / Research
Testing / Certification Vendors
Appliication Domains
Smart Grid/Utilitieis
Supply Chain
Health Care
Transportation
Smart Buildings
Smart Appliances
Smart Manufacturing
Critical Infratructure Protection
Environmental Monitoring / Protection
Sports / Entertainment
Automotive / Smart Cars
Personal Experience
Agriculture
Homeland Security
Public Safety
Physical Security
Border Protection
Others
Weather Montoring
Accessibility Support
Individualism
Assistive Technologies
Adaptive Devices

UNIVERAL UNIQUE IDENTIFIER

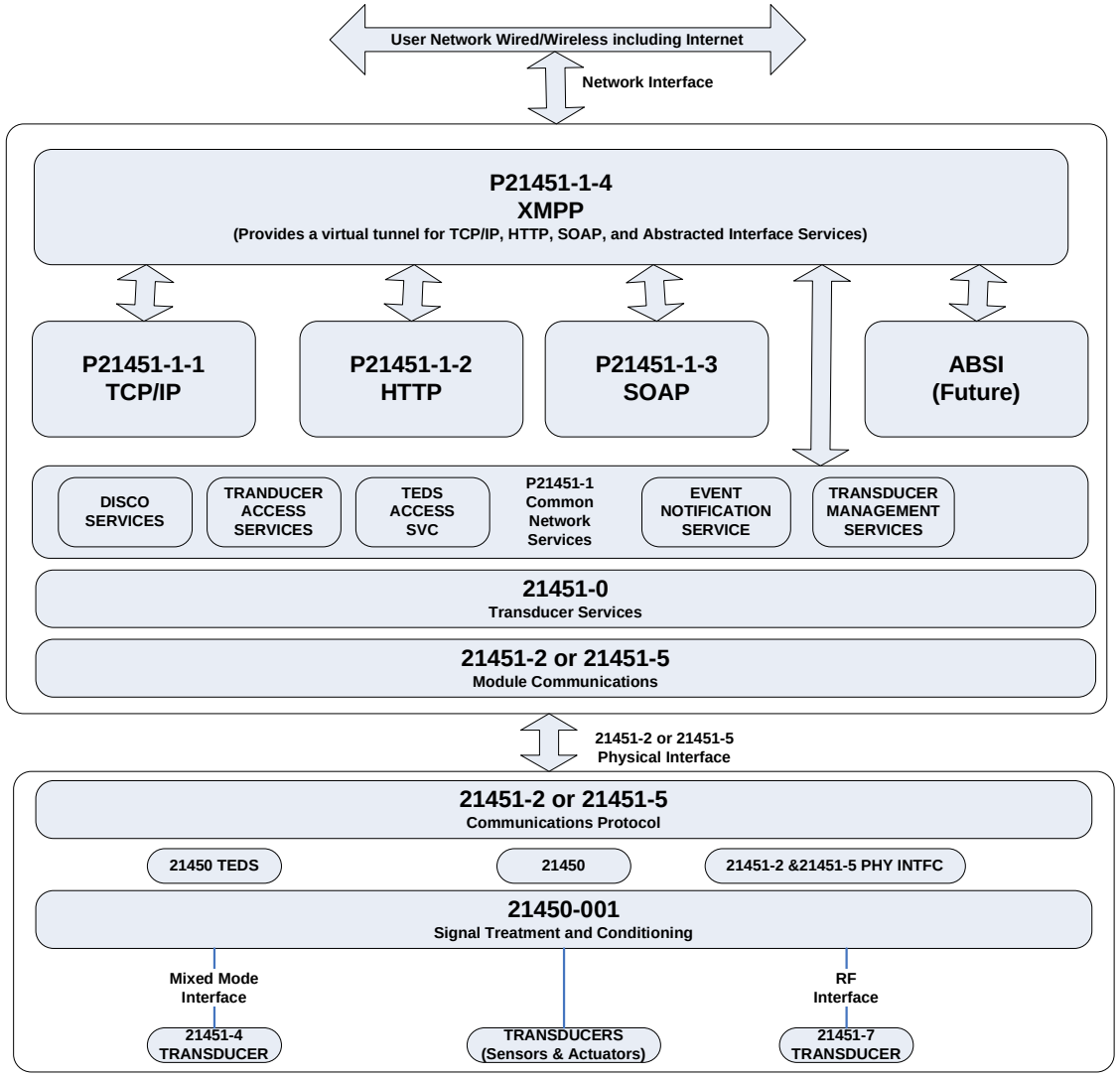
- **ISO/IEC/IEEE P21451-1-4** will use a JID (EUI-64) which is a Universal Unique IDentifier (UUID), defined in ISO 29161 Automatic Identification for the Internet of Things developed by ISO JTC1 SG31 WG2 Automatic Identification & Data Capture and TC122 Internet of Things (IoT).
- jid = [node “@”] domain [“/” resource {device}]

ISO/IEC/IEEE P21451-1-4
(Sensei/IoT*)

ISO/IEC/IEEE P21451-1-4

- *XMPP Interface Standard also known as "**Sensei/IoT***" is the first joint effort between ISO, IEC, and IEEE, known as P21451-1-4 XMPP Interface Standard for Sensor Networks, Machine-to-Machine (M2M), and the Internet of Things (IoT) as a first Semantic Web 3.0 Sensor Standard.*
- *Hosted by Dr. Kang Lee, Chairman of IEEE TC-9 Sensor Technology, and Craig Harmon Chairman of ISO JTC1/SC31 Automatic Identification/data capture and*

  TC122 Internet of Things



ISO/IEC/IEEE P21450
LOGICAL CONNECTION DIAGRAM

NCAP/TIM

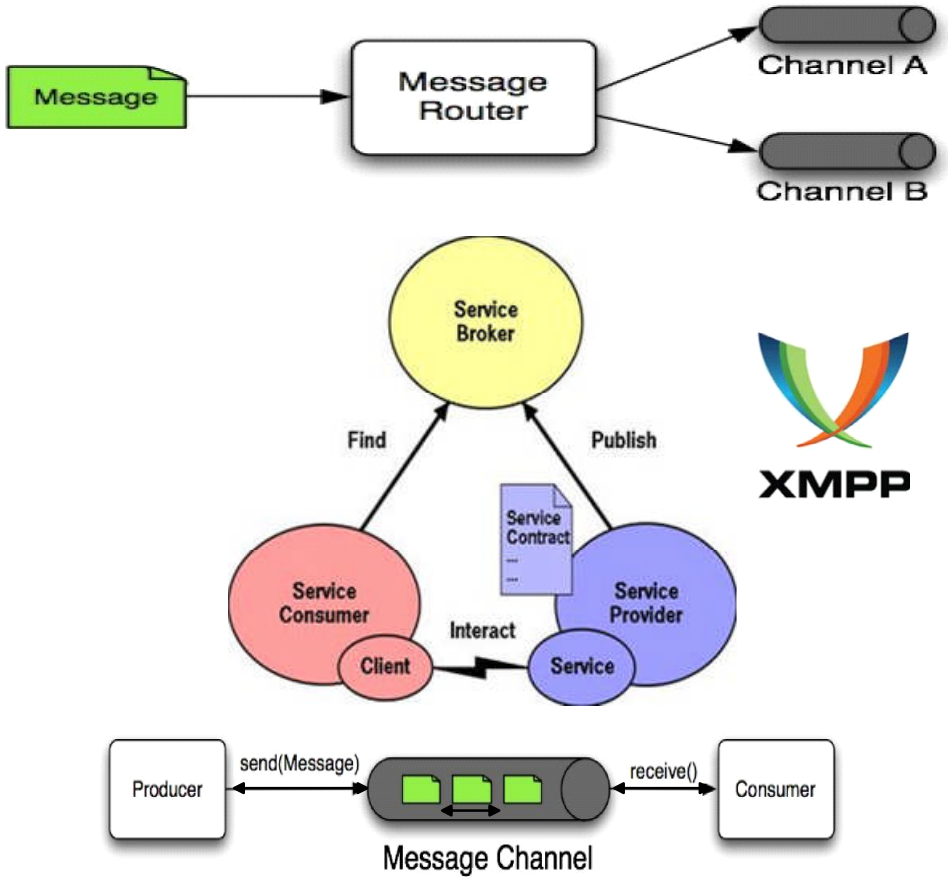
What is XMPP?

