

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Emerging Technology Roundtable - Cloud Computing on the Bulk Electric System

November 16, 2016

RELIABILITY | ACCOUNTABILITY



Cloud Computing on the Bulk Electric System

- 8:30 am Opening remarks and Introductions
 - *Mark Lauby, Senior Vice President and Chief Reliability Officer, NERC*
 - *Tobias Whitney, Senior Manager of CIP Compliance, NERC*
 - *Tom Hofstetter, Senior CIP Compliance Specialist, NERC*
- 9:00 am – 10:00 am – Overview of Cloud Services
 - *Jianhui Wang, Ph.D., Section Manager – Advanced Power Grid Modeling, Energy Systems Division, Argonne National Laboratory*
- 10:00 am – 11:00 am – Building the business case for Cloud Services
 - *Jeff Gooding, IT Principal Manager, Enterprise Architecture & Strategy, Southern California Edison (SCE)*
 - *Xiaochuan Luo, Technical Manager, Business Architecture & Technology, ISO New England*
- 11:00 am – 12:00 pm – Describing the Architecture of Cloud Offerings
 - *Stevan Vidich, Ph.D., Principal Program Manager, Azure Global Ecosystem engineering team, Microsoft*
- 12:00 pm – 1:00 pm – Lunch
- 1:00 pm – 2:00 pm – Security and CIP compliance considerations during Deployment
 - *Tobias Whitney, Senior Manager of CIP Compliance, NERC*
- 2:00 pm – 4:00 pm – Roundtable Discussion, Industry and Vendor Experiences
- 4:00 pm – 4:30pm – Closing and Next Steps
 - *Tobias Whitney, Senior Manager of CIP Compliance, NERC*



Questions and Answers

TransitionProgram@nerc.net

A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications

Jianhui Wang

Energy Systems Division,
Argonne National Laboratory

NERC Emerging Technologies Roundtables

November 16, 2016

Presentation Outline

1. Introduction to Cloud Computing
2. Project Overview
3. Progress to date
4. Conclusions



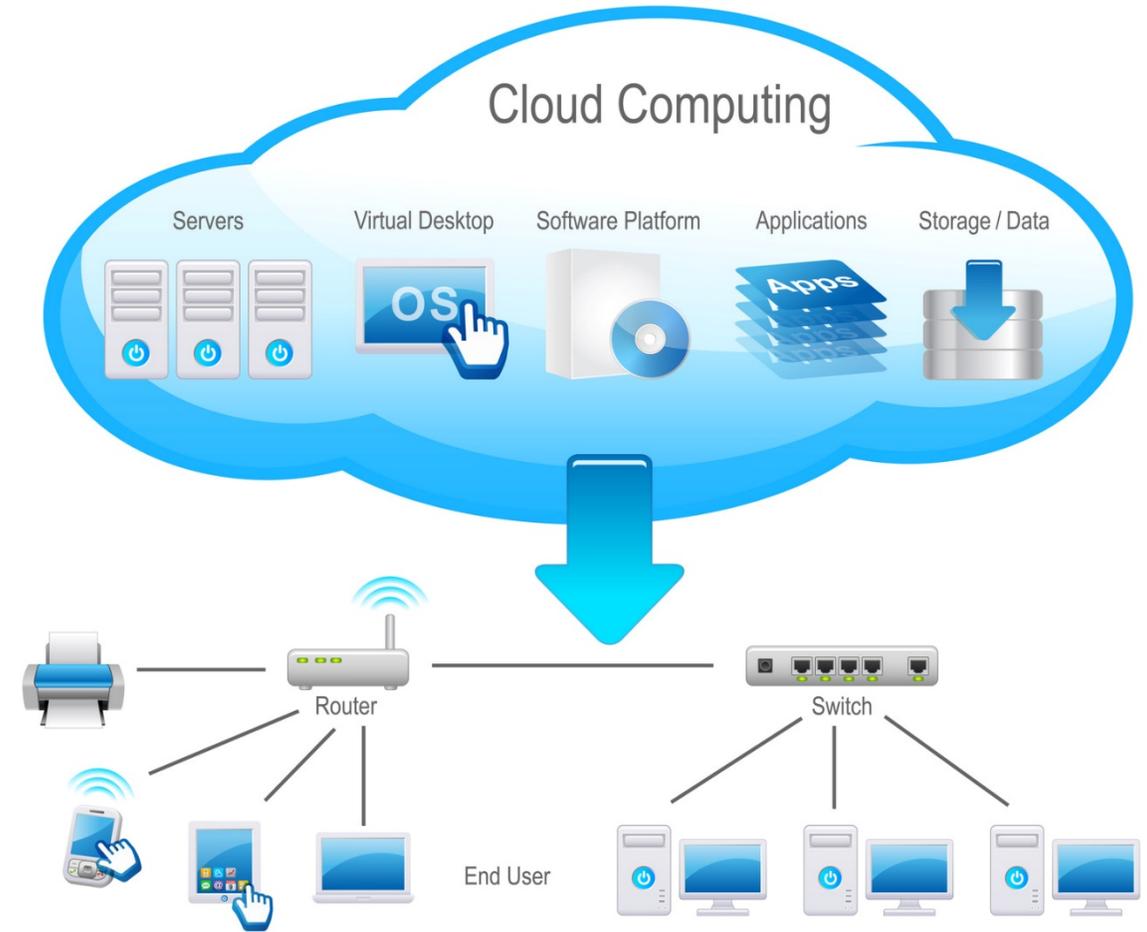
Introduction to Cloud Computing

What is it, the Need, Benefits, and Challenges



What is Cloud Computing?

- **Cloud Computing** is an umbrella term used to refer to Internet-based development and services
 - a group of integrated and networked hardware, software and Internet infrastructures
 - Using the Internet for communication and transport provides hardware, software and networking services to end-users
- Cloud platforms **hide the complexity** of the underlying infrastructure from users by providing **simple graphical interfaces**



Essential Characteristics of Cloud Computing

1. Resource Pooling

- No need to have servers in-house
- Reduce the need for advanced hardware in-house

2. Broad Network Access

- Data is available anytime, anyplace, and anywhere
- Secure backup and disaster recovery of data

