Wrap-up: Integrating all the Pieces

NASPI Working Group Meeting

New Orleans, March 6-7, 2008

Erich Gunther
Ron Farquharson
EnerNex Corporation

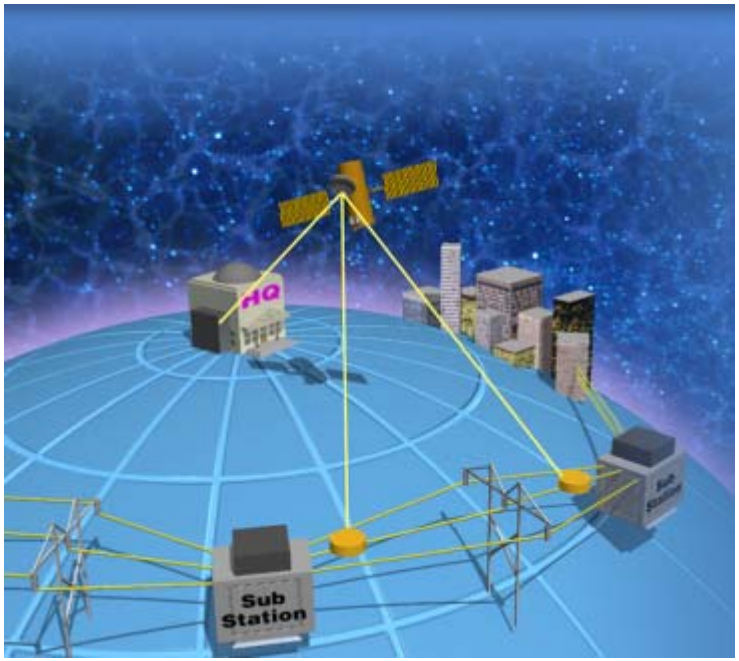
EnerNex CORPORATION

Future Installed Base – A LOT of "Pieces"

- One manufacturer indicates that they now have over 15,000 relays installed in North America with the capability to record synchrophasor values and another 80,000 units that could be upgraded to support this function.
- NASPInet long term objective includes the ability to support a distributed system of thousands of devices per average utility (*) and in range of 100,000 to one million devices providing phasor data.
- Challenges at the utility level and the NASPInet level.

(*) NASPI July 19, 2007 Architecture Meeting with PNNL, Update August 2007 – NASPI Data and Network Management Task Team.

Smart Grid: Power Delivery System of the Future



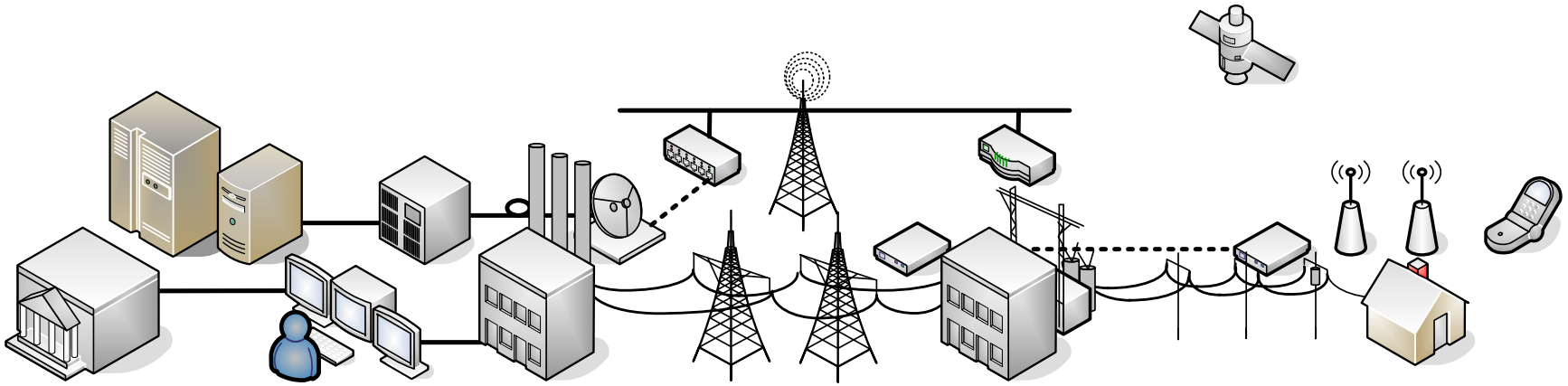
Makes use of communications, computing and power electronics to create a system that is:

- *Self-Healing* and *Adaptive*
- *Interactive* with consumers and markets
- *Optimized* to make best use of resources and equipment
- *Predictive* rather than reactive, to prevent emergencies
- *Distributed* across geographical and organizational boundaries
- ***Integrated*,** merging monitoring, control, protection, maintenance, EMS, DMS, marketing, and IT
- *More Secure* from attack

What is the Smart Grid – EISA 2007

- The term Smart Grid Functions shall include:
  - Ability to store, send and receive digital information through a combination of devices
  - Ability to do same to or from a computer or control device
  - Ability to measure and monitor as a function of time of day, power quality, source and type of generation, etc
  - Ability to sense disruptions in power flows and communicate on such instantaneously
  - Ability to detect, respond to, recover, etc relative to security threats
  - Ability of appliances and equipment to respond without human intervention
  - Ability to use digital information for grid operations that were previously electromechanical or manual
  - Ability to use digital controls to manage demand, congestion, and provide ancillary services

Smart Grid Applications



Real-time Simulation and Contingency Analysis

Distributed Generation and Alternate Energy Sources

Self-Healing Wide-Area Protection and Islanding

Asset Management and On-Line Equipment Monitoring

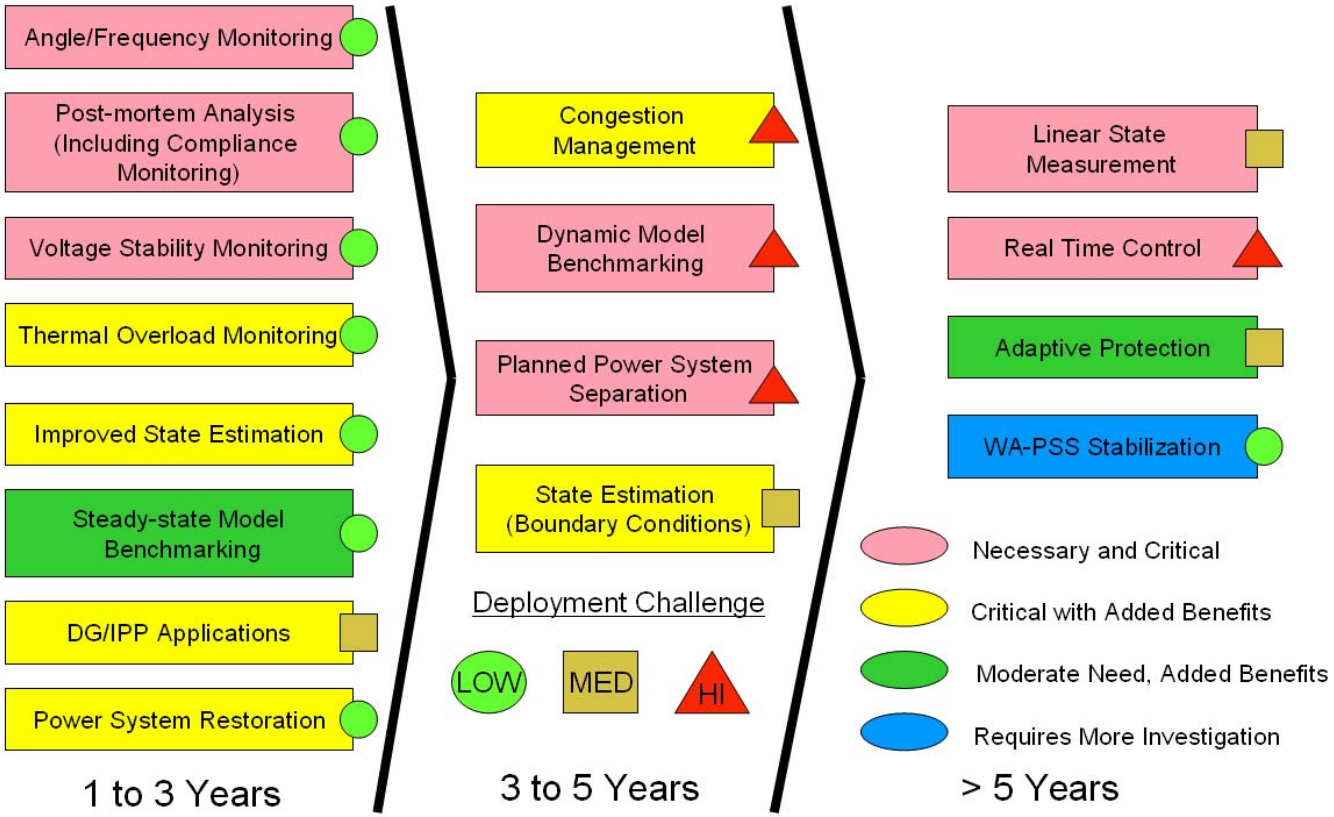
Demand Response and Dynamic Pricing

Participation in Energy Markets

Shared Information – Continuously Optimizing – Intelligent Responses!