- **XMPP Standards Foundation** (**XSF**) is the foundation in charge of the standardization of the protocol known as extensions of eXtensibile Messaging and Presence Protocol (XMPP), the open standard of instant messaging and presence of the IETF.

IETF XMPP

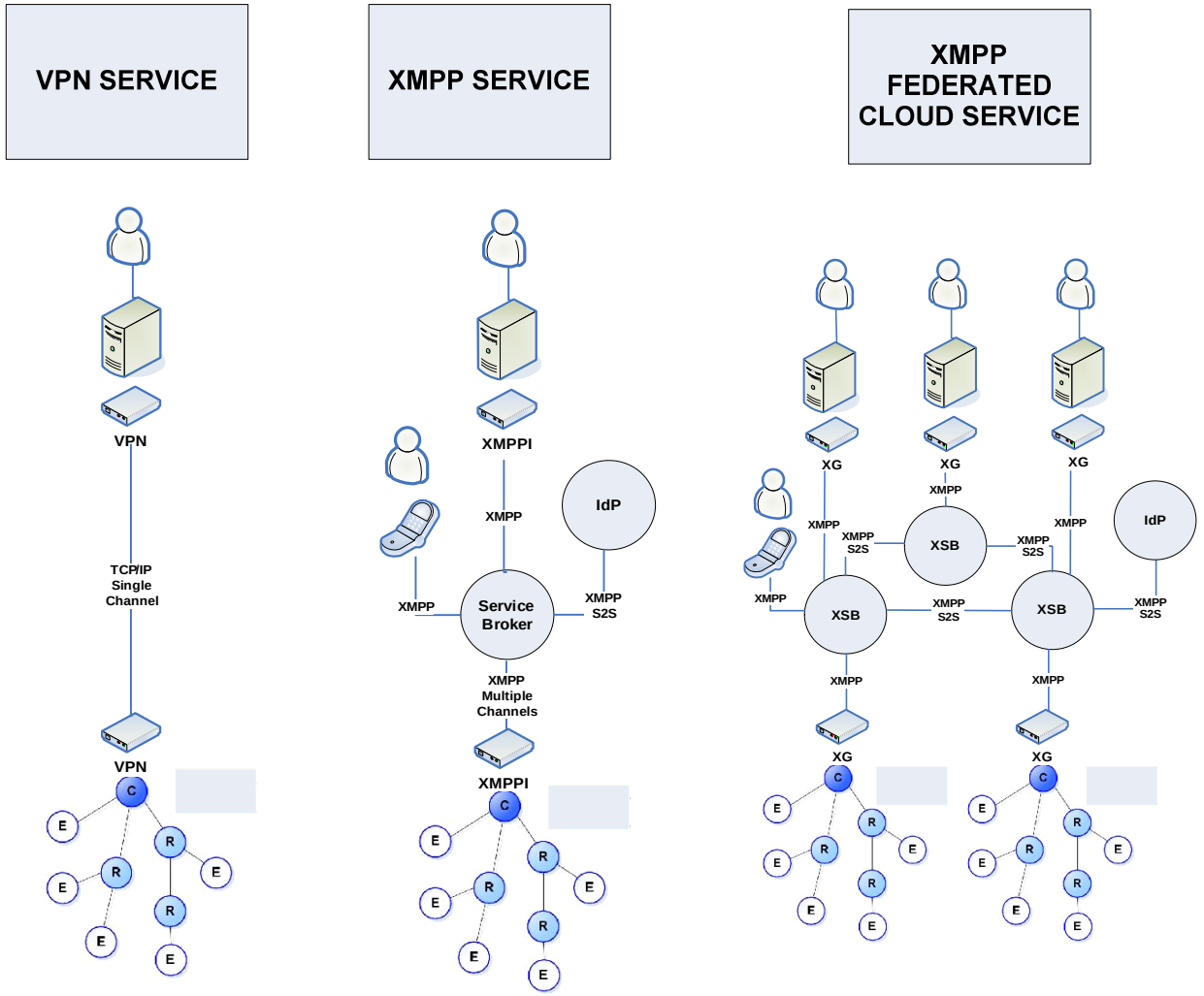
- IETF XMPP Working Group produced a number of documents:
- RFC 3920 – XMPP: Core, which describes client-server messaging using two open-ended XML streams. A connection is authenticated with Simple Authentication and Security Layer (SASL) and encrypted Transport Layer Security (TLS).
- RFC 3921 – XMPP: 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

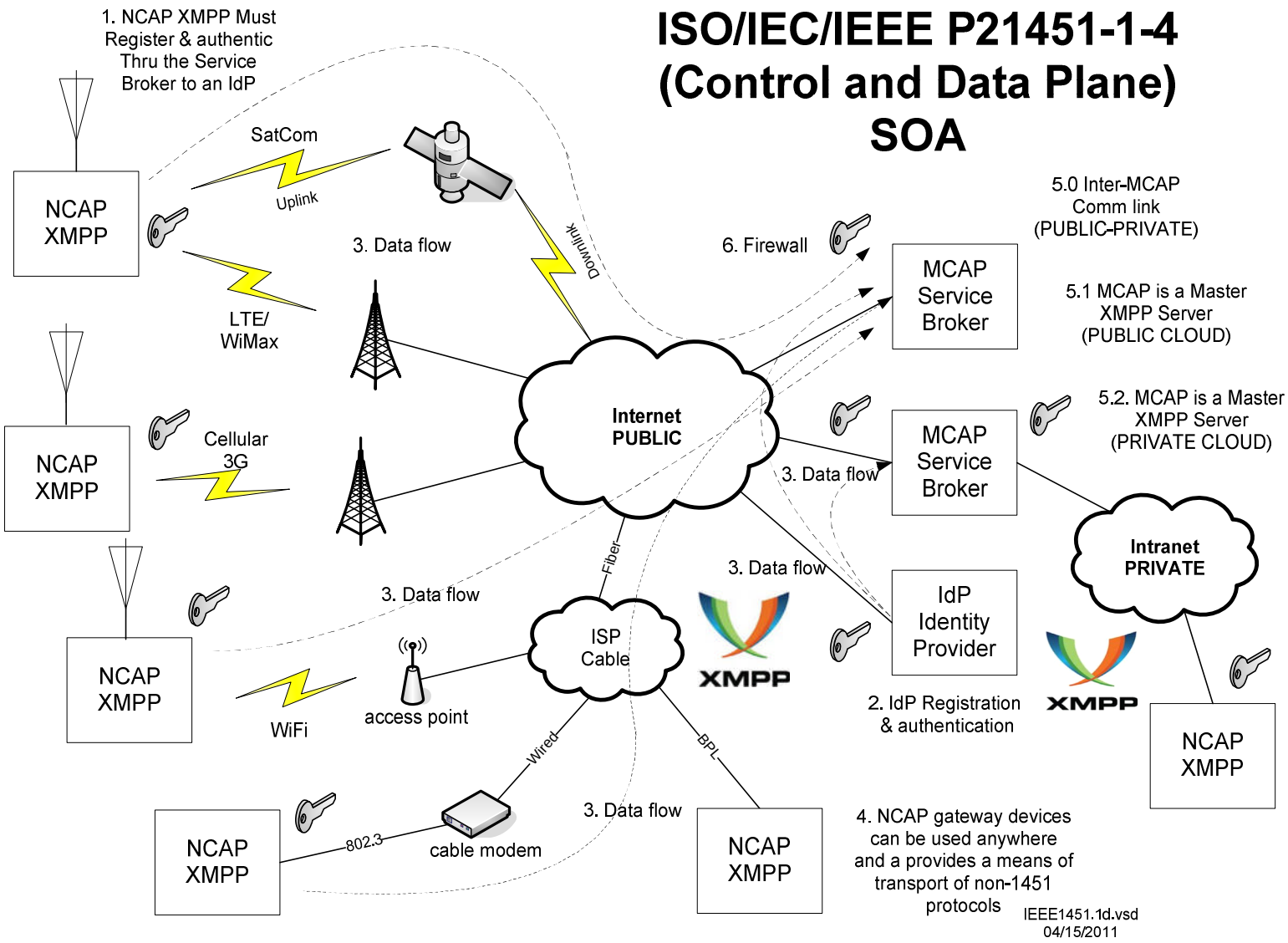
Service Oriented Architecture (SOA) Concept