3. Rapid Elasticity

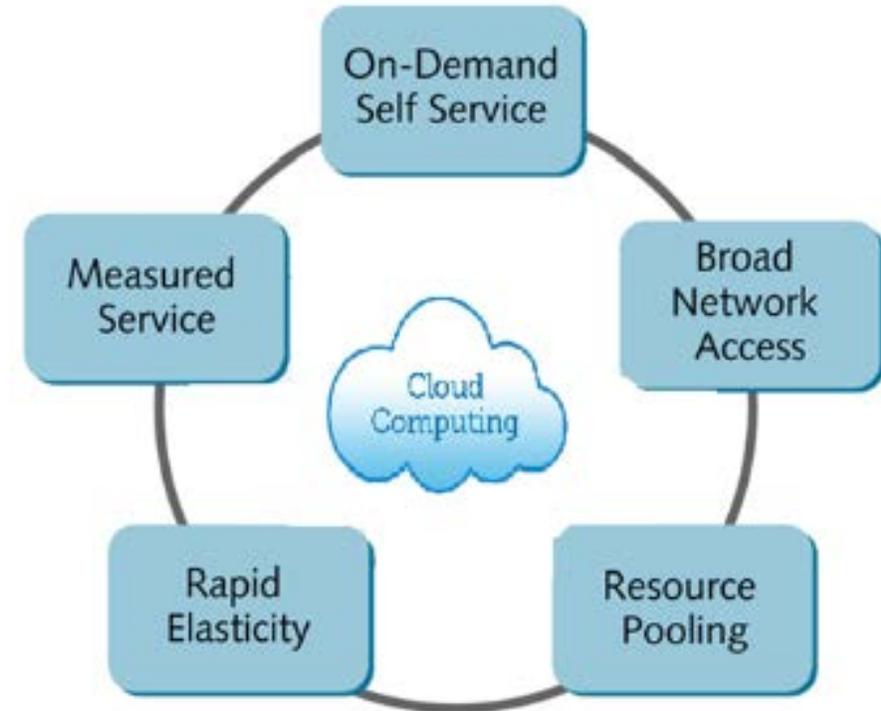
- Quickly scale operations

4. On-Demand Self Service

- Pay for only your use

5. Measured Service

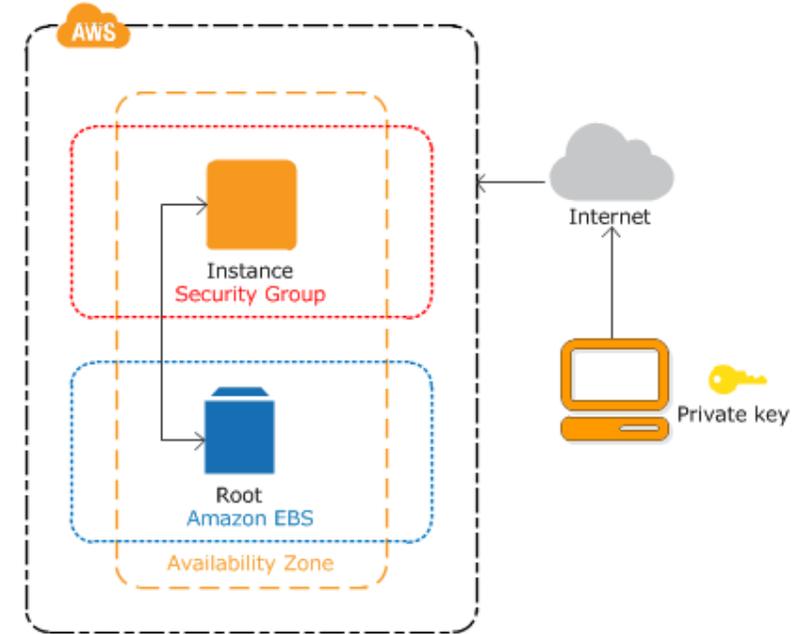
- Resource usage can be monitored, controlled, and reported
- Transparency



Characteristics defined by NIST

Example of a Cloud Provider → Amazon EC2

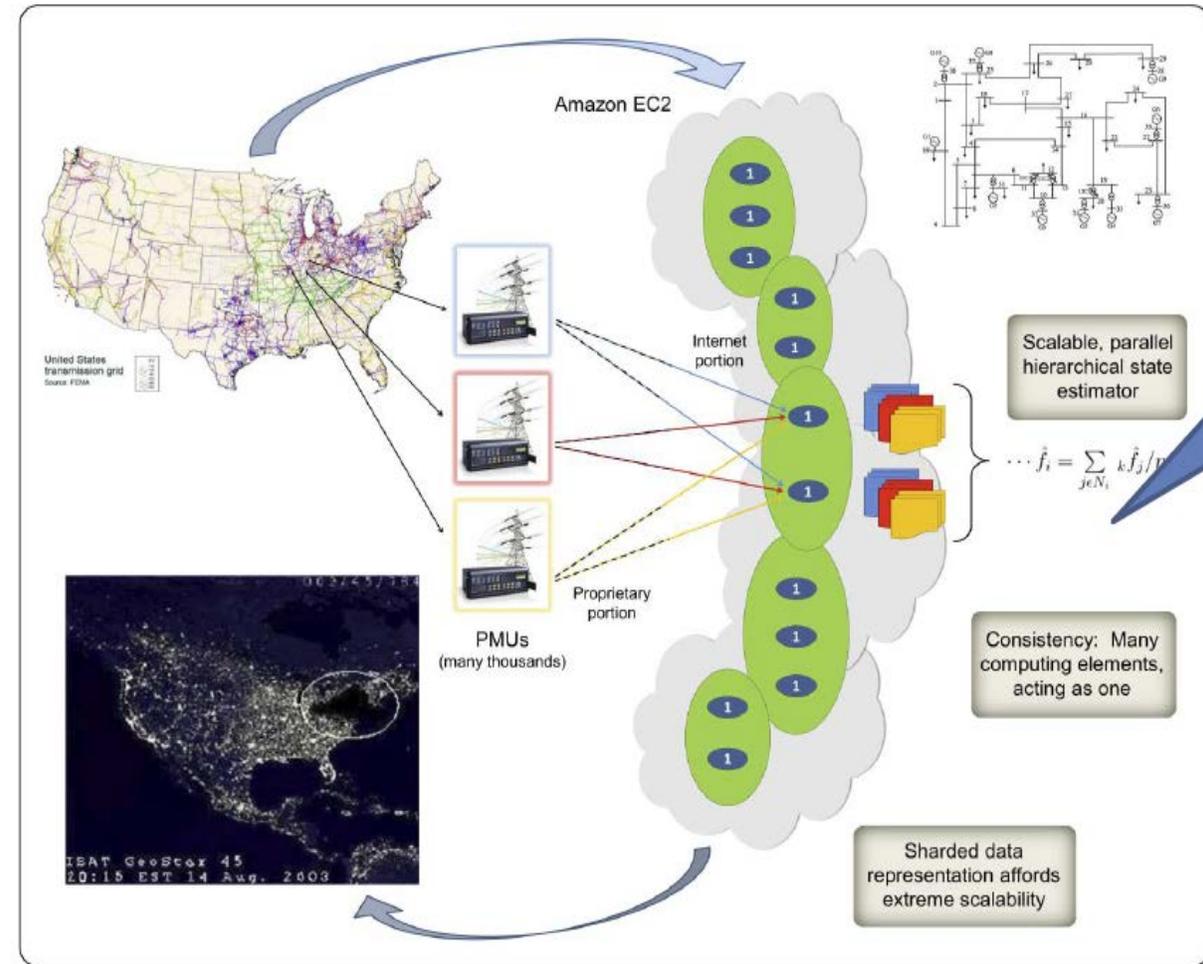
- Amazon EC2 is a widely-used platform in the cloud computing industry
- Typical services:
 - **Elastic**: increase or decrease capacity within minutes
 - **Full control**: direct root access to each cloud instance
 - **Flexible**: choose your Operating System and install any software packages
 - Redhat, Ubuntu, Windows Server, among others
 - Small, large, extra large instances based on disk space, RAM, and CPUs
 - **Reliable**: Amazon servers provide high availability and redundancies
 - **Secure**: firewall settings, private key management, and Virtual Private Clouds (VPC) available