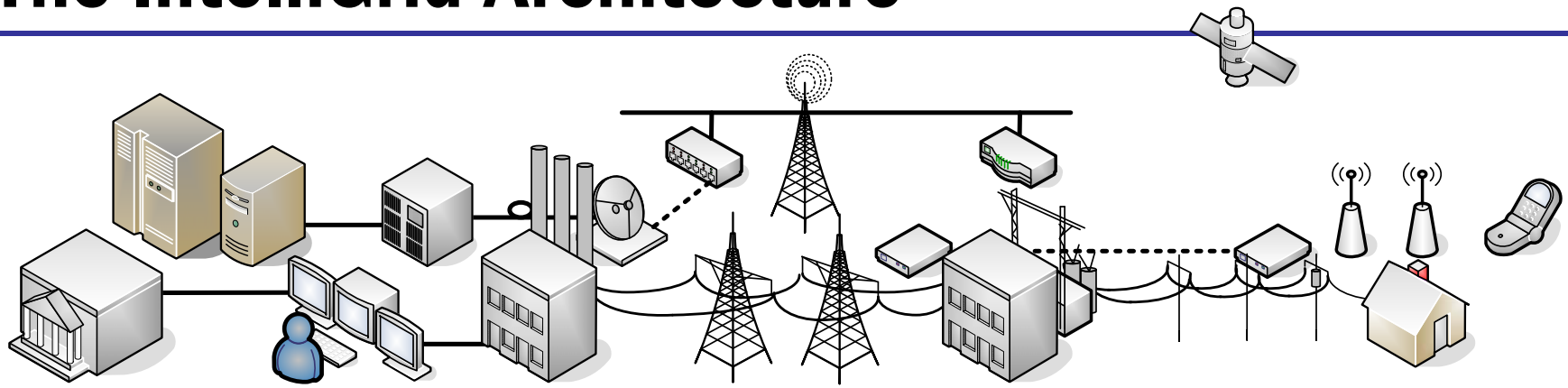
NASPI Application Roadmap

Roadmap for Capability Evolution Indicating Time to Achievement, Priority of Industry Need, and Severity of Deployment Challenge (11/30/07)

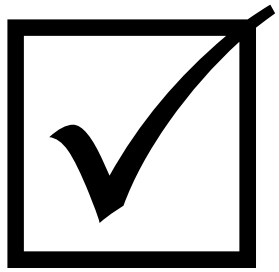


11-30-07

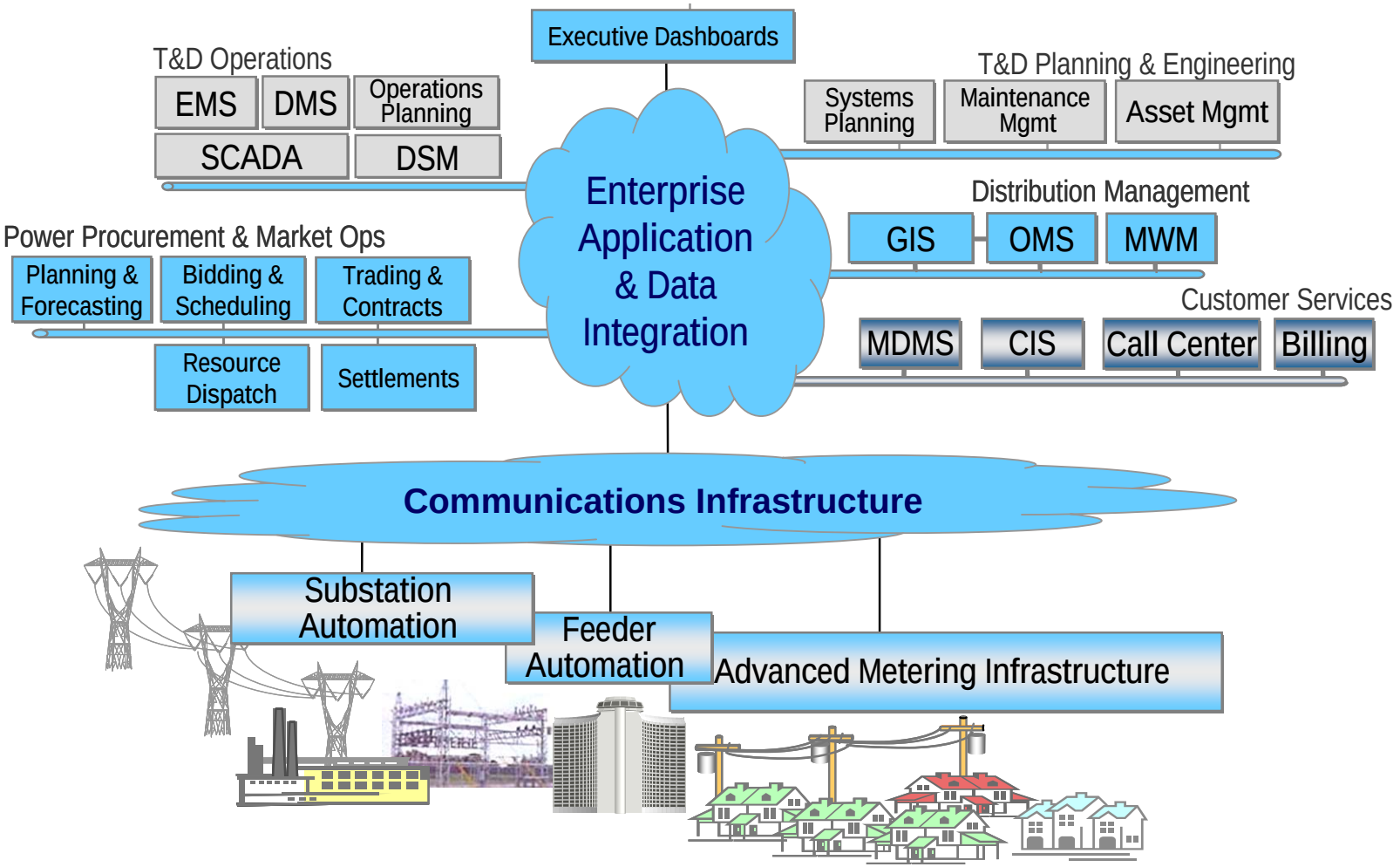
The IntelliGrid Architecture



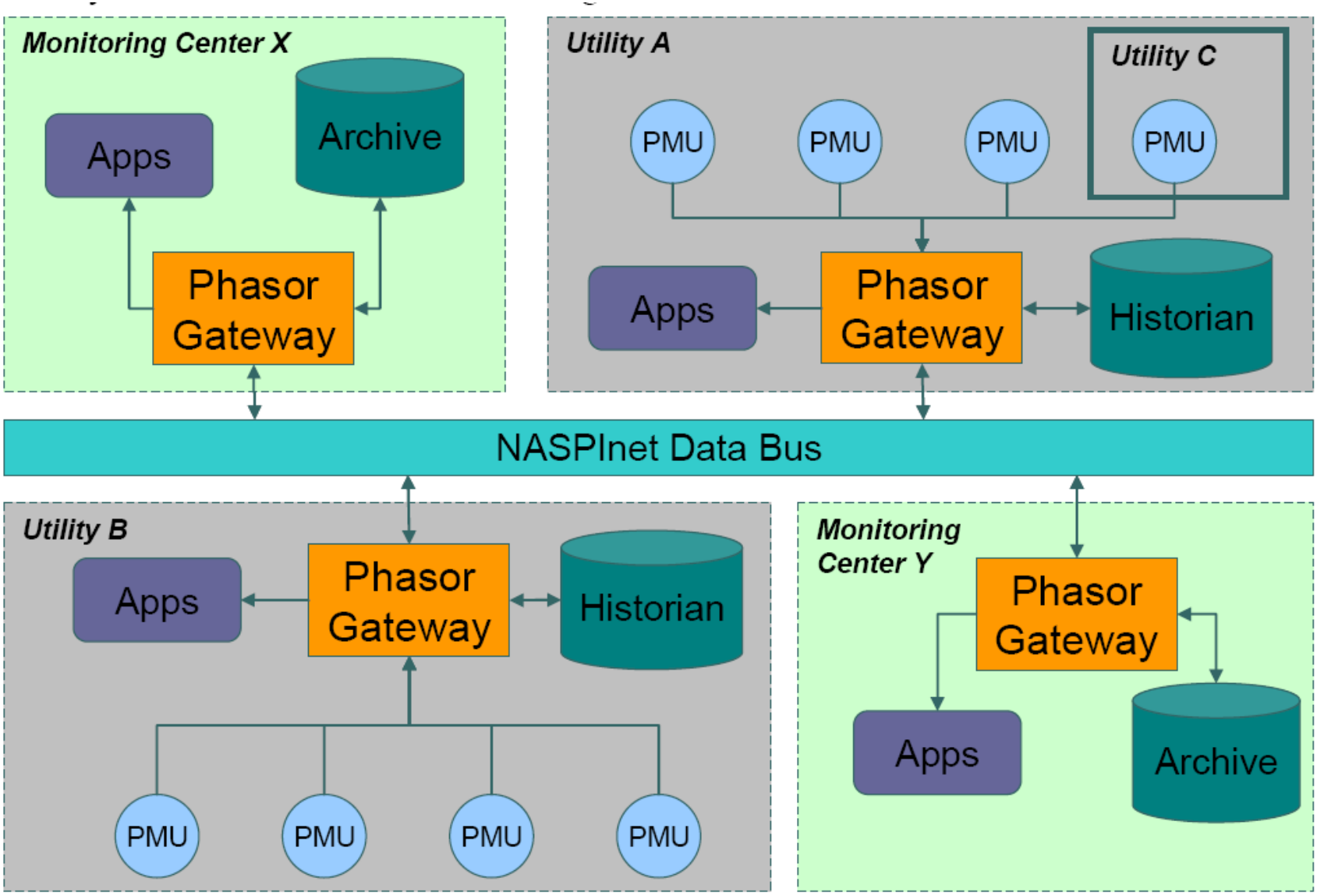
- An open, standards-based architecture for integrating the data communications networks and intelligent equipment needed to support the Power Delivery System of the Future
- Provides the methods, tools, best practices and recommendations for specifying “intelligent” systems in such a way as to promote:
  - Interoperability
  - Flexibility
  - Expandability
  - Effective security and data & system management