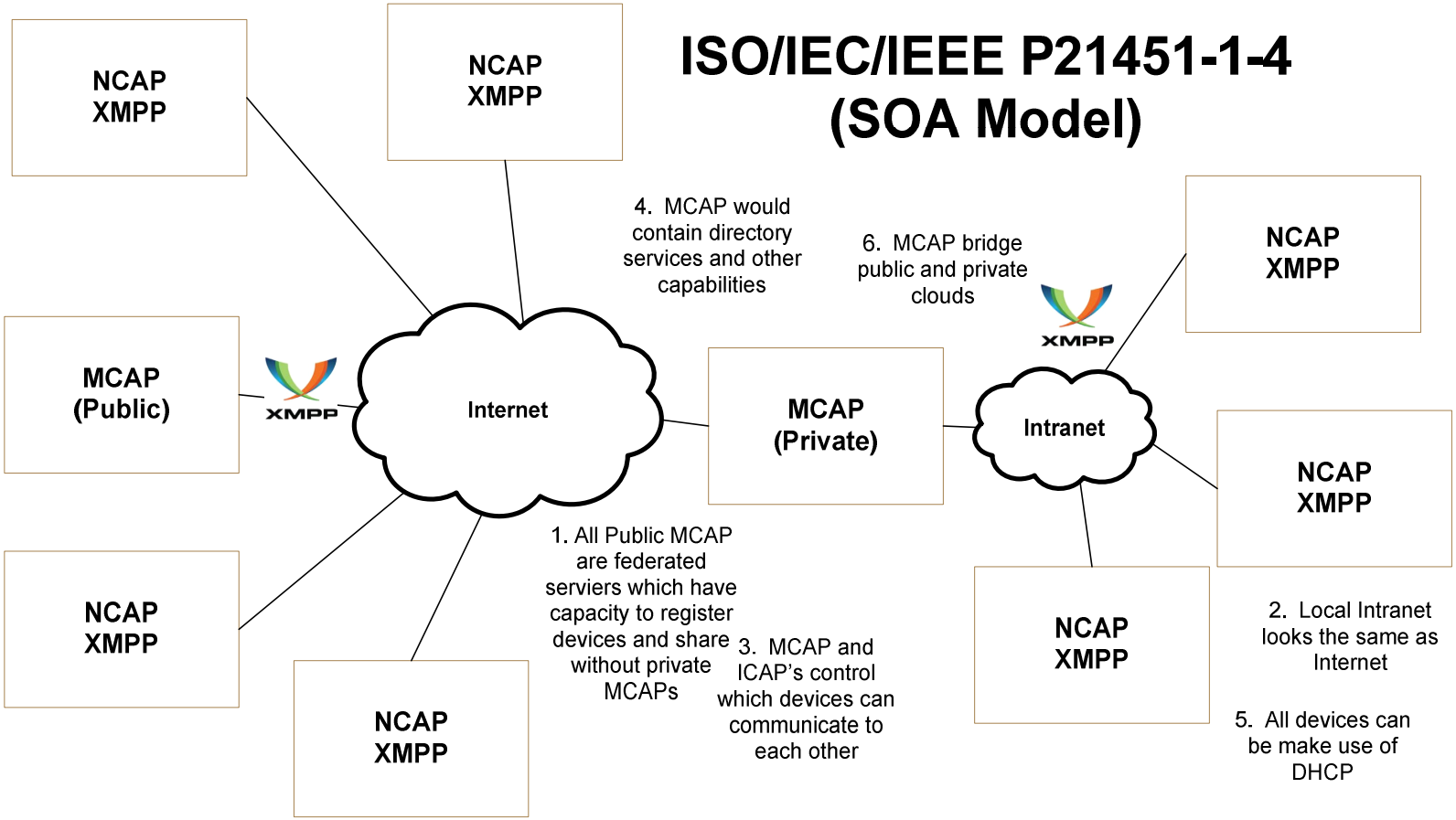
Scalability of

Cloud Services




ISO/IEC/IEEE P21451-1-4
(Control and Data Plane)
SOA
1. NCAP XMPP Must Register & authentic Thru the Service Broker to an IdP
NCAP XMPP
SatCom
Uplink
Downlink
3. Data flow
LTE/ WiMax
Cellular 3G
Internet PUBLIC
6. Firewall
5.0 Inter-MCAP Comm link (PUBLIC-PRIVATE)
MCAP Service Broker
5.1 MCAP is a Master XMPP Server (PUBLIC CLOUD)
5.2. MCAP is a Master XMPP Server (PRIVATE CLOUD)
Intranet PRIVATE
IdP Identity Provider
2. IdP Registration & authentication
XMPP
Fiber
ISP Cable
WiFi
access point
Wired
BPL
802.3
cable modem
4. NCAP gateway devices can be used anywhere and a provides a means of transport of non-1451 protocols
IEEE1451.1d.vsd
04/15/2011

ISO/IEC/IEEE P21451-1-4 (SOA Model)

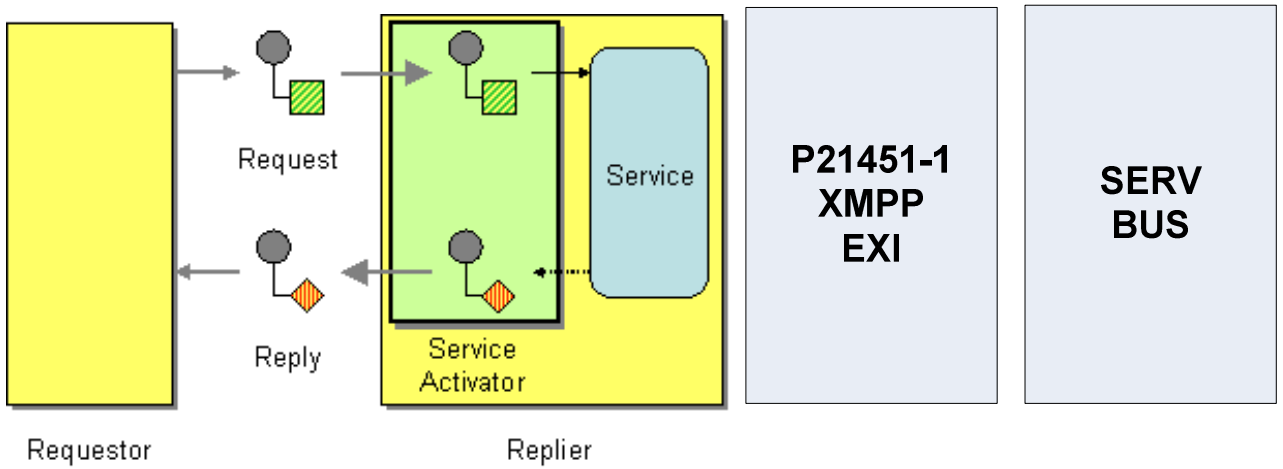


P21451-1-4
Abstracted Services

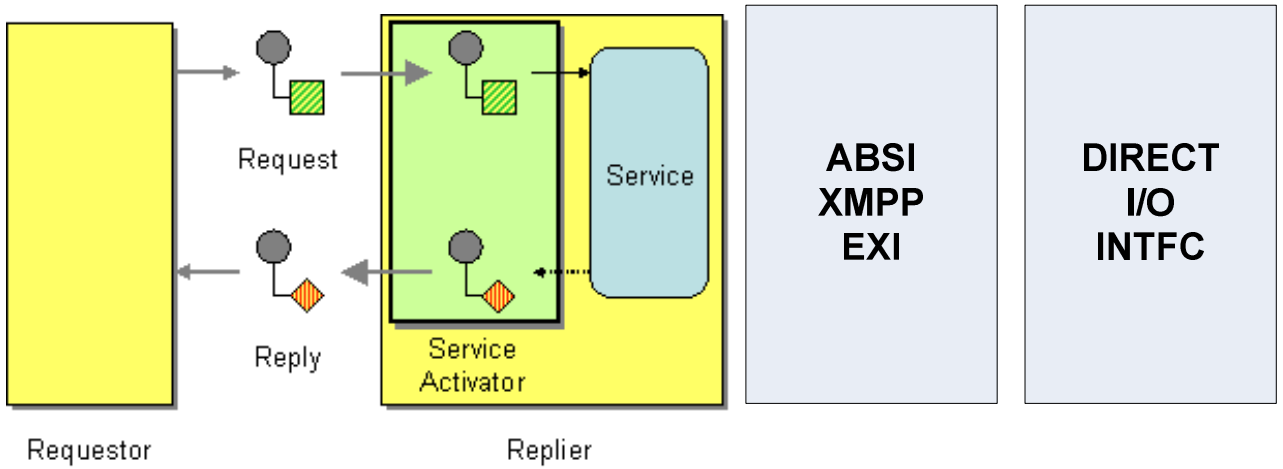
XMPP IoT Abstraction Types

- Gateway (P21451-1 over XMPP)
- Direct I/O (XMPP)
- Legacy Device Adapters (MODBUS over XMPP)
- Server-to-Server (OPC UA over XMPP)