Amazon Cloud Overview

The Need for Cloud Computing for Power Grid Applications

- Advent of smart grid technologies is causing simulations to increase in size
- Computationally intensive power grid applications include:
 - Wide-area state estimation
 - Contingency analysis
 - Security-constrained economic dispatch (SCED)
 - Security-constrained unit commitment (SCUC)
 - Faster-than-real-time grid dynamics simulation and analysis
 - Production cost simulation
 - On-line stability analysis
- In-house computing infrastructure is not flexible to solve such intensive applications
- Computational complexity hinders market development



Courtesy of Ken Birman

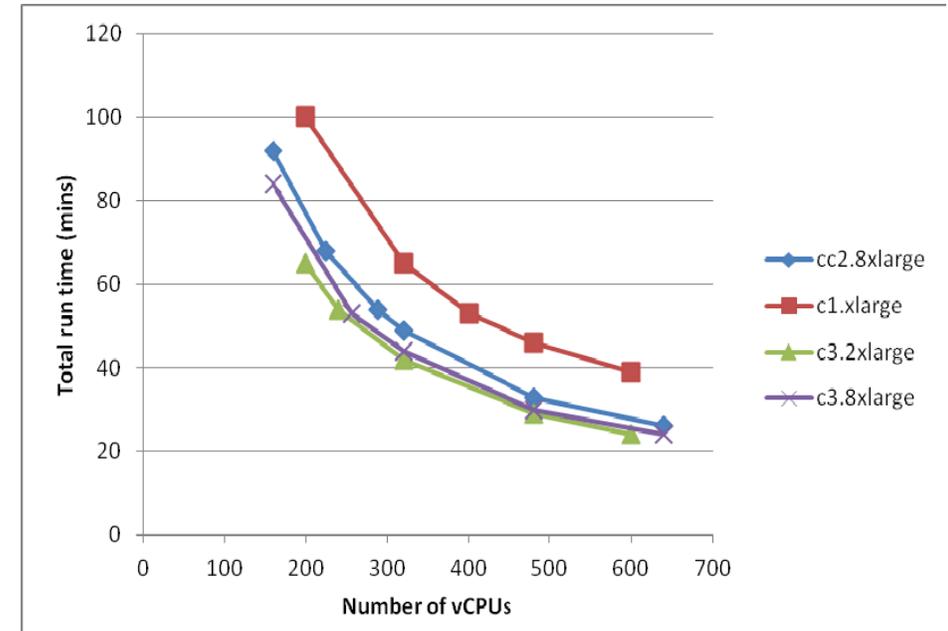
Benefits of Cloud Computing to System Operators

- System Operators currently exploit **High Performance Computing (HPC)** on **local in-house infrastructures**
 - Requires high-capital expenditures
 - Requires maintenance staff
 - Limits rapid scalability for power grid applications
- Cloud computing provides:
 1. **Powerful computational capacity** (e.g., Amazon EC2's go up to 128 CPUs)
 2. **Unparalleled scalability** (e.g., cloud instances can be launched quickly)
 3. **High cost-effectiveness**
- Typical in-house HPC cost is significantly higher than cloud-based HPC
 - *e.g.*, 2.88 \$/hour in-house compared to 0.84 \$/hour for Amazon EC2 cloud¹



Current State-of-Art of Cloud Computing for Grid Applications

- ISO-NE is at the forefront of cloud-hosted grid applications²
 - Platform for real-time PMU data collection, storage, and processing to achieve Wide Area Monitoring
 - HPC platform for large-scale simulations
 - Transmission Planning Studies (stability analysis, etc.)
 - Resource Adequacy studies
 - Software on the cloud: TARA, GE MARS, PSS/E, TSAT
- Majority of applications are focused on Grid Planning as opposed to Grid Operations
- Research and development of cloud-based operation models (e.g., SCUC, SCED) are needed



Total runtime for 7,090 TARA N-1-1 Planning Studies performed by ISO-NE

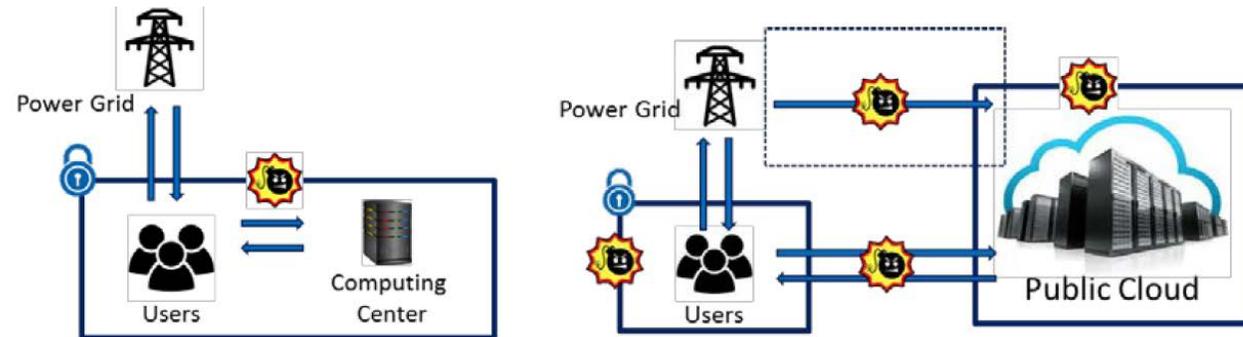
² E. Litvinov, F. Ma, Q. Zhang, and X. Luo, "Cloud-based next-generation IT paradigm for the operations of future power systems," in 2016 Power Systems Computation Conference (PSCC), June 2016, pp. 1–7.