Communication and Information Infrastructure

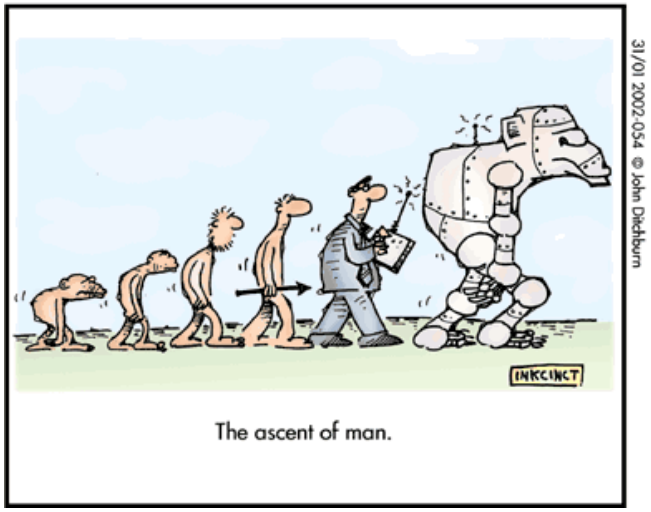


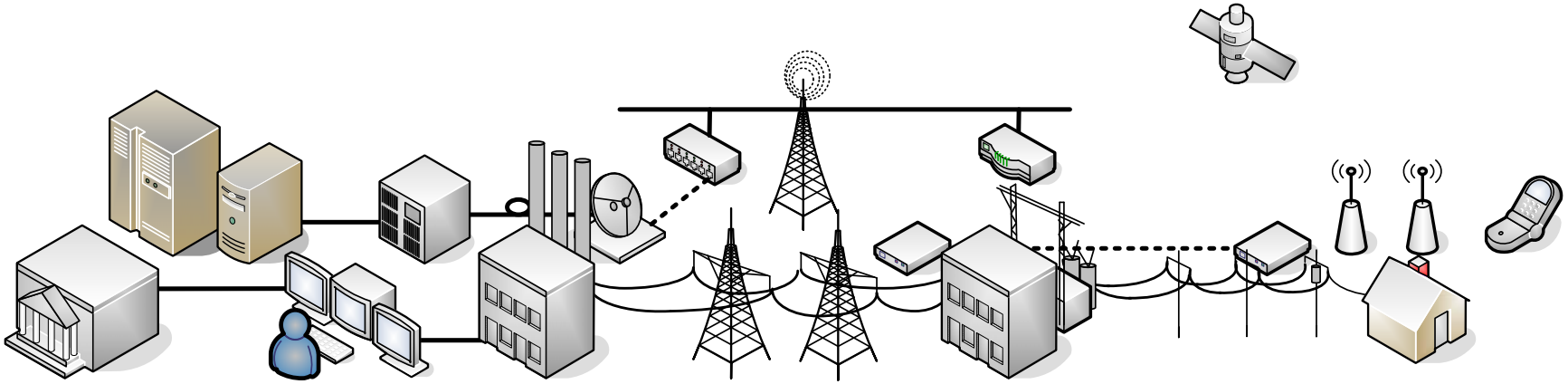
Basic NASPInet Architecture (Draft RFP)



How is the Smart Grid Created?

The smart grid is not created all at once – it will evolve over many years from today's infrastructure through the deployment and integration of ***Intelligent Systems***





Implementation Approach

The optimal approach for defining requirements for a system is to identify (with broad multi-disciplinary buy in) the suite of applications, by phase, with the most significant requirements that will be required and justified within the planned life cycle of the system (15 years).

Then estimate the total number of possible applications and the total number of possible installations of PMUs or other devices delivering phasor data.

Proposed Utility PMU Integration Plan

Phase One

Intended to address a number of the fundamental deficiencies such as substation communications reliability with the current PMU installations. Recommendations include moving to standards based protocols for all devices.

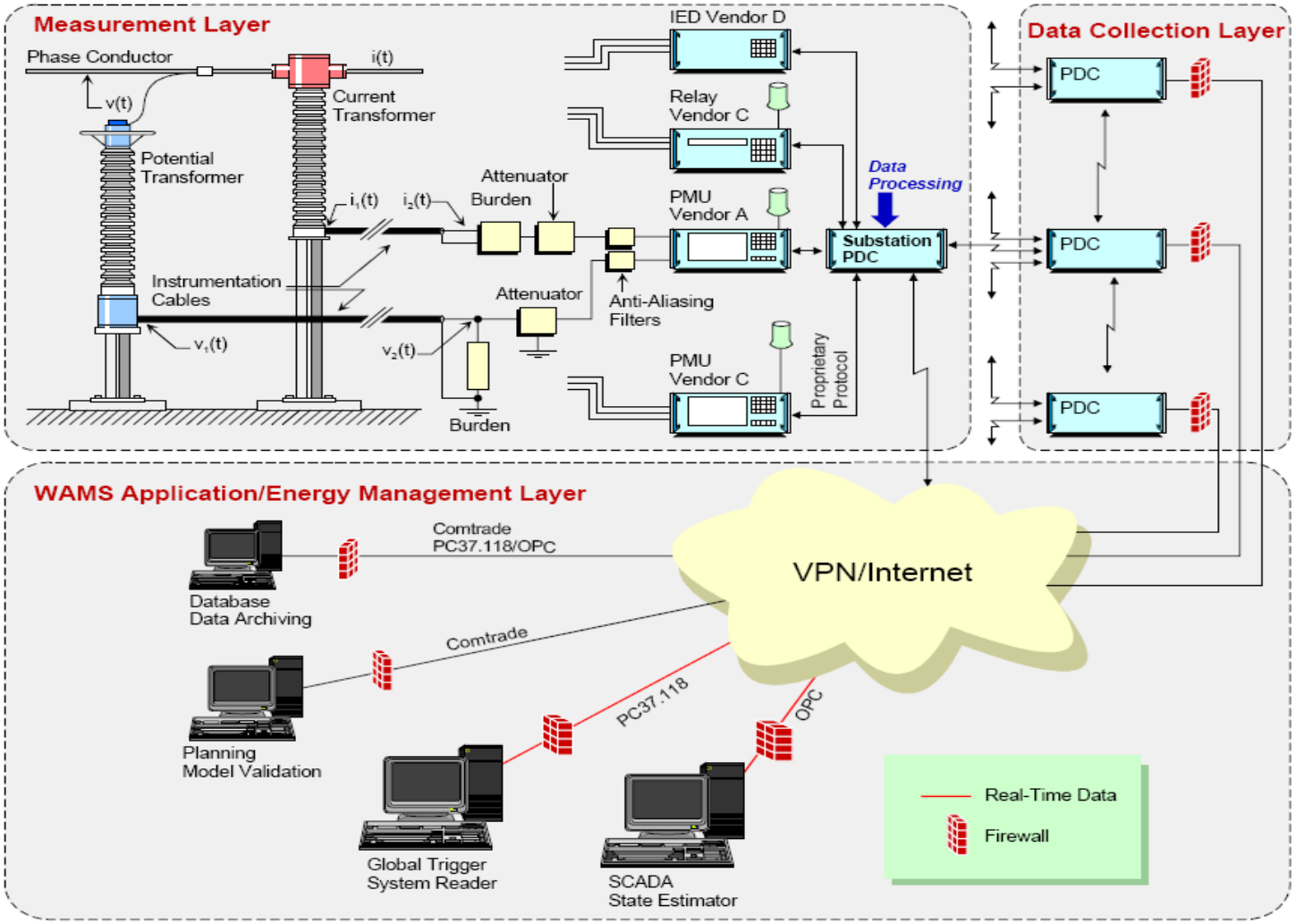
Phase Two

Builds on Phase One and is focused on supporting and implementing important new phasor based applications using phasor data from a larger hybrid system of IEDs that interoperate to share data. An upgraded communications infrastructure, substation based PDCs, cyber security and compliance with the current NASPI phasor data interface requirements as defined by TVA are also included.

Phase Three

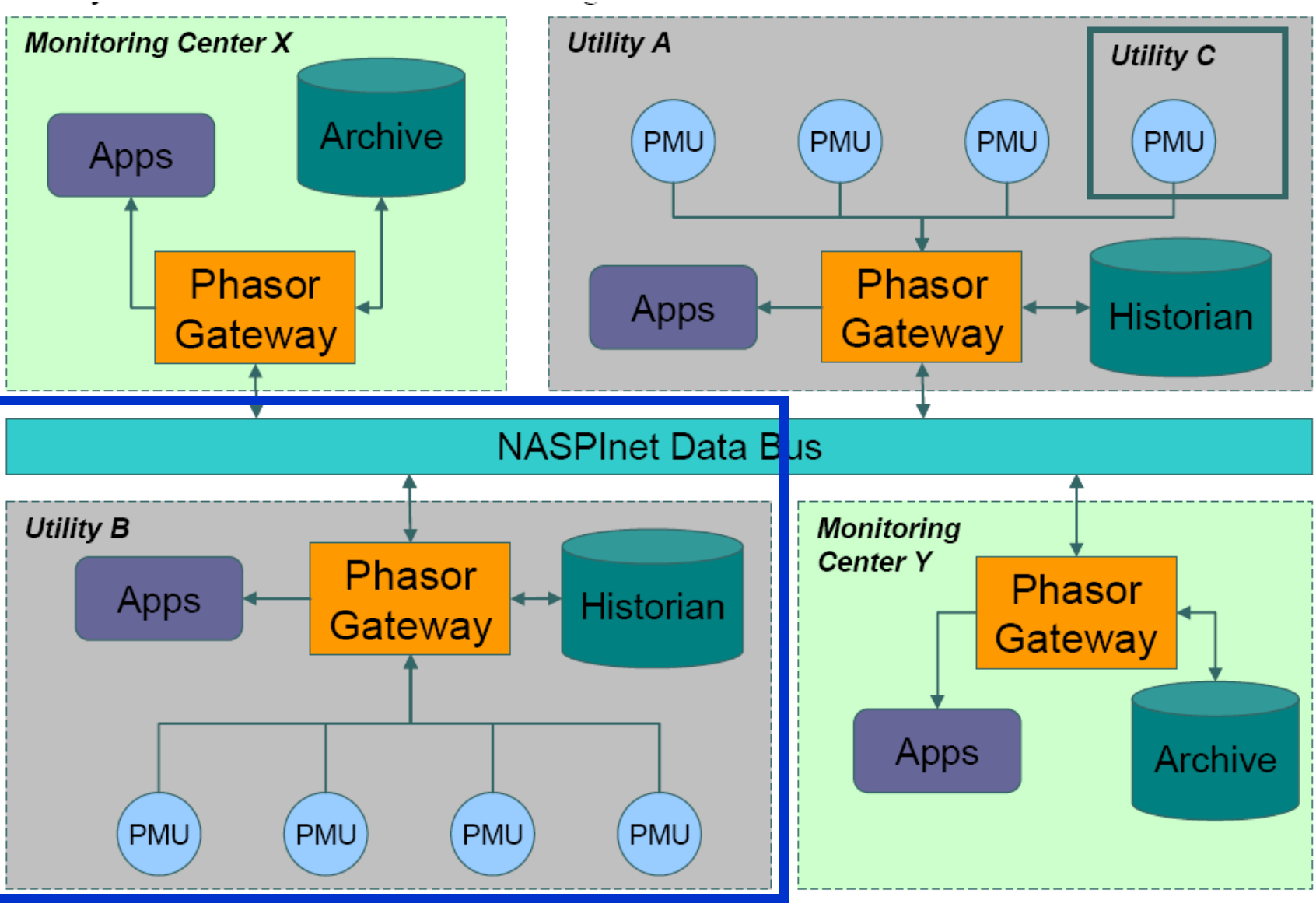
Builds on Phase One and Two to propose a fully **integrated grid communications and automation architecture (IGCA).** A key aspect is the much larger implementation of integrated devices such as relays and DFRs as well as dedicated purpose PMUs resulting in a high level of penetration of phasor measurement across the system. Such a large hybrid system for phasor measurement requires a fully integrated, high performance architecture based on open standards such as IP and IEC 61850 that support extensive services, QoS (where applicable), object modeling, meta data and self description. Key elements in this integrated architecture also include the substation gateway/proxy server, implementation of SuperCalibrator technology at the substations and the substation data historian.