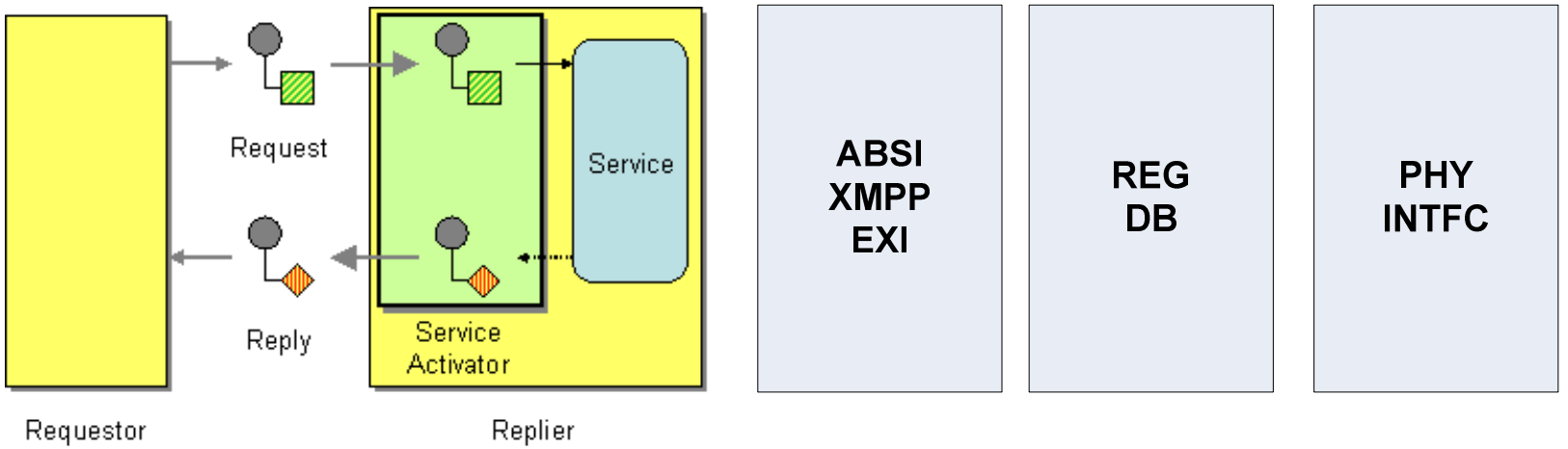
P21451-1-4 XMPP ABSTRACTED SERVICE 1



P21451-1-4 XMPP ABSTRACTED SERVICE 2



P21451-1-4 XMPP ABSTRACTED SERVICE 3



P21451-1-4
Requests/Responses

Discovery

Nodes, Resources, and Interfaces

NCAP/TIM Discovery (Request)

- The MCAP asks for a list of NCAP/TIM Resources with this message}
- • <**iq type**=’get’
- • from=’requester@example.org’
  to=’responder@example.org’
  id=’info1>
  <**query** xmlns=’https://jabber.org/protocol/disco#info>
  <**identity** category’gateway’ type=’ncap name=’ncapid’/>
  <**feature var**=’urn:xmpp:iot:interoperability'/>
  <**feature var**=’urn:xmpp:iot:sensordata'/
  <**feature var**=’http://jabber.org/protocol/disco#info’/>
  <**feature var**=’http://jabber.org/protocol/disco#items’/>
  <**identity**>
  </guery>
  </iq>

NCAP/TIM Discovery (Response)

- The NCAP/TIM provides the following response message
- <**iq type**=’result’
- from=’responder@example.org’
- to=’requester@example.org’
- <**accepted** xmins=‘urn:xmpp:iot:interoperability'
- <**accepted** xmins='urn:xmpp:iot:sensordata'
- <**iq type**

Getinterfaces (Request)

- <**iq type**='get'
  from=’requester@example.org’
- to=’responder@example.org
- id='1'>
  <**getInterfaces** xmlns='urn:xmpp:sn:interoperability'/>
  </**iq**>

Getinterfaces (Response)

- <**getInterfacesResponse** xmlns='urn:xmpp:sn:interoperability' >
- • <interface name='XMPP.IoT.Sensor.Temperature'/>
- • <interface name='XMPP.IoT.Sensor.Temperature.History'/>
  <interface name='XMPP.IoT.Identity.Clock'/>
  <interface name='XMPP.IoT.Identity.Location'/>
  <interface name='XMPP.IoT.Identity.Manufacturer'/>
  <interface name='XMPP.IoT.Identity.Name'/>
  <interface name='XMPP.IoT.Identity.Version'/>
  </**getInterfacesResponse**>
  </**iq**>

SensorData (Request)

- If you have interface XMPP.IoT.Identity.* (ID for NCAPs), read that data using XEP sensor-data (for instance read identity information only)
- <**iq type**='get‘

  from=’requester@example.org’

  to=’responder@example.org’ >

  id='1'>

  <**req xmlns**='urn:xmpp:iot:sensordata' seqnr='1' identity='true'/>

  </**iq**>

Sensordata (Response)

- <**message**
  from=’responder@example.org’
  to=’requester@example.org’ >
  <**fields** xmlns='urn:xmpp:iot:sensordata' seqnr='1' done='true**'>**
  <node nodeId=‘Device01'>
  <timestamp value='2013-03-07T16:24:30'>
  <string name='...ID' identity='true' automaticReadout='true' value='1234567'/>
  </timestamp>
  </node>
  </fields>
  </message>

  If not concentrator: Done

New URI

- HTTP over XMPP and EXI will be used to transport HTTP traffic utilizing a new URI.
- Ex. httpx://www.xmpp.org
- HTTPX will establish a secure XMPP session with a Service Broker where a device, application, or user can exchange information with anyone who is registered and authorized to share their information.
- Ref. XEP-0332

BIG DATA for Smart Grid

What is it? How is it used?

Big Data Definition

- ***Big Data*** *refers to digital data volume, velocity and/or variety [veracity] that: enable novel approaches to frontier questions previously inaccessible or impractical using current or conventional methods; and/or exceed the capacity or capability of current or conventional methods and systems.*

Big Data Characteristics

- HADOOP MapReduce breaks up a task into smaller tasks and being able to act upon a large data set to provide data collection, data analytics, visualization, and logistics information moving intelligence to the edge
- Big Data generally makes use of unstructured data but can be combined with structured relational database access using SQL
- HADOOP is often referred to as NOSQL since it acts upon unstructured data
- HADOOP is not a protocol like SQL it is an architecture designed to provide high performance using commodity computers to provide clustered parallel processing over high-speed Ethernet
- Data Compression is key to transfer and storage of Big Data

exi

- **XML Interchange** (**Efficient EXI**) is as a Binary XML format which was adopted as a recommendation by the World Wide Web Consortium (W3C) in March 2011. It was developed by the W3C's Efficient XML Interchange and is one of the most prominent binary XML efforts to encode XML in a binary data format, rather than plain text.
- EXI can use any data compressor .
- Ref: XEP-0322

Stream Compression

- <stream:features>
  <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/> {Inovkes TLS session}
  <compression xmlns='http://jabber.org/features/compress'>
  <method>zlib</method>
  <method>lzw</method>
  <method>exi</method>
  <method>exi:54321</method>
  </compression>
  </stream:features>