Challenges in Cloud Computing for Grid Operations

Three major challenges exist:

1. Infrastructure security

- Confidentiality and integrity of data-in-transit to and from cloud providers
- Outside attackers compromise data in transmission
- Inside attackers comprise a user or a cloud provider



Traditional Scenario vs. Cloud Scenario

2. Data confidentiality

- Grid data must be kept confidential
- Grid data must remain unaltered

3. Time criticality

- Power system applications require timeliness assurance
- Data must be time-consistent, requiring high-speed data synchronization

Project Overview

A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications

Overview of Framework, Cyberattacks, and Potential Approaches



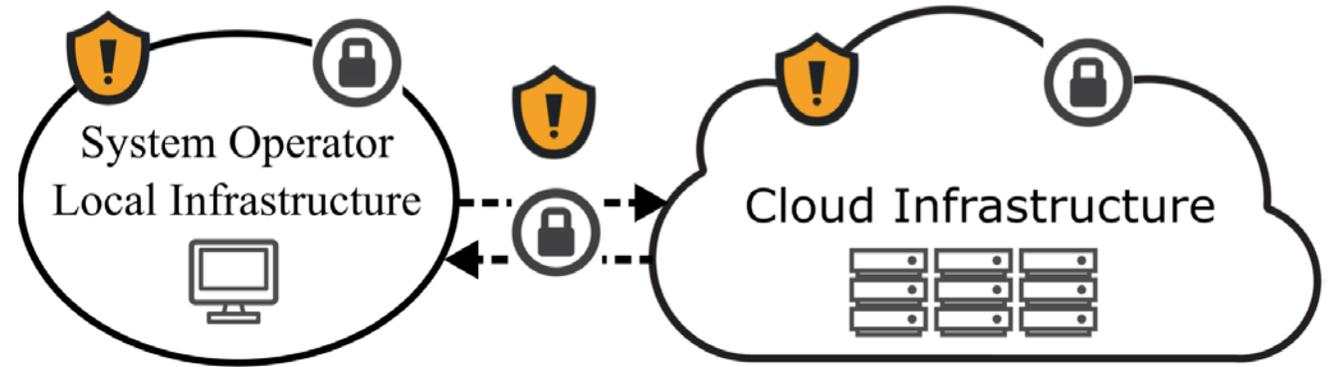
Project Synopsis

Objective

- The computational complexity of power grid applications is increasing
- Cloud computing provides *powerful computational capacity, scalability, and high cost-effectiveness*
- **Goal:** Develop a secure and trustworthy cloud computing and outsourcing framework for power grid applications

Project Schedule

- Started August 2016
- Framework and white paper (Q2 2017)



Performer: Argonne National Laboratory

Partners: University at Buffalo, Illinois
Institute of Technology

Federal Cost: \$1,500,000

Cost Share: N/A

Total Value of Award: \$1,500,000

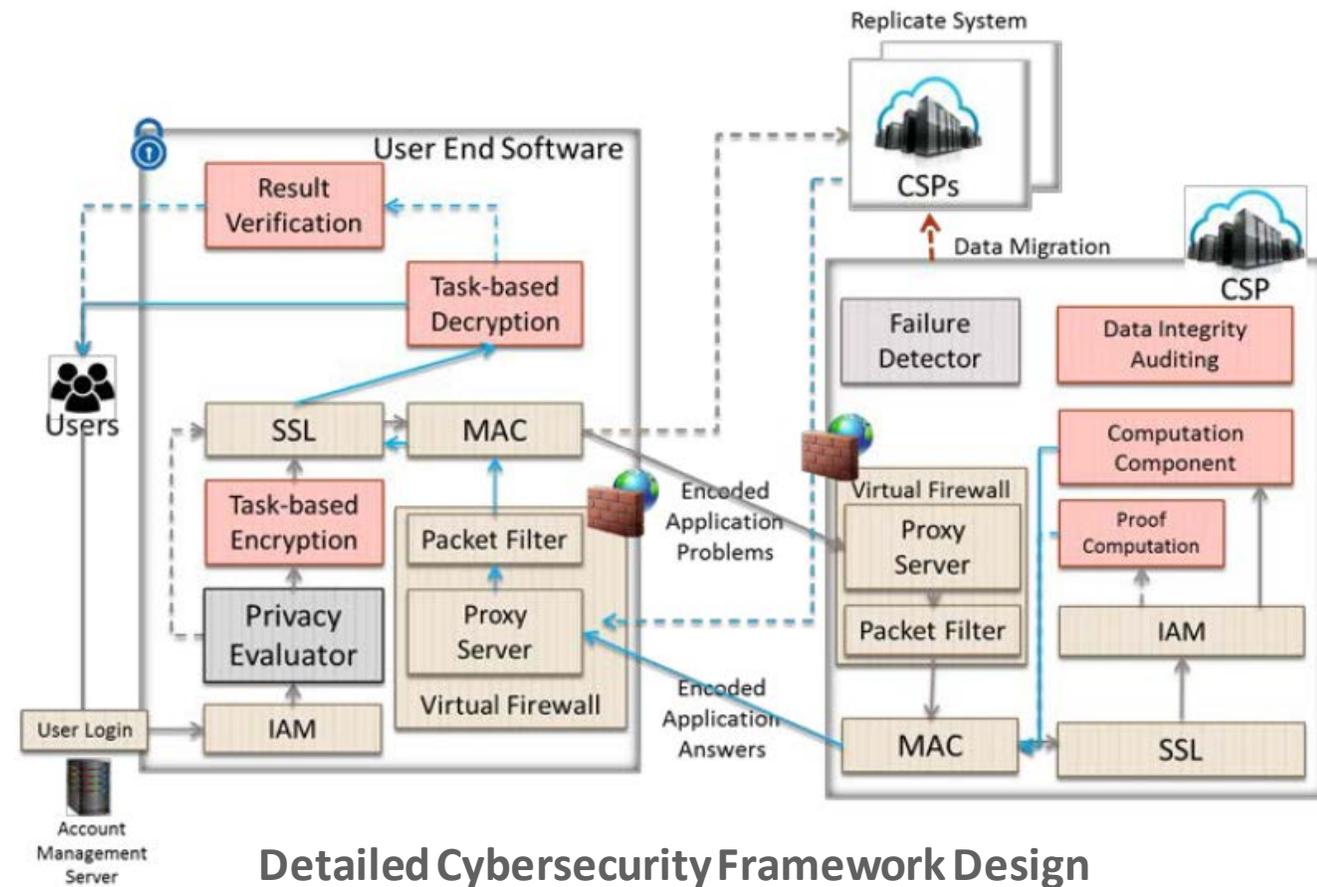
Project Objectives

1. Design a comprehensive cloud-based framework for power grid applications
2. Model/quantify the security and time criticality requirements of grid applications
3. Deploy grid applications with different time criticality requirements in cloud
4. Model/quantify different types of cyberattacks against grid applications
5. Deploy security enhancements to cloud-based power grid applications.
6. Recommend cybersecurity improvements
7. Demonstrate best practices in cybersecurity for cloud-based grid applications