Phase II Architecture

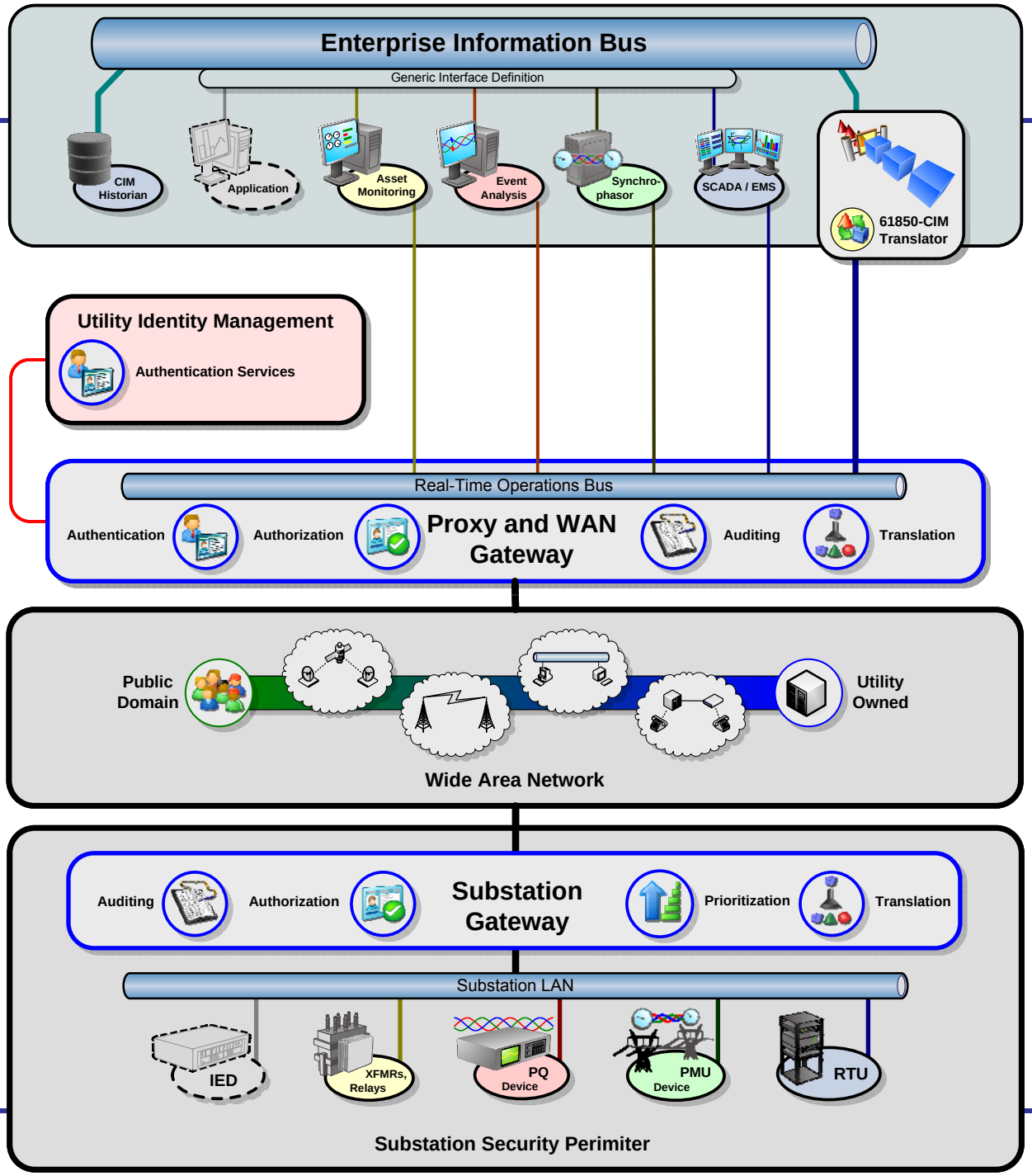


"Performance Requirements Part I – Targeted Applications: Raw Data Utilization", EIPP Performance Requirements Task Team (PRTT), February 28, 2005. Available at http://phasors.pnl.gov/resources_performance.html.

Phase III - Basic NASPInet Architecture (Draft RFP)



The Smart Grid Architecture

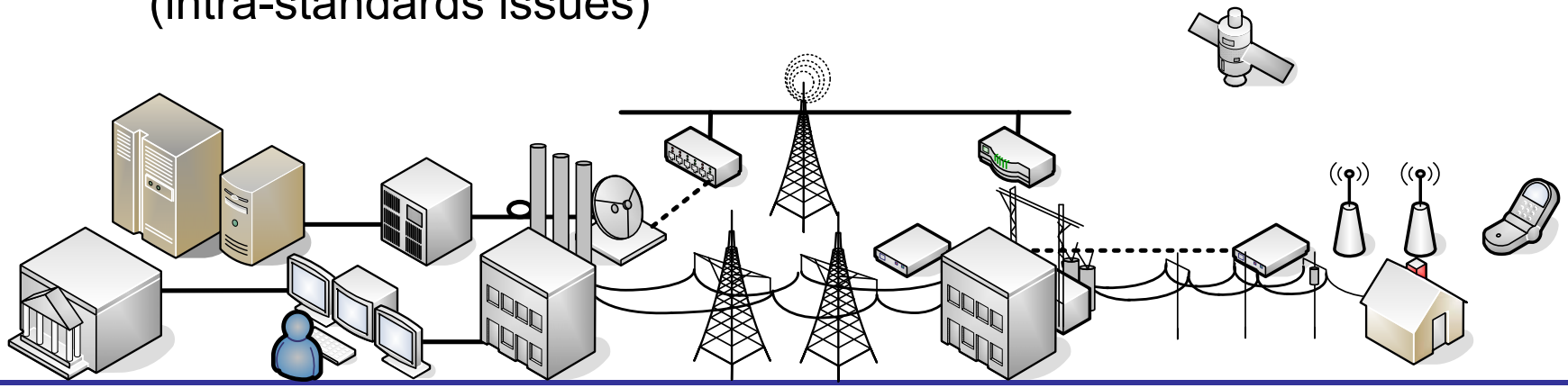


Key Components

1. Enterprise Information Bus
2. Generic Interface Definition (GID)
3. IEC 61850 to CIM Translator
4. Operational applications
5. Real-Time Operations Bus
6. Utility Identity Management
7. Proxy & WAN Gateway
8. WAN
9. Cyber security
10. Substation Gateway / Phasor Gateway?
11. Substation LAN
12. Substation IEDs
13. Feeder IEDs
14. Consumer devices
15. Mobile work force

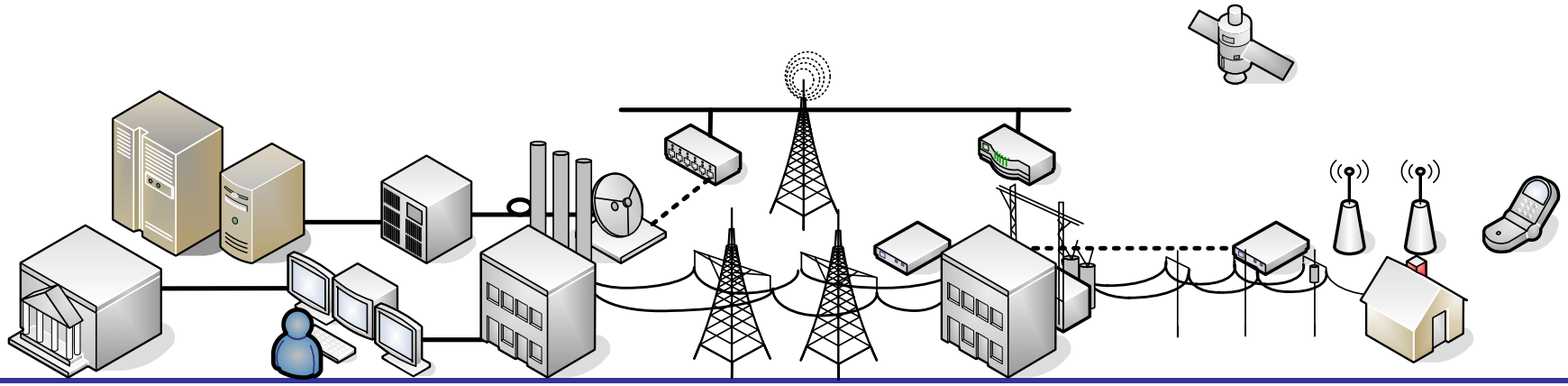
Barriers Impeding the Vision

- Utility culture
- Lack of integration methods, tools and technologies
  - Effective tools for specifying, designing and procuring intelligent systems
  - Effective approaches for security, data and system management
- Standards
  - Incomplete set of standards (inter-standards issues)
  - Lack of maturity of key standards (intra-standards issues)

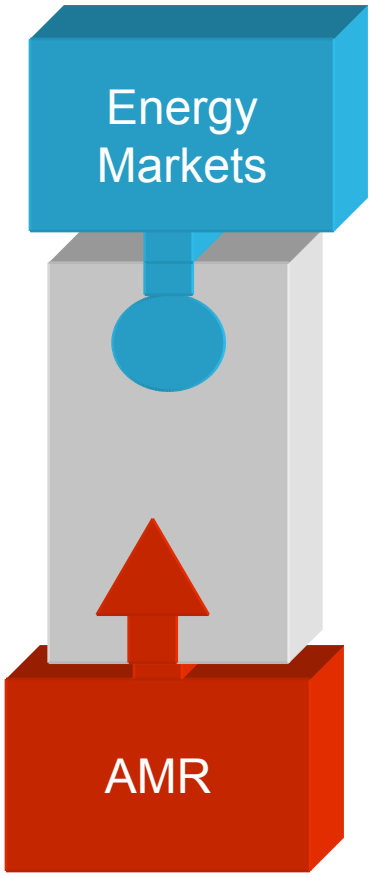


Barriers Impeding the Vision

- Suppliers not providing products that comply with standards and support integration
- Lack of understanding of what is possible
  - New capabilities and approaches
    - Business case (benefits and costs)
    - New technology requirements
  - Awareness of stakeholders
    - Utilities
    - Suppliers
    - Public sector