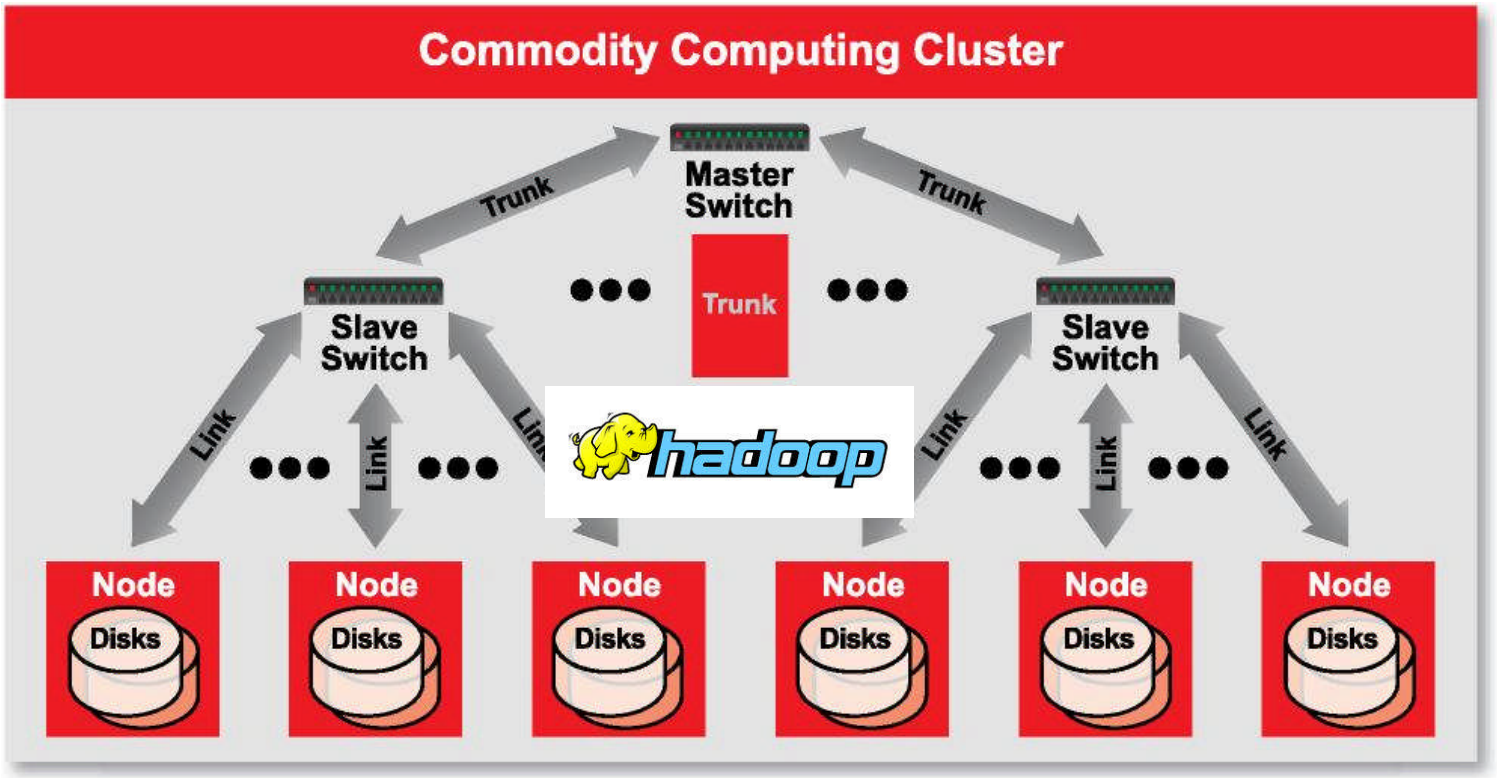
bzip2

- **bzip2** is a free and open source file compressor that uses the Burrow-Wheeler algorithm. The compressor uses Huffman Encoding. The bzip2 is used in HADOOP MapReduce for efficient storage and transfer of information for Big Data applications. Sensordata can send data to a Big Data store and retained in an unstructured dataset, such as AMI, or DER

qzipx

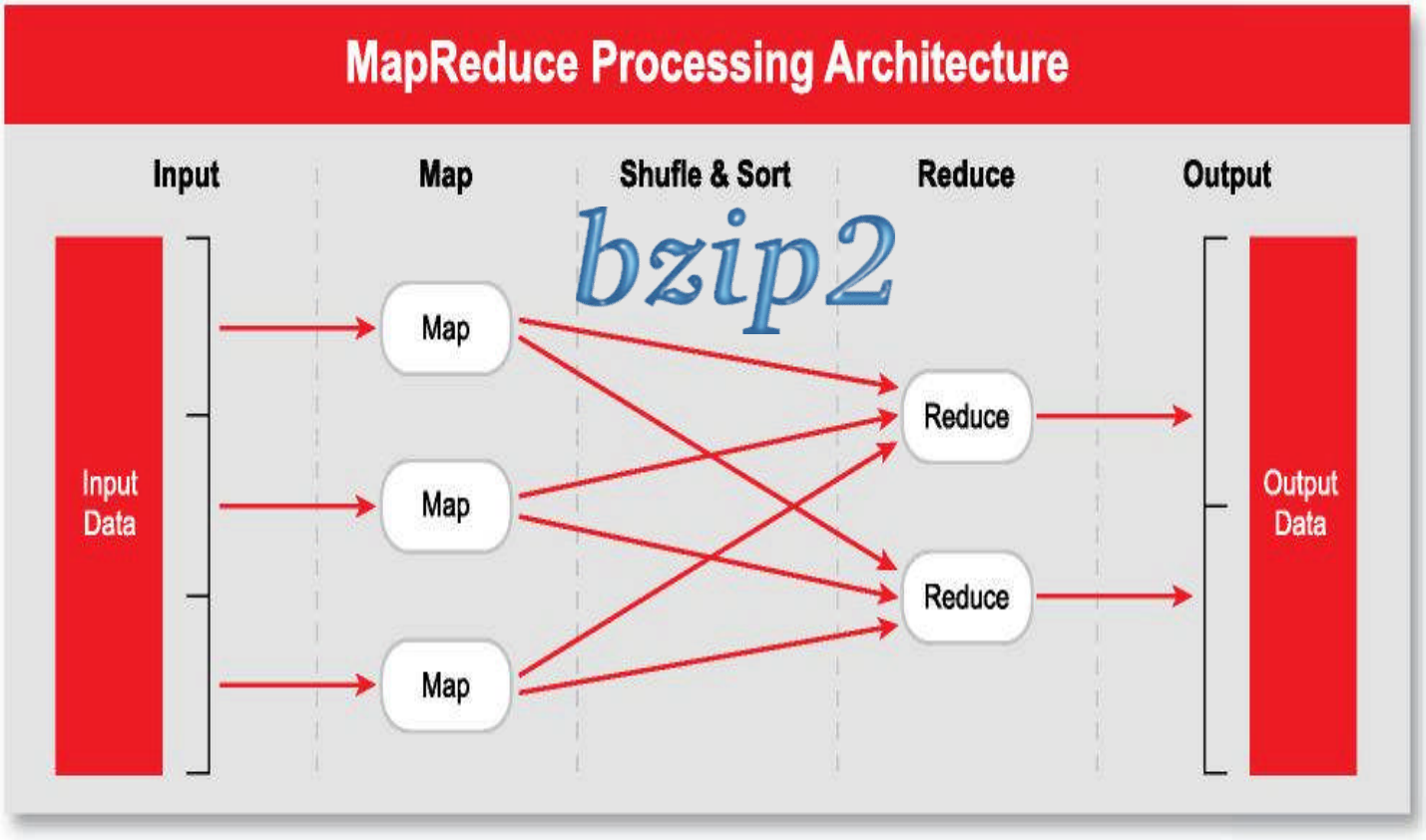
- **qzipx** is a new approach combining Huffman Encoding/LZW (zipx) and block sorting for storing data within constrained memory devices such as RFID. qzipx is still in research, but offers key benefits including fast "reconstruction" of data at rest using a minimal set of information.