Comprehensive Cloud and Outsourcing Security Framework for Power Grid Applications

Develop a comprehensive framework that considers:

- **Infrastructure Security:** ensure data-in-transit is secured
- **Data confidentiality:** ensure confidentiality and integrity of grid data outsourced to the cloud
- **Time critical:** ensure system efficiency, computation efficiency, communication efficiency, and cloud provider availability

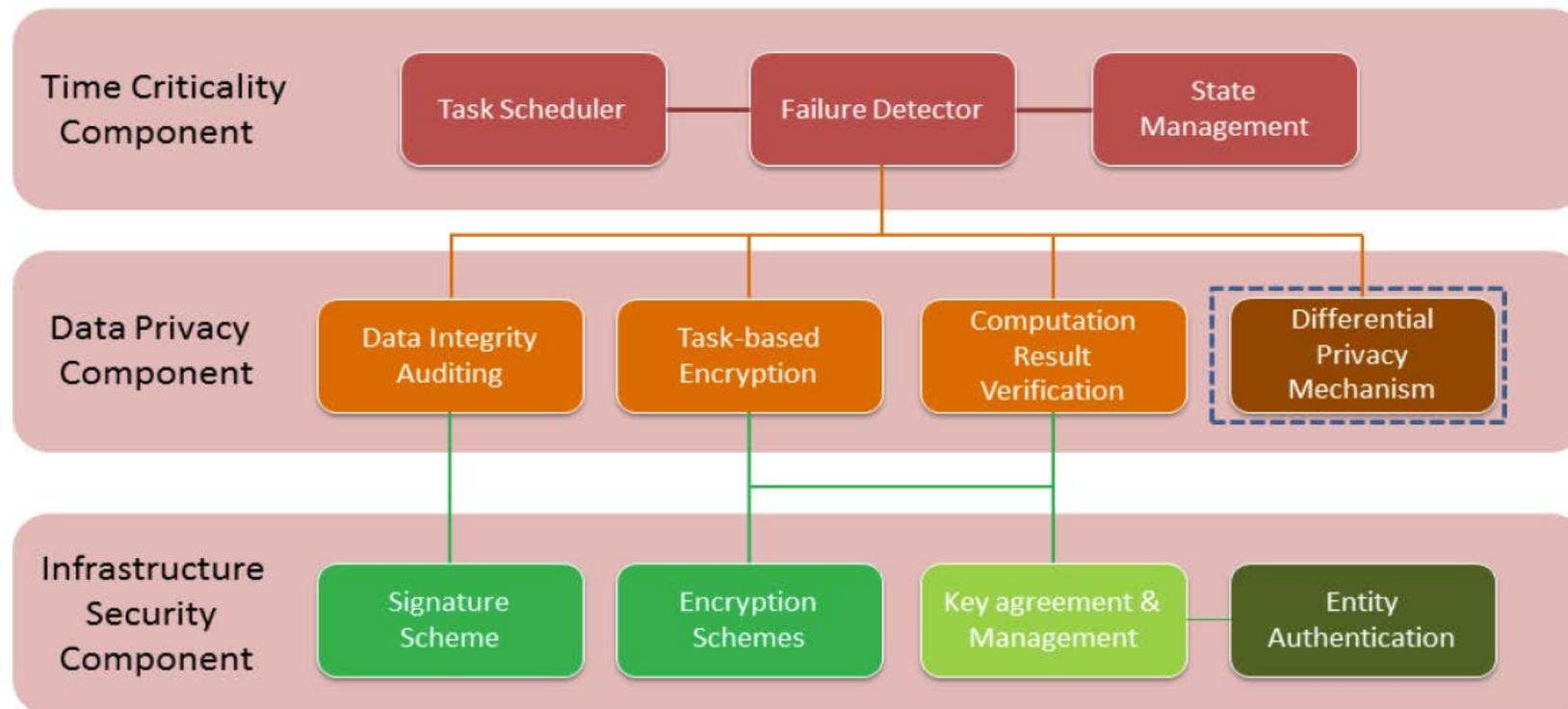


Detailed Cybersecurity Framework Design

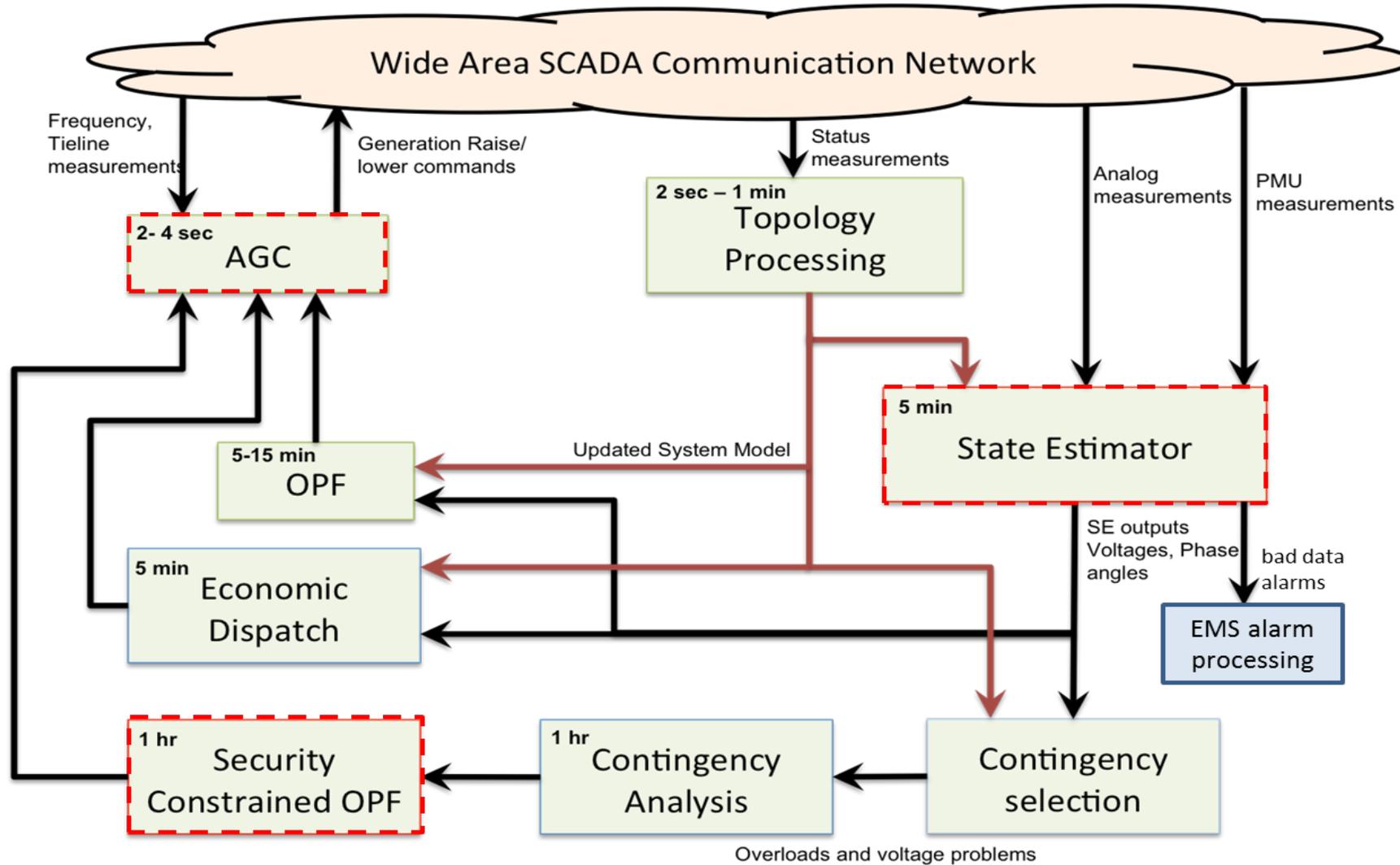


Module-based Components for Grid Computing Framework

- Each grid application is unique in its computational, security, and time requirements
- Develop flexible module-based components that include Infrastructure Security, Data Confidentiality, and Time Criticality
 - Modules can be customized to each grid application's needs



Fundamental WAMPAC Applications and Their Time Scales



What types of Cyberattacks?

Cyberattacks may result from two groups - *insiders* and *outsiders*

Within the insider group are passive and active entities