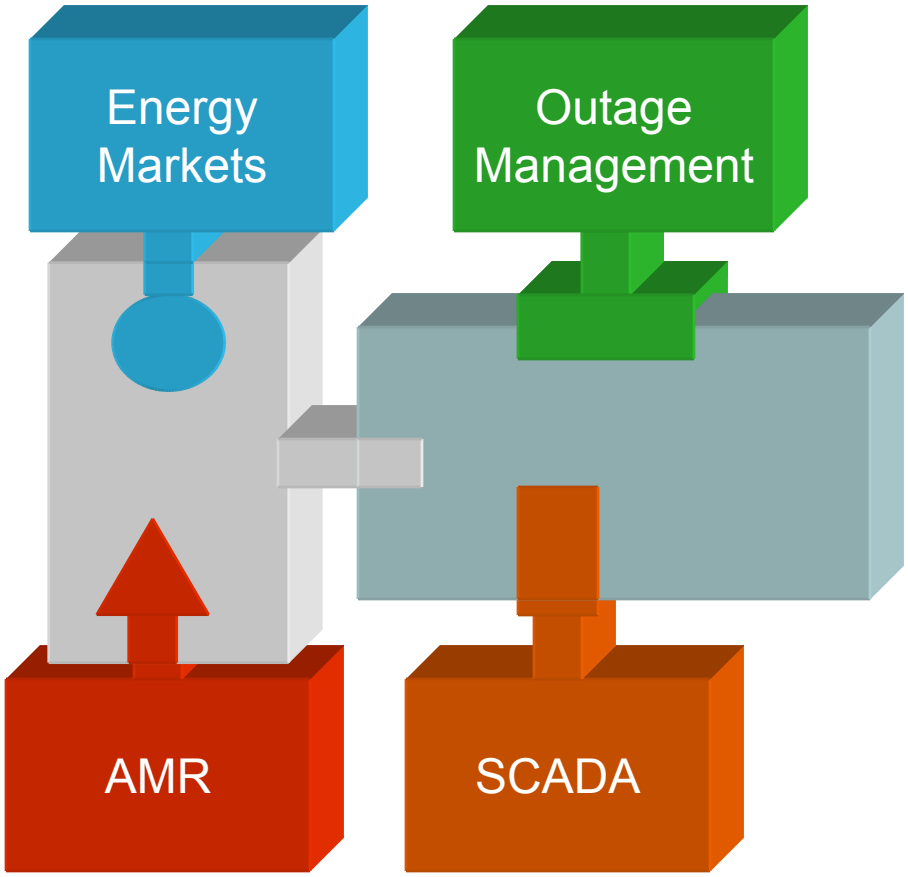


One-Off Integration



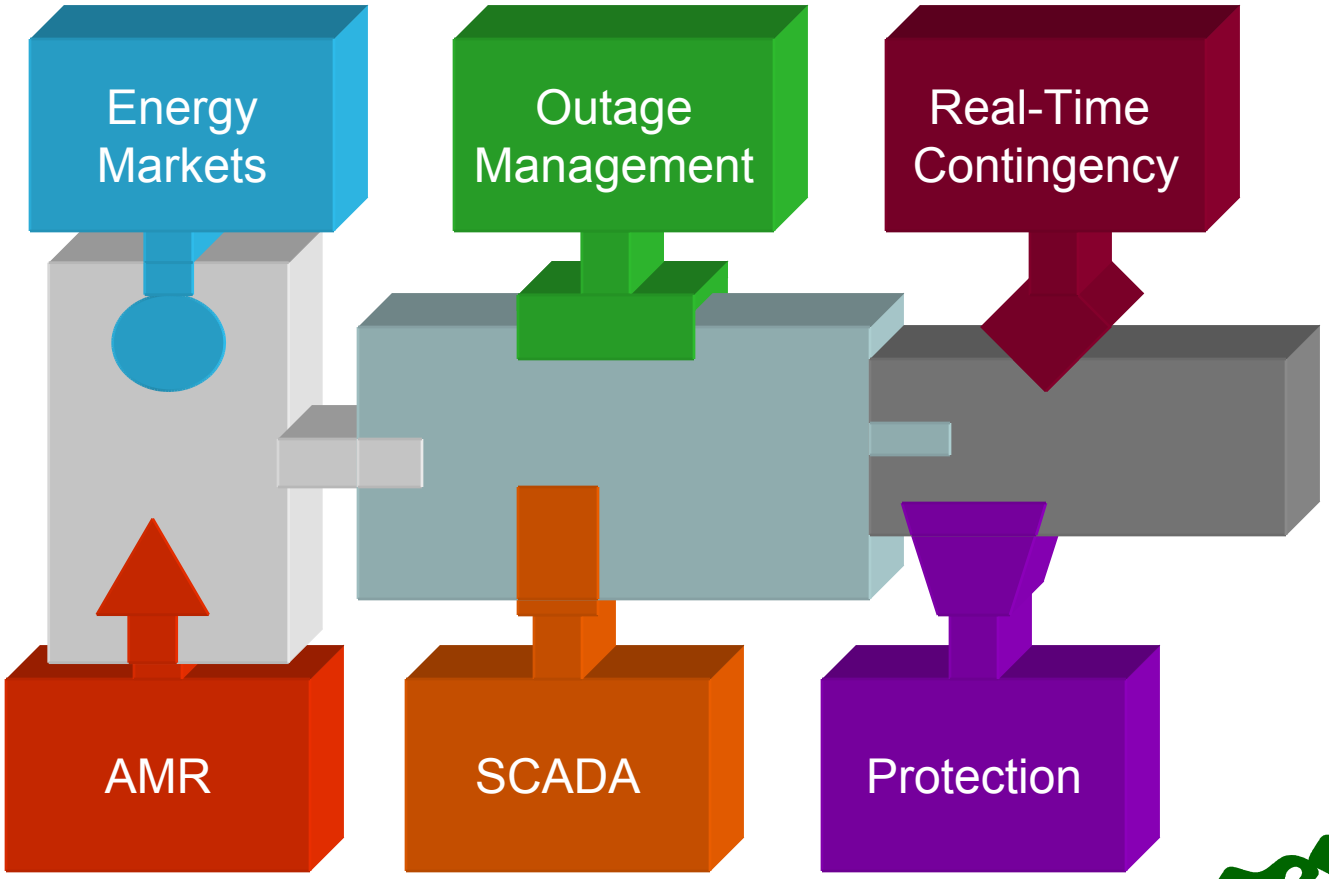
- Integration is typically done after the fact
- Cost is significant

Doing it the Next Time

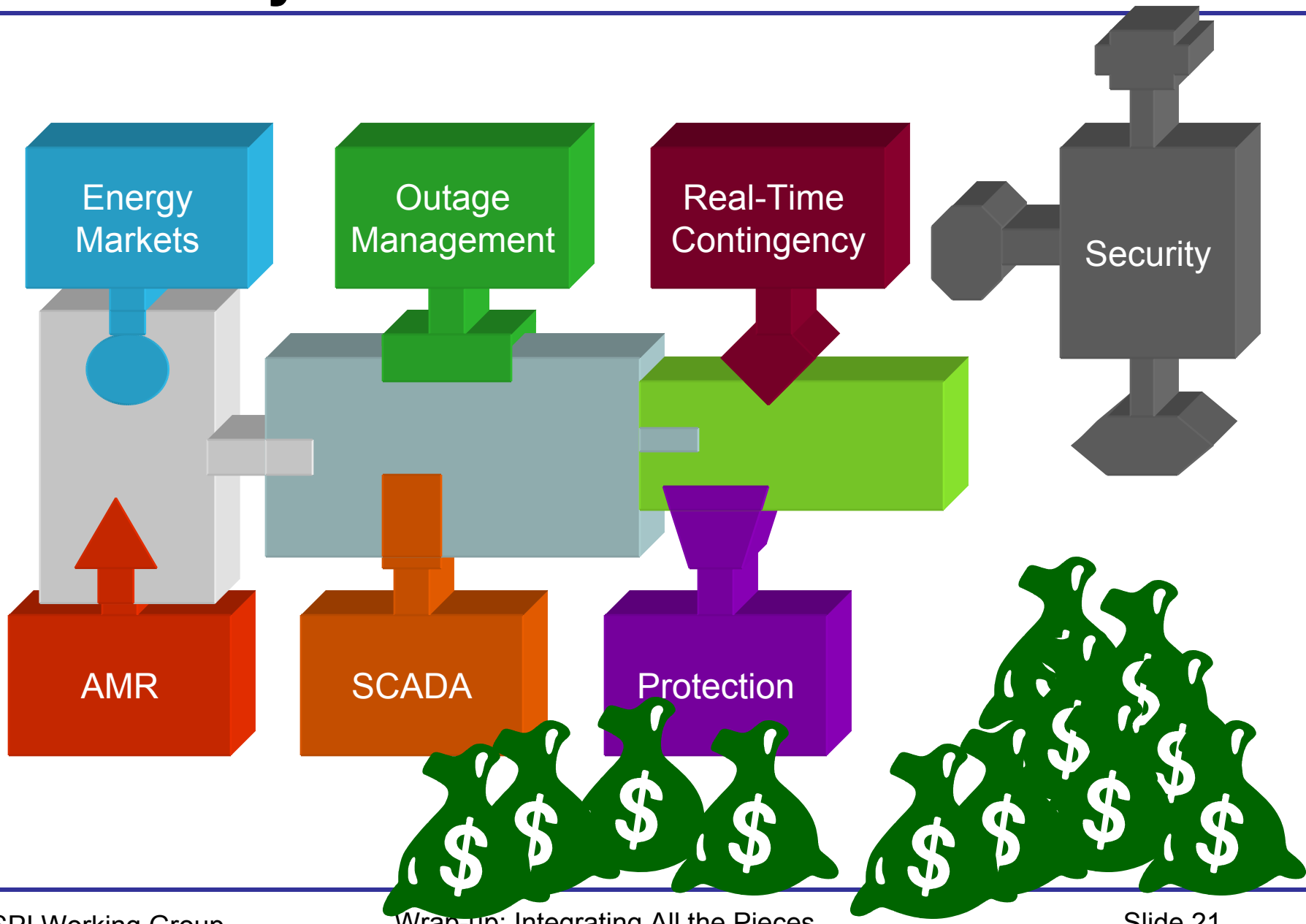


- Now want to link in new systems
- Must first make the old system expandable
- Then must do another “one-off” integration