Computing Clusters

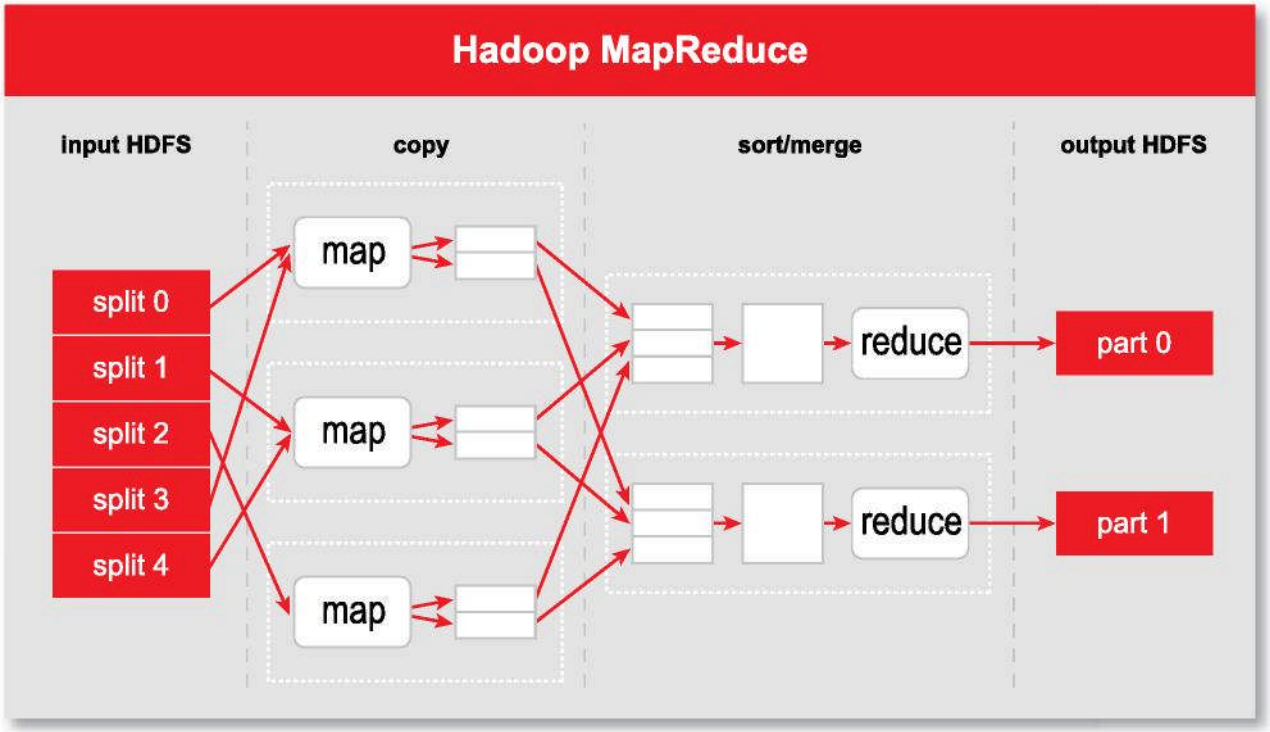


Google

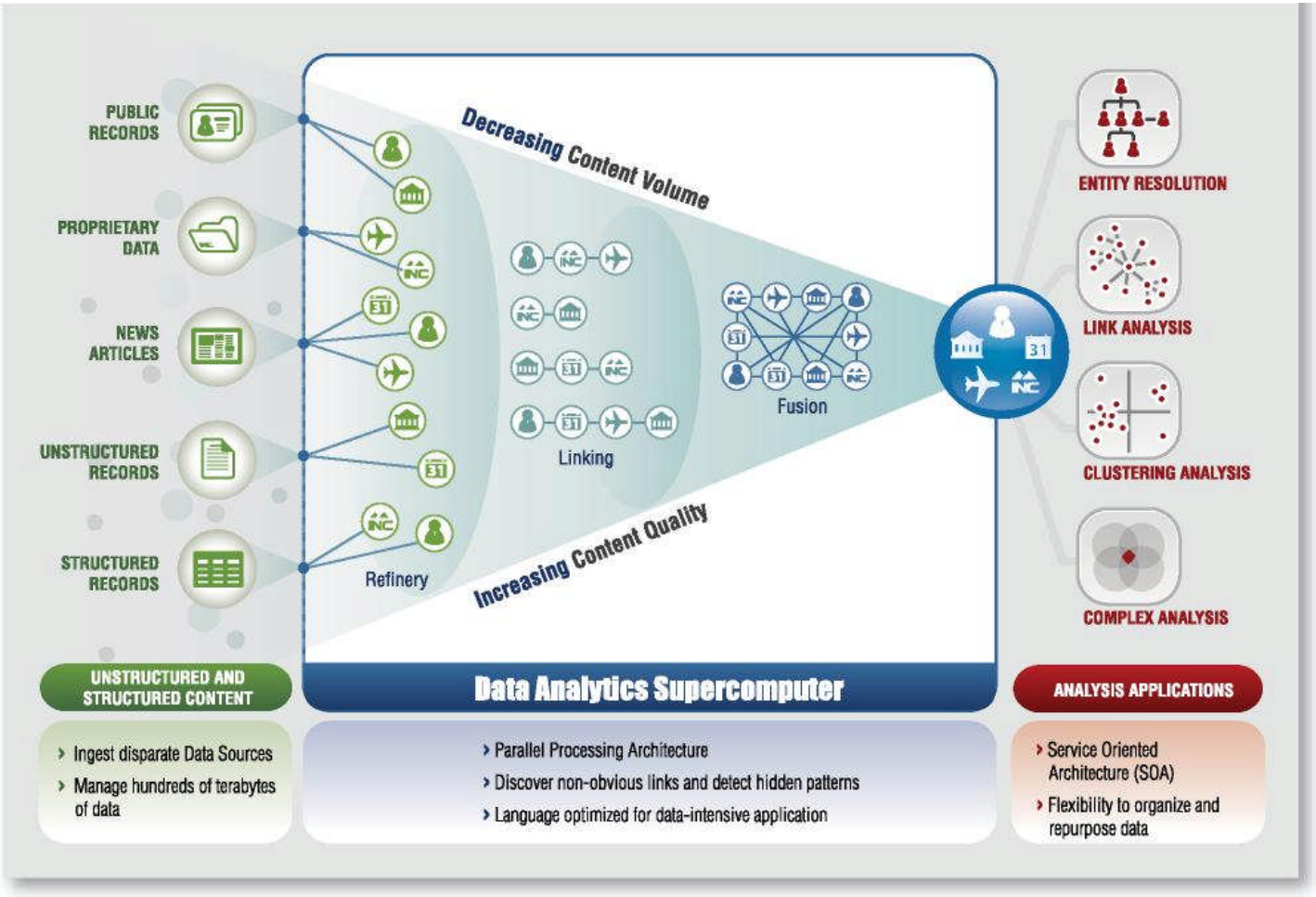
Big Data Architecture

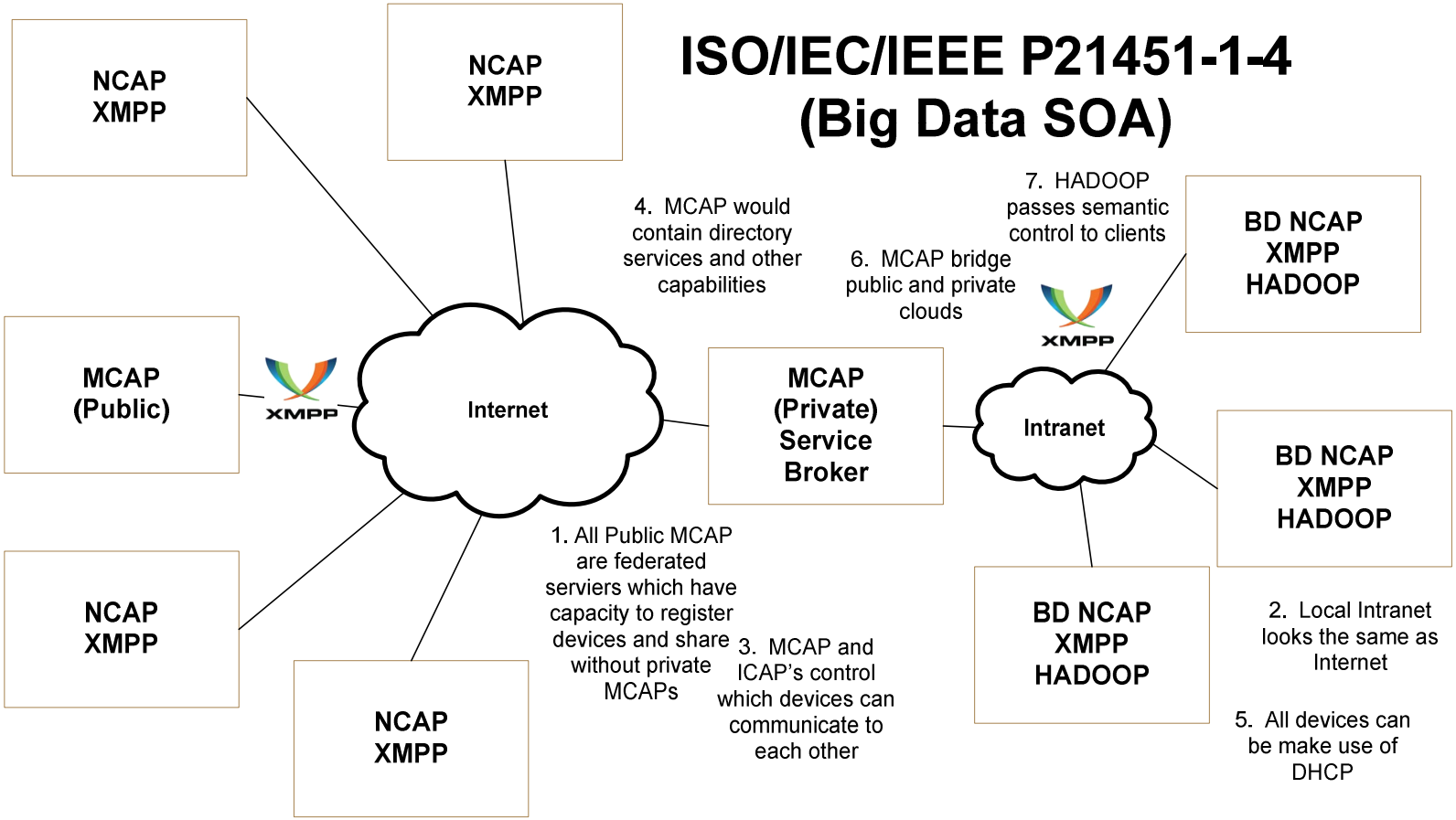


HADOOP MapReduce



Big Data Analytics




ISO/IEC/IEEE P21451-1-4
(Big Data SOA)
NCAP XMPP
NCAP XMPP
NCAP XMPP
NCAP XMPP
MCAP (Public)
XMPP
Internet
4. MCAP would contain directory services and other capabilities
MCAP (Private) Service Broker
1. All Public MCAP are federated serviers which have capacity to register devices and share without private MCAPs
3. MCAP and ICAP's control which devices can communicate to each other
6. MCAP bridge public and private clouds
7. HADOOP passes semantic control to clients
XMPP
Intranet
BD NCAP XMPP HADOOP
BD NCAP XMPP HADOOP
BD NCAP XMPP HADOOP
2. Local Intranet looks the same as Internet
5. All devices can be make use of DHCP

Use Cases for the Smart Grid

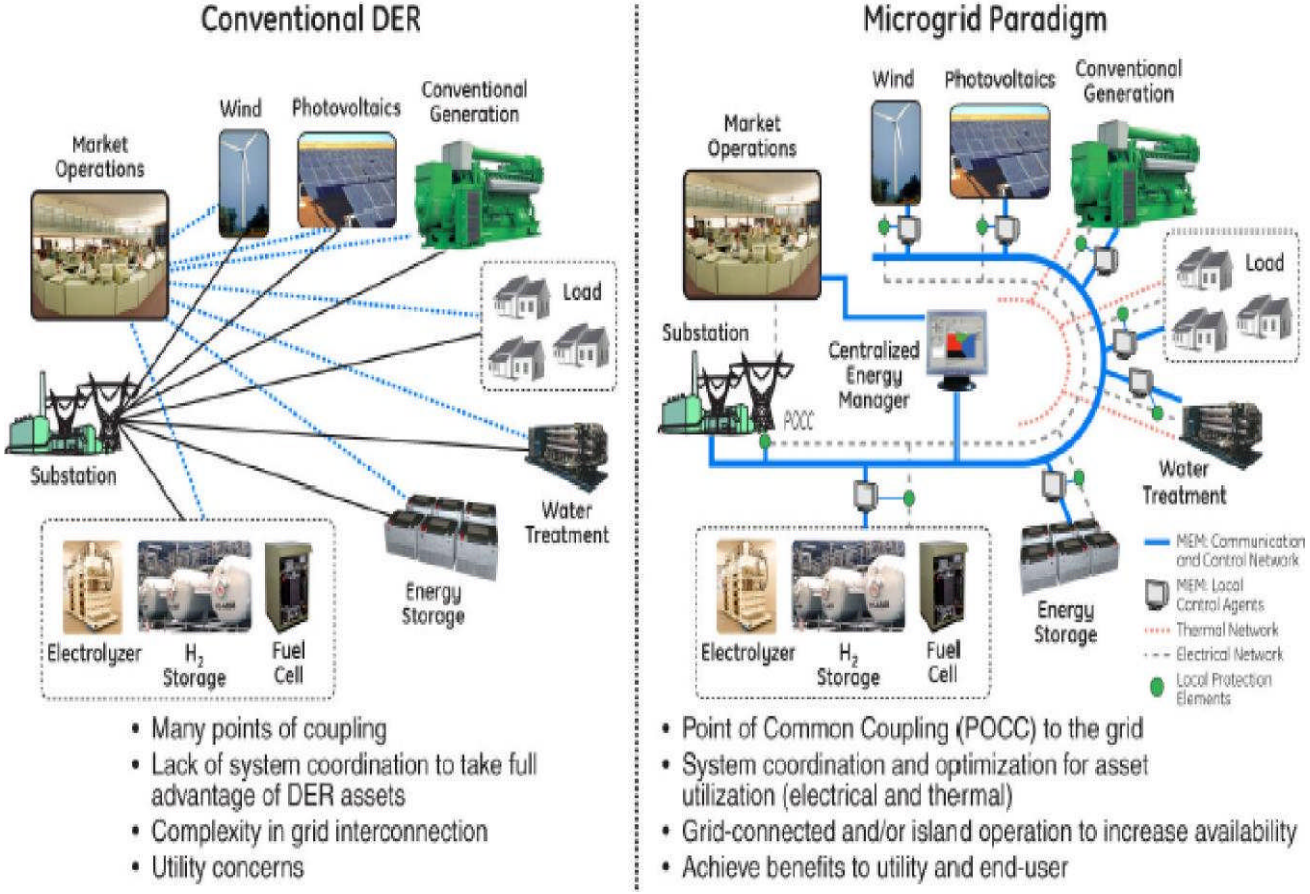
Key Challenges
slowing adoption of Smart Grid

1. Effectiveness - Internet is not effectively utilized for Smart Grid
2. Implementation - Software has implementation variances
3. Interoperability - Interoperability issues with standard protocols
4. Scalability - Peer-to-peer connections limit scalability
5. Session Persistency - Sessions are not persistent using web services
6. Cyber Vulnerabilities - Cyber vulnerabilities are often built-in
7. Cyber Exposure - IP addresses present cyber exposure
8. Legacy Devices - Legacy devices must be supported
9. Presence Detection - Lack of “Presence” requiring polling for information
10. Security - Security is layered on which increases complexity
11. Cost/Complexity - The resulting costs and complexity escalate exponentially

Sensei/IoT* XMPP Cyber Defense meeting the challenges of the Smart Grid

- Sensei/IoT* is technology agnostic and protocol independent
- Sensei/IoT* uses Transport Layer Security (TLS) to encrypt data traffic which is built-in to the protocol
- Sensei/IoT* is firewall friendly utilizing port translation eliminating exposures common to use of Port 80
- Sensei/IoT* utilizes ***Semantic Web 3.0*** (XML metadata to provide a semantic conversation between devices)
- Sensei/IoT* can utilize a Service Broker as an trusted intermediary to establish a trust relationship between users, applications, and devices
- Sensei/IoT* can use an Identity Provider (*IdP*) to provide Single Sign On (SSO) capability
- Sensei/IoT* includes end-to-end digital signing and encryption (RFC 3923) using Efficient XML Interchange (EXI)