- **Passive:** monitor communication channel between the user and the cloud
- **Active:** attacks to alter system resources, *e.g.*, flood attack, spoofing attack

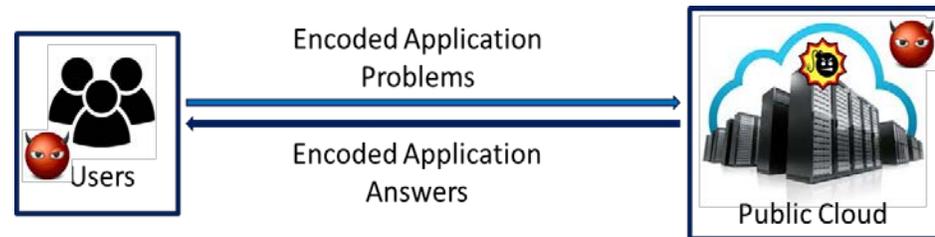


Illustration of Outsider Attackers

Within the outsider group are compromised users and cloud providers, or malicious administrators

- **User:** compromise infrastructure security
- **Cloud provider:** compromise data confidentiality
- **Administrator:** obtain sensitive data

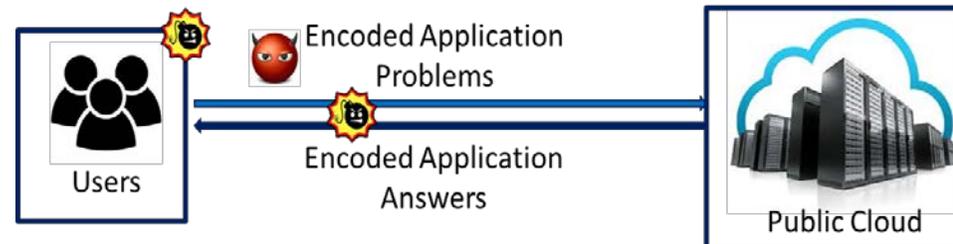
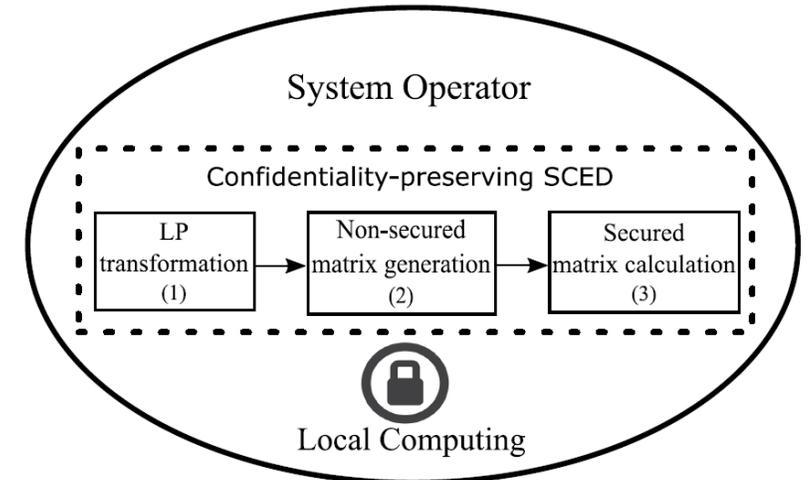


Illustration of Insider Attackers

Progress to Date

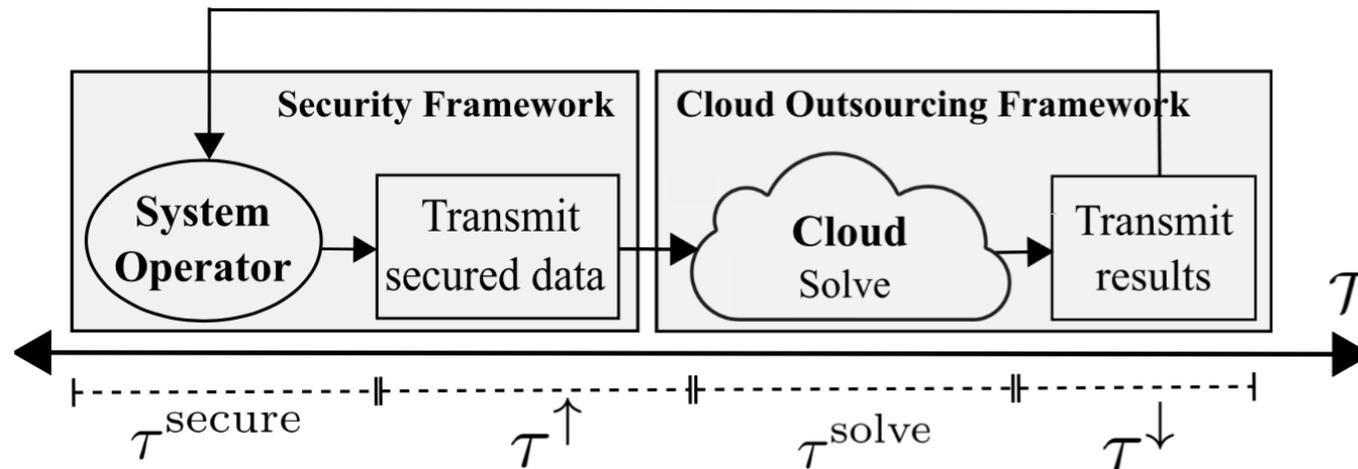
Major Accomplishments to-date

- Industry Advisory Board consisting of a diverse group of individuals applying cloud computing:
 - Xiaochuan Luo, ISO-NE
 - Alex Rudkevich, Newton Energy Group
 - Jianzhong Tong, PJM
 - Tobias Whitney, NERC
- Two papers under preparation
 - Security and Cloud Outsourcing Framework for Security-Constrained Economic Dispatch
 - Fast Encryption Scheme for Cloud-based SCUC Problem Outsourcing System
- Framework report and white paper being developed