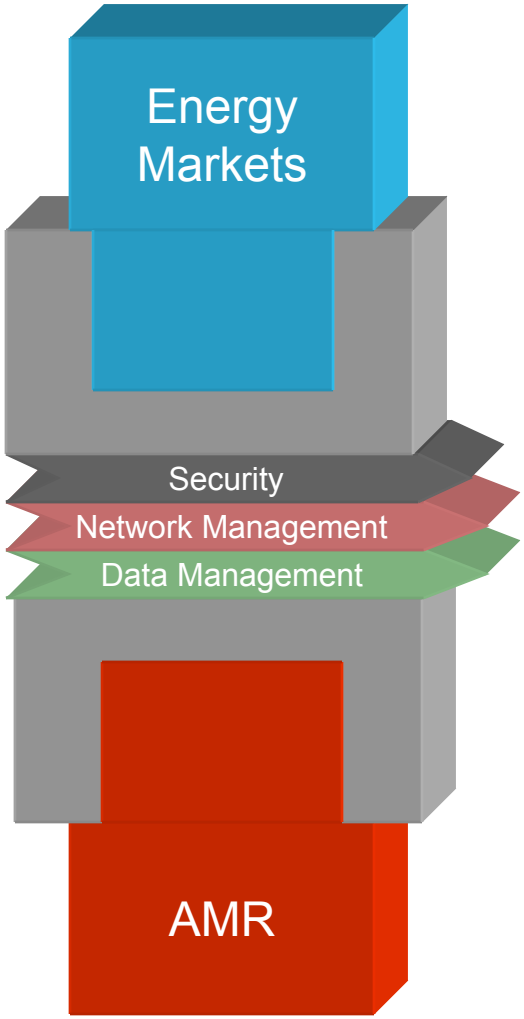
And again…


Energy Markets
Outage Management
Real-Time Contingency
AMR
SCADA
Protection

And then you remember…

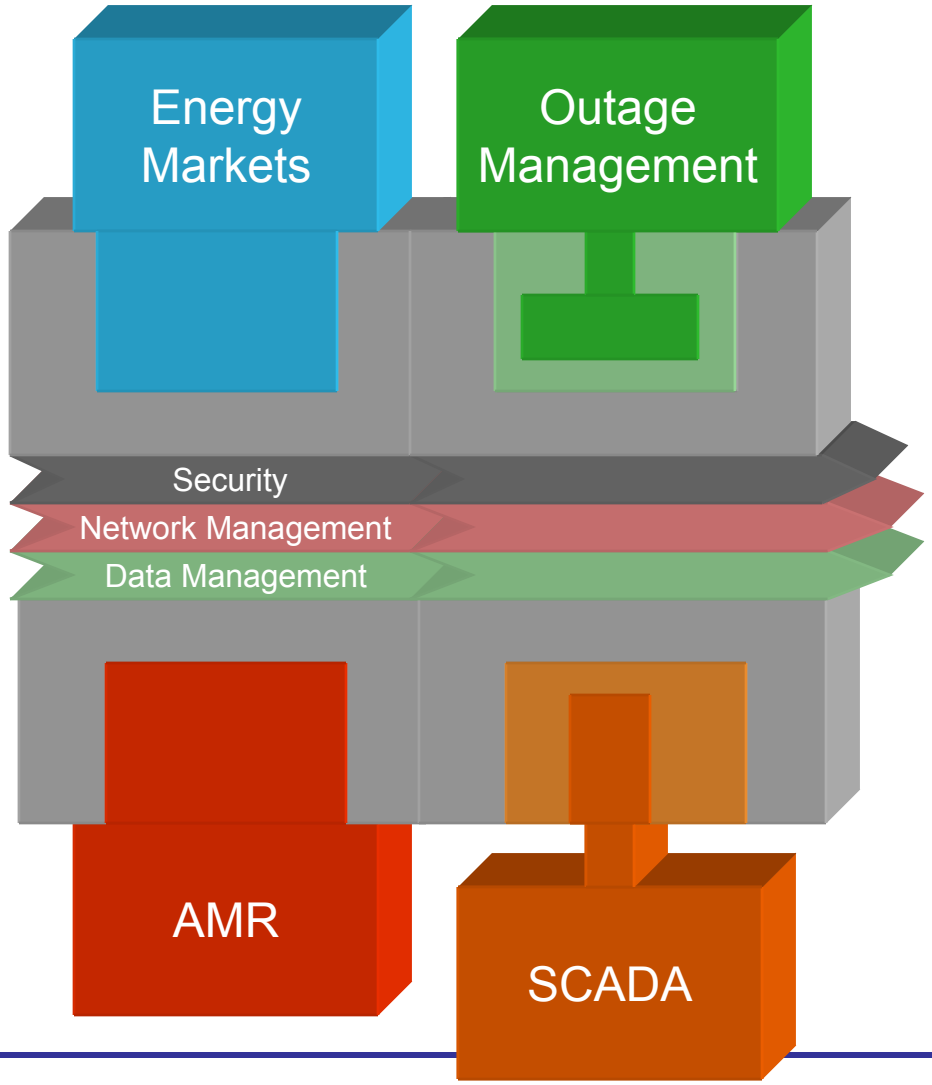


A Better Way: Top-Down Design



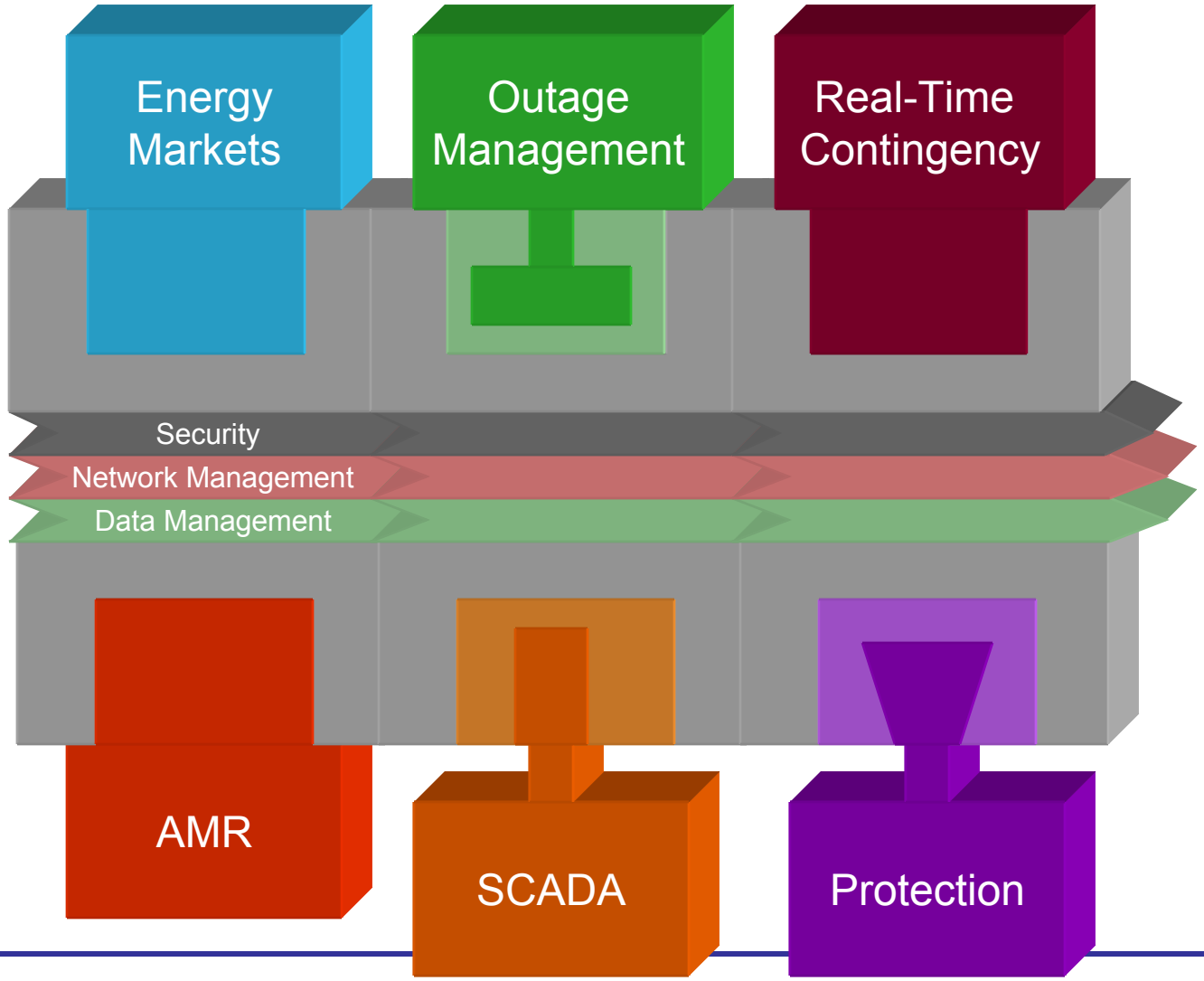
- Define standardized interfaces first
- Incorporate security, network management and other strategies right from the beginning
- Initial costs are a bit more than one-off integration, but not much more
- New applications can build directly to the new architecture

A Better Way: The Next Phase



- Can re-use the development from the first phase
- Expansion was expected
- Adaptation to legacy systems was planned in advance
- Overall costs much lower

A Better Way: And so on…



- Benefits INCREASE with time
- Opposite of the old way

Smart Grid Technology Checklist

- Impact
- Openness
- Standardization
- Security
- Manageability
- Upgradeability
- Scalability
- Extensibility
- Cost-Effective
- Self-Healing
- Interactivity

Criteria for Technology Assessment

- ***Level of Standardization*** - Who recognizes it as a standard?
- ***Level of Openness*** – How easy/costly is it to obtain and use?
- ***Level of Adoption –*** How widely used is it now? In the future?
- ***Users' Group Support*** – Does someone promote it? Improve it? Test it?
- ***Security*** – Can it be secured? Is it inherently secure?
- ***Manageability*** – Can you control, monitor and/or upgrade it remotely?
- ***Scalability*** – Will it work when deployed at a large number of sites?
- ***Object Modeling*** – Does it group and structure data?
- ***Self-Description*** – Can it automatically configure and initialize itself?
- ***Applicability***
  - ***to the Power Industry*** – was it intended for use here?
  - ***to the Consumer Area*** – e.g. metering, building automation?