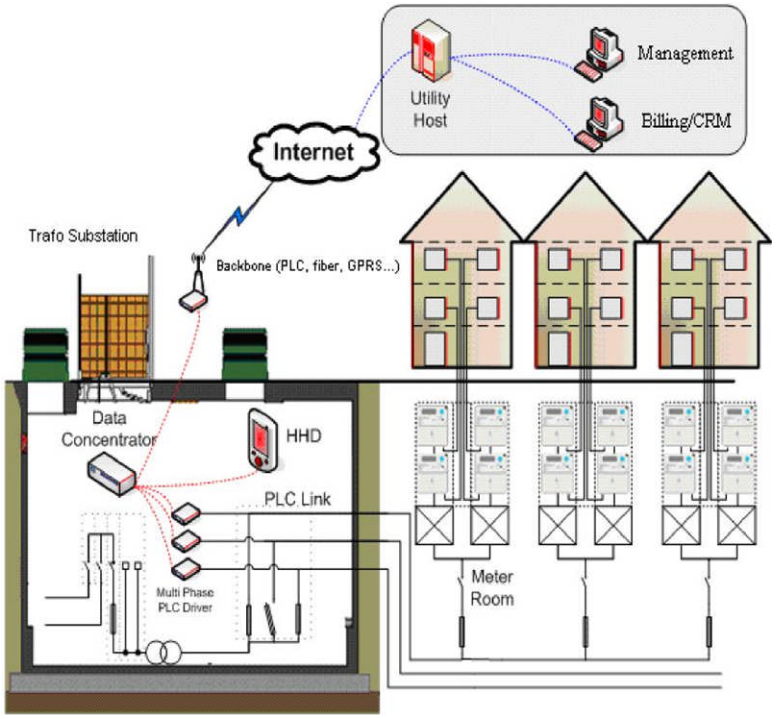
Demand Energy Acquisition (DEA)
Conventional vs. Decentralized



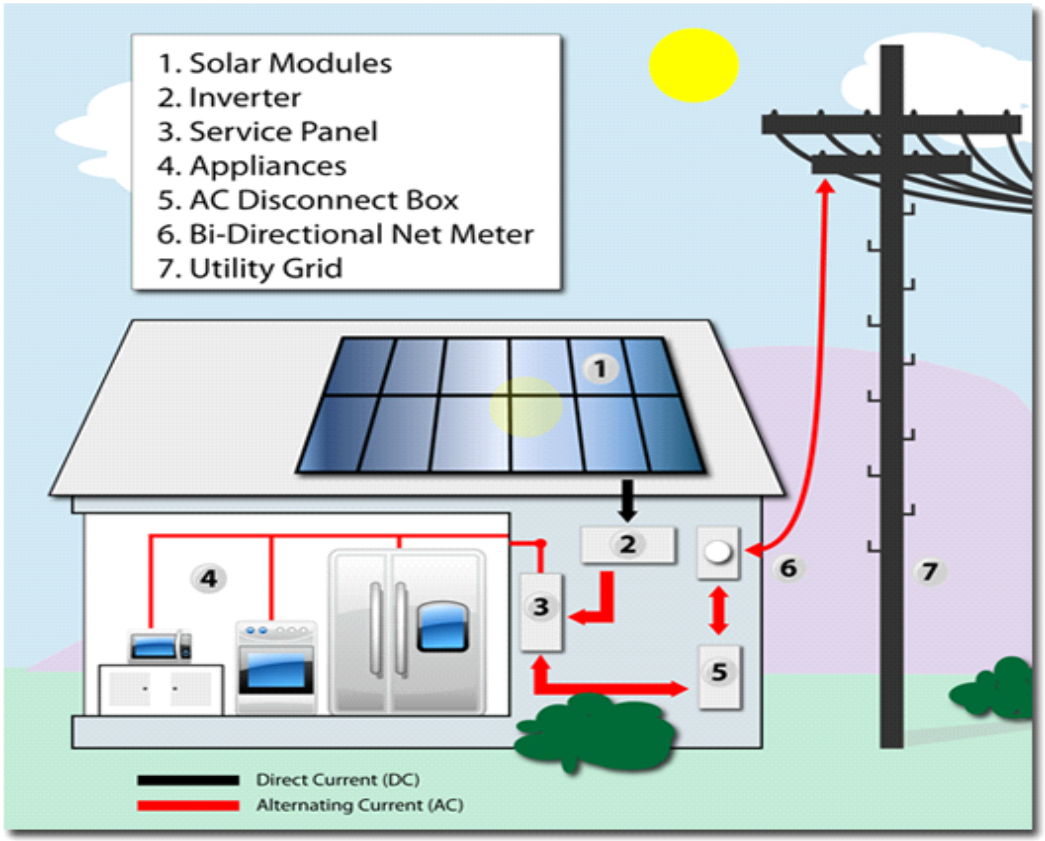
- Many points of coupling
- Lack of system coordination to take full advantage of DER assets
- Complexity in grid interconnection
- Utility concerns

- Point of Common Coupling (POCC) to the grid
- System coordination and optimization for asset utilization (electrical and thermal)
- Grid-connected and/or island operation to increase availability
- Achieve benefits to utility and end-user

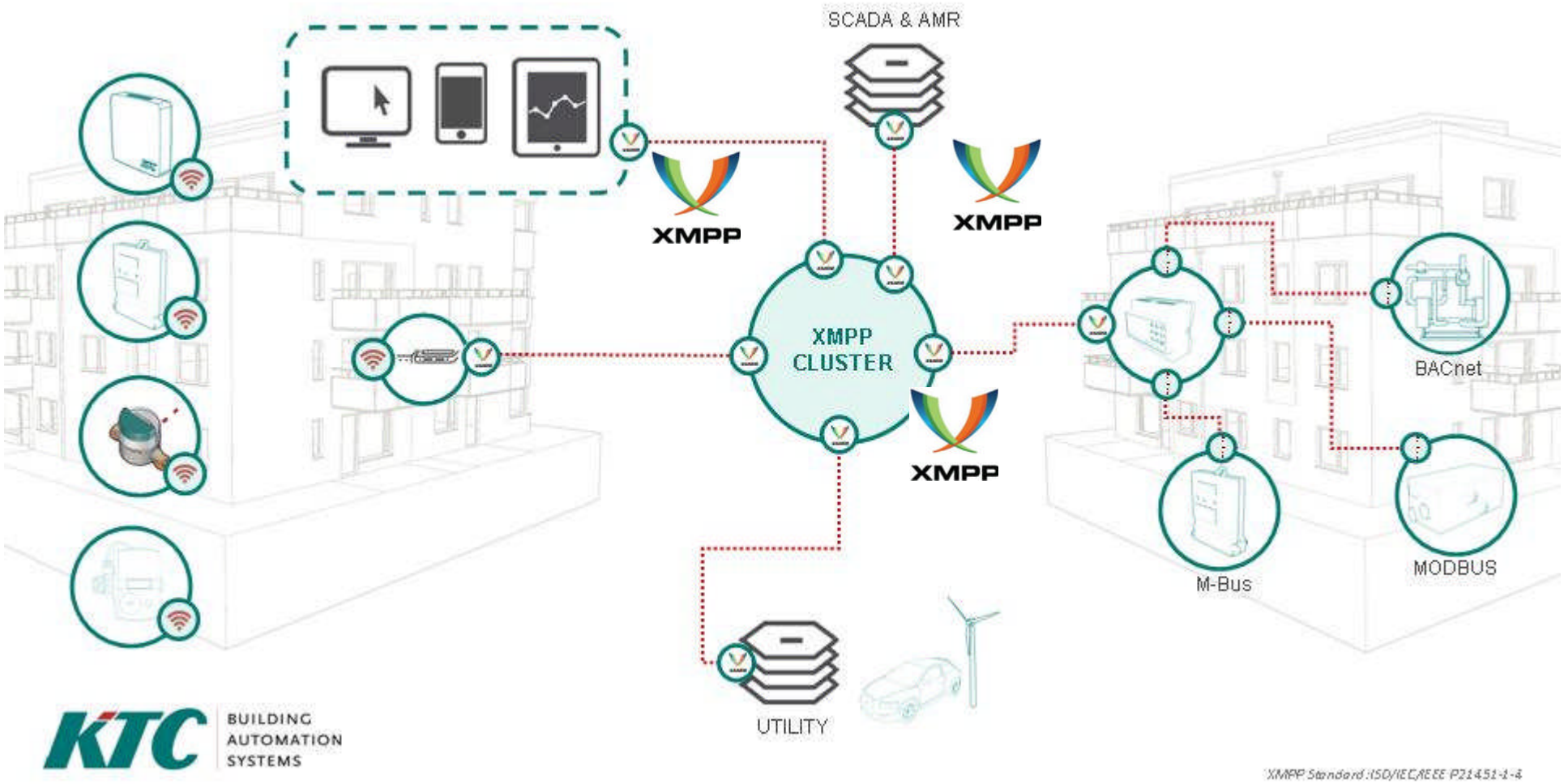
Microgrid Automation
Broadband over Power Lines (BPL)



Home Automation



Smart Grid XMPP
Cluster Service Broker (Sweden)



Thank you

Questions?