Preliminary Technical Approach

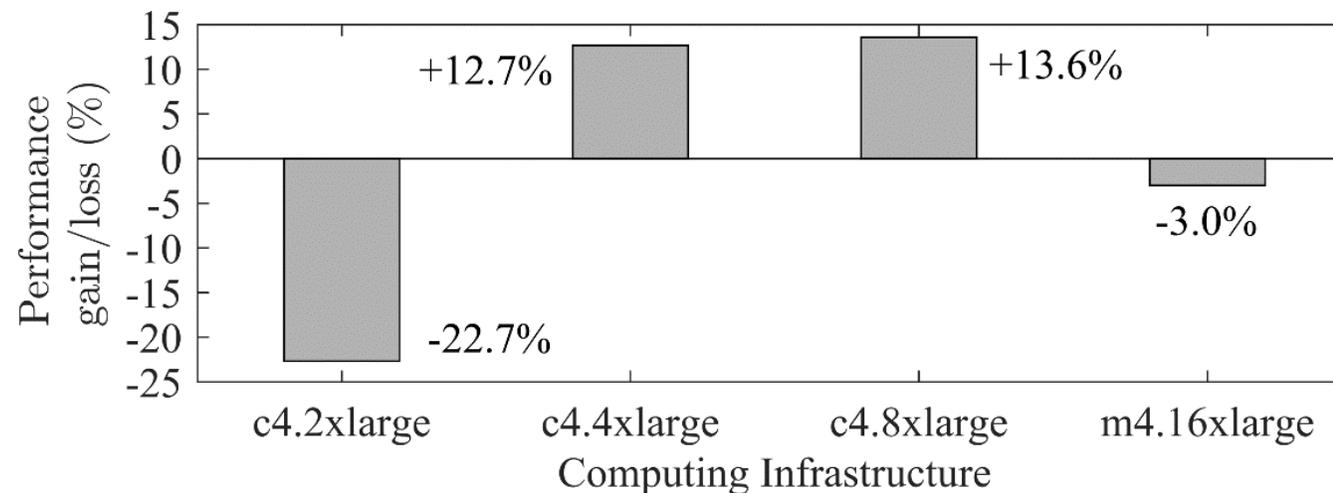
- Grid data must be kept confidential while in transmission and storage on the cloud
 - Various techniques (e.g., encryption, cryptography) will be explored
 - Mathematical models (SCED, SCUC) can be reconstructed to consider confidentiality
 - Leverage existing works in fields of Communications, Operational Research, among others
- Development of Confidentiality-Preserving SCED and SCUC models
 - Must conform to market rules, e.g., $\tau^{\text{solve}} + \tau^{\downarrow} \leq 5\text{-min}$ if market operates under 5-min



Security and Outsourcing Flow Chart

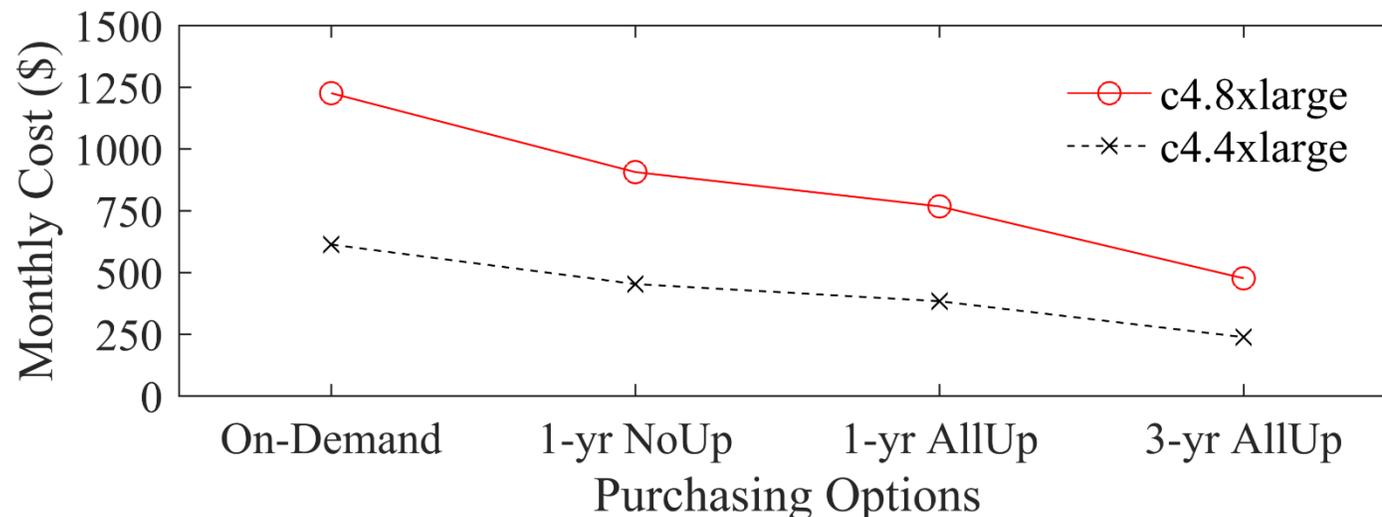
Results: Security-Constrained Economic Dispatch (SCED) on the Cloud

- In recent work, a confidentiality-preserving SCED was developed and simulated on
 - Argonne National Laboratory's (ANL) Blues HPC cluster
 - Four (4) Amazon EC2 instances
 - C4.2xlarge → less compute-optimized than ANL blues
 - C4.4xlarge and c4.8xlarge → more compute-optimized than ANL blues
 - M4.16xlarge → more memory-optimized than ANL blues
- A comparison of the **computational performance gain** against ANL Blues was performed



Results (cont.): Cost Savings of SCED on the Cloud

- Amazon EC2 has different payment options, such as:
 - Pay as used with no commitments (on-demand)
 - 1-year contract with no upfront payment (1-yr NoUp)
 - 1-year with full upfront payment (1-yr AllUp)
 - 3-year with full upfront payment (3-yr AllUp)
- A **monthly cost comparison** was performed for compute-optimized EC2s and ANL Blues
 - ANL Blues cost is \$2073.6 → EC2 provides max. savings of **88.5%** with increased performance