Technology Assessment

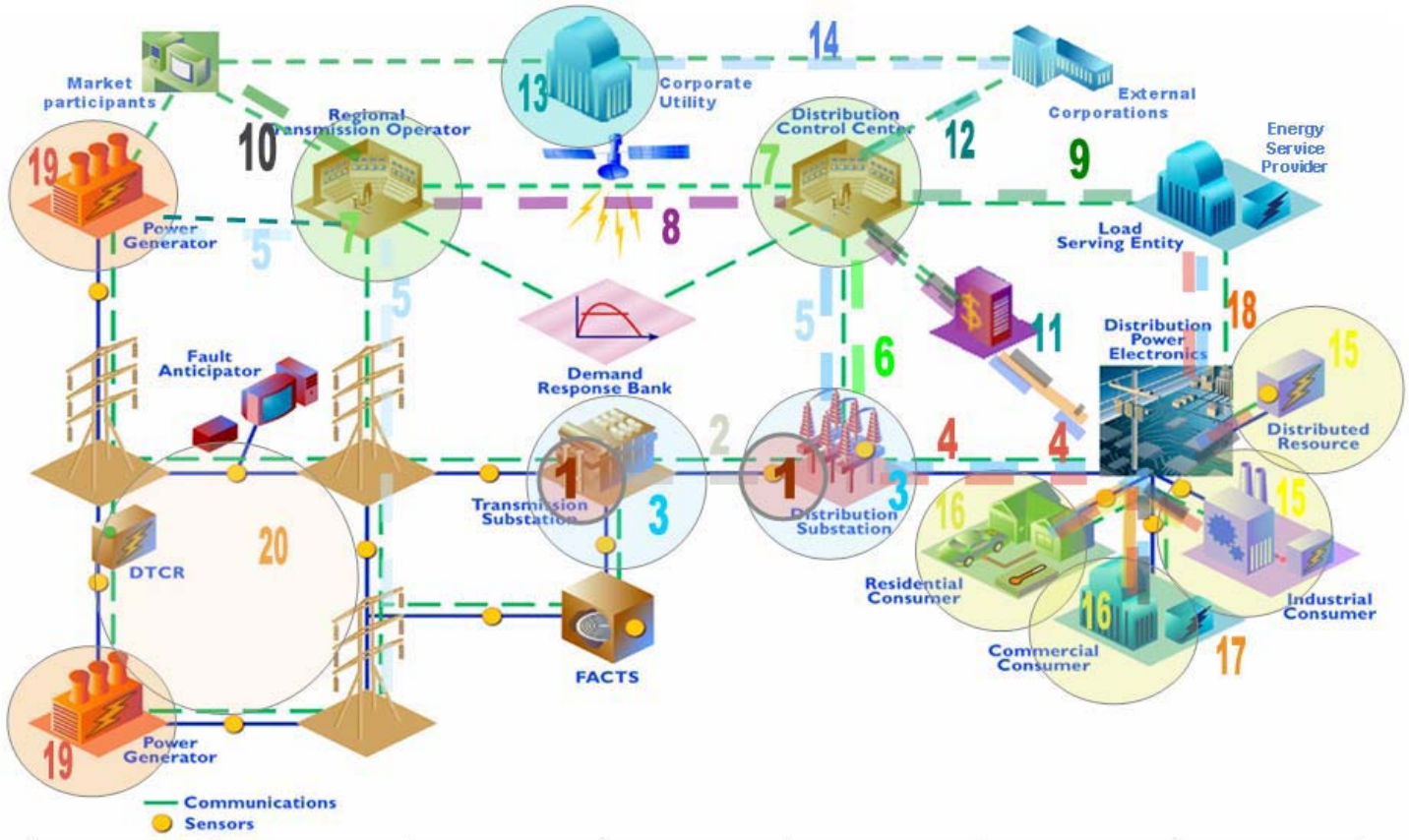
- Group technologies by interface
- Identify pros and cons
- Give each a 1-5 scale rating
- e.g. for standardization:

Rating	Title	Description
1	Proprietary	Not a standard
2	de Facto	Not a standard, but published and widely used
3	Consortia	Standardized by a group of vendors or an industry
4	National	Standardized by a national or regional organization
5	International	Standardized by an international organization

	Standardization	Openness	Adoption	User's Group	Security	Manageability	Scaleability	Object Modeling	Self-Description	Power Industry	Consumer	TOTAL	Bar Graph
Core Networking													
IPv4	3	5	5	4	2	4	4	1	2	3	1	34	
IPv6	3	5	2	4	4	4	5	1	5	2	1	36	
TCP	3	5	5	4	2	4	4	1	2	3	1	34	
UDP	3	5	5	4	1	4	4	1	1	3	1	32	
HTTP	3	5	5	5	2	3	4	1	4	3	1	36	
Security													
TLS	3	5	5	4	5	3	4	1	3	3	2	38	
IPSec	3	5	5	5	5	3	5	1	3	3	2	40	
HTTPS	3	5	5	5	4	2	4	1	4	3	2	38	
SSH	2	4	4	3	5	2	2	1	2	2	2	29	
X.509	5	4	4	1	5	5	3	1	4	3	2	37	
IEEE 802.11i	5	3	2	5	5	4	2	1	2	2	1	32	
Management													
Basic IP	3	5	5	4	1	5	4	1	3	3	3	37	
SNMP	3	5	5	4	2	5	3	4	2	2	2	37	
CMIP	5	3	2	1	3	5	3	4	2	1	1	30	
NTP/SNTP	3	5	5	4	1	5	4	1	2	3	3	36	
IEEE 1588 (PTP)	5	3	2	4	1	5	3	1	2	4	4	34	
Presentation													
HTML	3	5	5	4	2	5	5	4	4	3	3	43	
XML	3	5	5	4	2	5	5	5	4	2	2	42	
BNF	2	5	3	1	1	1	5	5	3	3	3	32	
ASN.1	5	5	5	1	1	1	5	5	3	3	2	36	
IEC 61850-6 (SCL)	5	5	2	5	2	5	2	4	4	4	2	40	
SOAP and Web Servic	3	5	4	4	2	5	2	4	5	2	2	38	
ebXML	5	5	2	4	2	5	2	4	5	2	2	38	
LANs													
Ethernet	5	5	5	1	3	4	3	1	5	3	2	37	
Wi-Fi	5	4	4	5	3	4	2	1	5	2	2	37	
ZigBee	5	4	1	5	4	4	2	1	5	4	4	39	
Bluetooth	5	4	4	5	2	4	2	1	5	1	1	34	
HomePlug	3	3	2	5	3	3	3	1	5	2	2	32	
X10	1	4	5	2	1	1	1	1	5	4	4	29	
WANs													
DSL	5	4	5	5	4	4	4	3	3	2	2	41	
Cable	5	5	5	5	4	4	4	3	3	2	2	42	
WiMAX	5	4	2	5	4	3	3	3	5	1	1	36	
Access BPL	1	2	2	2	3	2	4	1	2	4	4	27	
IEC 61334-5 PLC	5	3	4	1	1	2	3	1	1	5	4	30	
Paging	3	2	5	1	1	2	4	1	5	3	3	30	
Satellite	2	2	2	1	4	4	3	1	1	3	3	26	
Cellular	5	1	2	2	3	4	4	3	5	3	3	35	
FTTH	5	3	2	2	4	4	4	3	3	1	1	32	
Power System Operations													
DNP3	5	4	5	5	2	1	3	2	3	4	2	36	
IEC 60870-5-104	5	4	5	4	2	1	3	2	3	5	2	36	
IEC 61850	5	3	2	5	3	1	3	4	5	5	1	37	
IEC 61968/61970	5	3	2	4	2	1	2	5	5	5	1	35	
IEC 60870-6 TASE.2	5	4	5	4	2	1	2	2	2	5	1	33	
Consumer Application													
ANSI/IEEE C12	5	4	3	2	2	1	4	4	3	5	5	38	
DLMS/COSEM	5	4	3	5	3	1	4	4	3	5	5	42	
BACnet	4	4	4	5	2	1	2	2	2	4	5	35	
EIA 709 (LONWorks)	4	2	3	5	2	2	3	2	3	3	5	34	
Konnex (EN 50090)	4	4	3	5	1	4	2	3	5	3	5	39	

Technology Environment Definitions

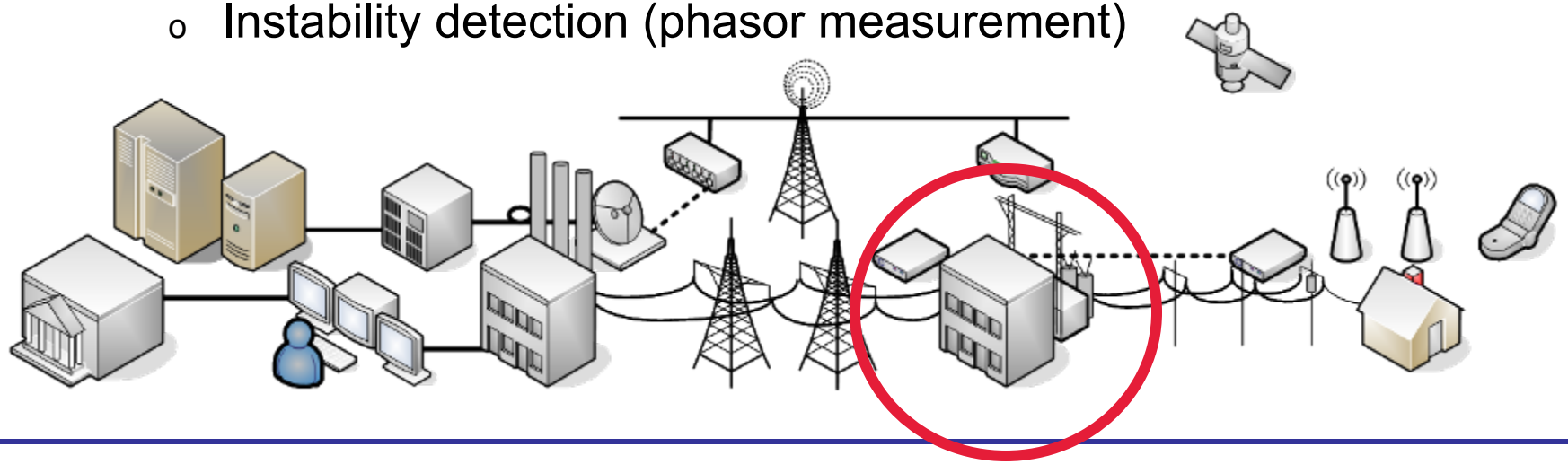
- Identify the major operational areas of utilities
- Identify comms requirements and tech options for each



1 Deterministic Rapid Response Intra-Substation	4 Inter-Field Equipment	7 Intra-Control Center	10 RTOs / Market Participants	13 Intra-Corporation	16 Intra-Customer Site	19 HV Generation Plant
2 Deterministic Rapid Response Inter-Site	5 Critical Operations DAC	8 Inter-Control Center	11 Control Center / Customer Equip	14 Inter-Corporation	17 Inter-Customer Sites	20 Field Equipment Maintenance
3 Critical Operations Intra-Substation	6 Non-Critical Operations DAC:	9 Control Centers / ESPs	12 Control Center / Corporations	15 DER Monitoring and Control	18 Customer / ESP	21 Special

Environments 1, 2 and 3: High Speed Data

- Between and inside substations
- Secure and non-secure
- Within the substation:
  - “Process bus” and “smart CTs”
  - Replacing protection wiring with LANs
- Outside the substation
  - Wide area protection schemes
  - Islanding
  - Instability detection (phasor measurement)



Environments 1, 2 and 3: High-Speed Technologies

- IEC 61850
  - Part 7-2 Generic Object-Oriented Substation Event (GOOSE)
  - Part 7-2 Sampled Measured Values
  - Part 90-1 Between Substations (in progress)
- IEEE C37.118-2005 Phasor Measurement
- Wide-Area Networks
  - SONET (Synchronous Optical Network)
  - ATM (Asynchronous Transfer Mode)
  - Frame Relay
  - DWDM (Dense Wavelength Division Multiplexing)
  - MPLS (Multi Protocol Label Switching)
- Not used with network layer, for performance
- Not really any other options
- Use with satellite time synch e.g. GPS
- IEC 1613 standard for substation networking equipment

Standard Protocol Options – NASPInet RFP

- "The IEC 61850 specification " … "provides a comprehensive model for how power system devices should organize data in a manner that is consistent across all types and brands of devices." However, IEC 61850 is presently limited to the substation in scope, and, while does consider publish-subscribe programming, provides no wide area data delivery mechanisms. However, it is quite possible that wide-area data delivery system built as part of this RFP process could support the delivery of message in the IEC 61850 GOOSE message format."
- WG10 have developed the draft report IEC 61850-90-1 "Use of IEC 61850 for Communications Between Substations" – first step towards extension of the standard (IEC 61850 Update C. Brunner, PAC World)

Example Communication Stds - Transmission/Substations

- Common Information Model – Middleware requirements and application integration
  - IEC 61968 and 61970
  - Generic Interface Definition
- Substation Communications
  - IEC 61850 or DNP3 (IEEE Std 1379) migrating to IEC 61850
  - IEEE Std 1646 – 2004 (Performance)
- Substations IED Configuration
  - Substation Configuration Language (61850-6)
  - DNP XML Schema for configuration
- SCADA – DNP3, IEC 60870-5, IEC 60870-6, IEC 61850
- IEC 61850 approaches for distribution communications
- Phasor Measurement Units – IEEE C37.118-2005
- NERC CIP Requirements for cyber security

- IEC 62351 security guidelines
  - TCP/IP, VPN, IEC 61850
  - DNP3 specifications for secure authentication
- Hardened substation devices
  - IEEE 1613-2003
  - IEC 61850 Part 3 & 5
- Time Synchronization
  - DNP embedded method – supports to +/- 5mSec (adequate for feeder devices in most applications)
  - NTP/SNTP – supports to +/- 10uS
  - GPS – supports to +/- 1 uS (adequate for substation devices in most applications today)
  - IEEE 1588-2002 – to +/- 100 nS
  - Future upgrade to IEEE 1588 Ver 2.0 (will be increasingly required for substation devices in the future)
- COMTRADE and PQDIF for data exchange
  - IEEE C37.111-1999 – COMTRADE
  - IEEE 1159.3 - PQDIF

(See Standards Landscape and Recommendations at GridWise Knowledge Base

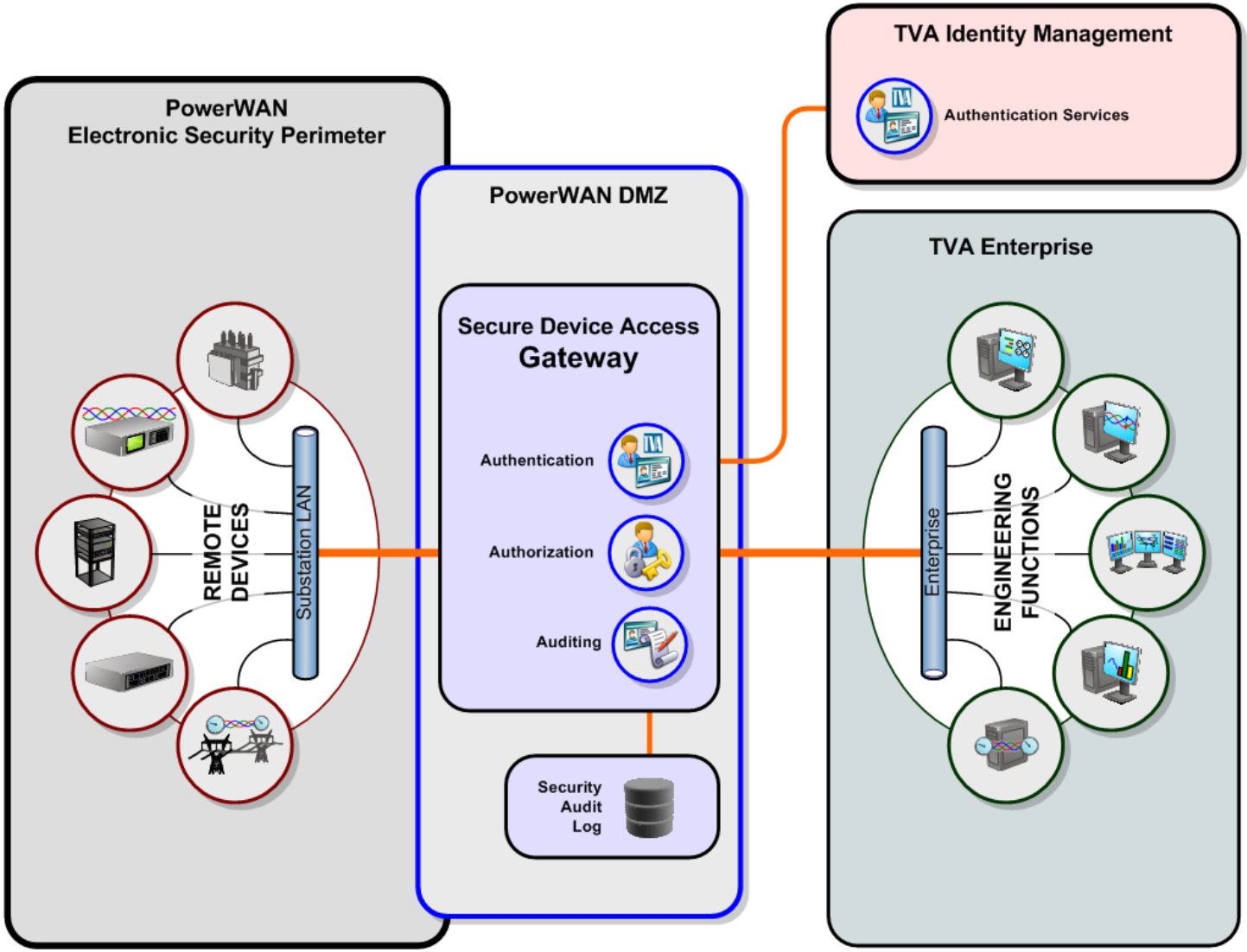
Example Communication Stds–Distribution, AMI & Customer

- Broadband over Powerline (BPL)
- Wireless for Distribution Communications and Metering Communications
  - WiMax (IEEE 802.16)
  - Wireless Mesh Networks
  - ADSL (wired telephone circuits)
  - Cable – DOCSIS
  - BPL – Proprietary but IEEE has begun work on a BPL Standard
  - Cellular – GSM/CDMA
  - Packet-Switched Cellular – CDMA 2000, UMTS (3GSM)
- Metering Information and Communications – ANSI/IEEE C12 Series
  - IEEE 1377/ANSI C12.19 – Meter Data Tables
  - IEEE C12.22 – Trasmitting data tables over a wide area network
- Commercial and Industrial Customer Systems
  - BACnet – ANSI/ASHRAE SSPC 135
  - LONWorks – ANSI/EIA/CEA 709
- Home Area Network (HAN) – Note these protocols can also be applicable for wireless applications in substations
  - Zigbee (IEEE 802.15.4)
  - Wifi (IEEE 802.11)
  - Homeplug BPL
  - X10 PLC

Cyber Security – Example "Bake It In"

- Applicable security functions must be included in the Phasor Measurement System and other intelligent substation devices in accordance with the security policy. Virtual Private Network (VPN) technology is recommended in conjunction with the MPLS WAN. A detailed policy for fully complying with NERC CIP cyber security specifications may include:
  - Authorization and access control
  - Device management
  - Addressing and port management
  - Authentication and credential management
  - Encryption technology
  - Intrusion detection
  - Logging and auditing
- Future compliance with the new and pending network security standards and specifications should be reviewed and considered including:
  - IEC 62351 Part 6
  - IEC 61850 Part 15
- DNP3 - Specification for Secure Authentication (03Feb2007)

Case Study: Remote Device Access



Network Management Policies

- Key functions that need to be performed:
  - Understand current status (up/down/congested)
  - Take corrective action (enable/disable links and devices)
  - Gather audit logs of past events
  - Commission/decommission devices
  - Upgrade configurations and software
- Key principle is the network must be ***UPGRADEABLE!***
- Network Management and security policy closely related
  - Security requires credential management
  - Intrusion detection can help diagnose congestion

Questions?

Erich Gunther
EnerNex Corporation
Knoxville, TN
erich@enernex.com
(865) 691-5540 / 114

Ron Farquharson
EnerNex Corporation
Calgary, AB
ron@enernex.com
(403) 690-0787

EnerNex CORPORATION