Collaboration/Technology Transfer

- Technology will conform to operating paradigms of system operators
 - Enable ease of implementation and high impact to business processes
- Testing will occur on large-scale datasets to ensure applicability and scalability
 - PJM and ComEd grid datasets will be used
- End-users may be but not limited too:
 - 1. System Operators:** directly implement on cloud services (*e.g.*, Amazon EC2, Microsoft Azure, among others)
 - 2. Software-as-a-Service (SaaS):** entity can host and maintain the technology framework for a usage/service fee
 - 3. Software-as-a-Product (SaaP):** entity can sell licenses of the technology to practicing users



Conclusions

- Cloud Computing is a paradigm-shifting technology for the Power System
- A comprehensive Cloud Security and Outsourcing Framework must:
 - Ensure infrastructure security, data confidentiality, and time criticality
 - Be economical against in-house infrastructures
 - Provide computational performance gains that justify the paradigm shift
 - Conform to market operating rules in practice today
- This project attempts to identify the benefits, challenges, and applicability to specific grid applications



An aerial photograph of the Argonne National Laboratory campus, showing various buildings, parking lots, and green spaces. The text "Questions?" and "THANK YOU!" is overlaid in the upper center of the image.

Questions?
THANK YOU!

Jianhui Wang

Energy Systems Division

ARGONNE NATIONAL LABORATORY

9700 South Cass Avenue, Bldg. 362

Argonne, IL 60439

Tel: +1 630-252-1474

jianhui.wang@ANL.gov

Cloud Storage & Security for Sensitive & Protected Data

Jeff Gooding
Southern California Edison
IT Principal Manager
Enterprise Architecture & Strategy

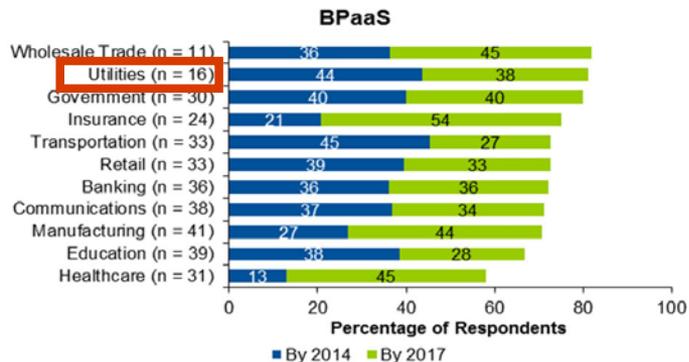
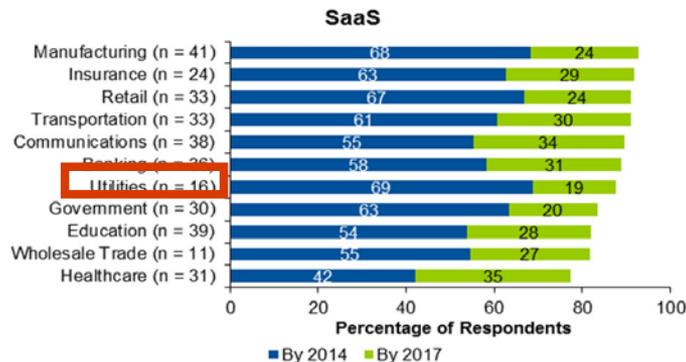
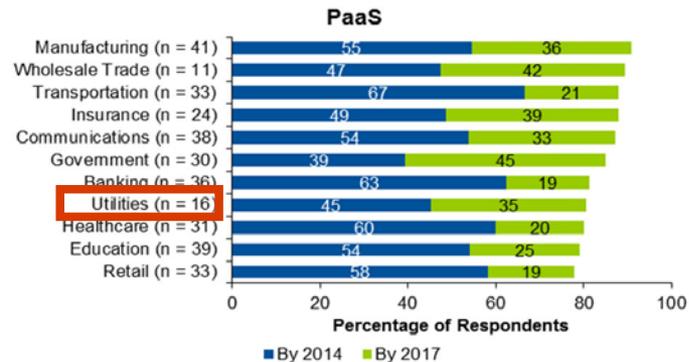
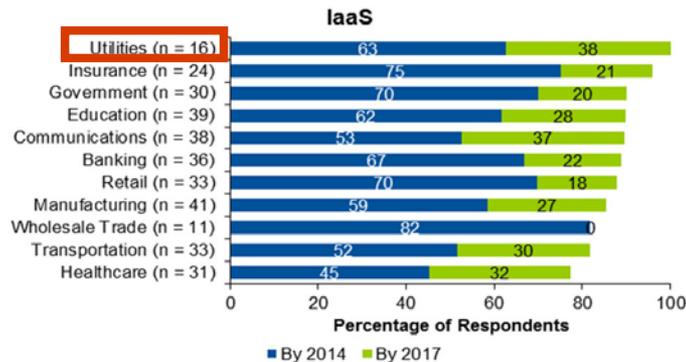
November, 2016

Big Data from the Electric Grid

- Synchro phasors, Intelligent Relays, Transformers, Switches and other IEDs on the electric grid & connected to control centers are creating increasingly vast amounts of data each day.
- Grid modernization will dramatically increase the number of sensors and control devices on the electric grid over the decade.
- Big data from the grid will yield high operational value through engineering, analytics, simulations and situational awareness applications
- To maximize the value of this data, storage, access, security and compliance requirements must be met at a reasonable cost.
- Securely transmitting and storing grid data in the cloud will allow utilities to realize the full value of the data created by systems and sensors deployed on the electric grid.

Cloud service usage trends by industry

When cloud usage is examined across all cloud service types in aggregate, **the utilities industry** is overall the most progressive in current and planned usage, followed by the insurance, communications and retail industries



- When considering current usage only, and when usage is taken in aggregate, respondents from the retail industry indicated the broadest current use of cloud services, across all cloud service types, followed by utilities, government and wholesale trade
- When considering planned usage of cloud services, across all cloud service types, respondents from the healthcare industry indicated the most planned adoption, followed by the communications, manufacturing and transportation industries

Source : Gartner Survey, Cloud Adoption Across Vertical Industries , Feb 2015

Investment in Public Cloud Services by Industry

The highest percentage of organizations having made significant investments in public cloud were found in the manufacturing and banking industries. In contrast, only 30% of government organizations reported having made a significant public cloud investment.



SaaS is the most common and the most widely used type of cloud service, regardless of industry.

Source : Gartner Survey, Cloud Adoption Across Vertical Industries , Feb 2015

Top drivers of public cloud adoption

The most significant driver for cloud adoption is overall cost reduction across industries

	Manufacturing (n = 25)	Communications (n = 24)	Government (n = 18)	Education (n = 23)	Retail (n = 16)	Wholesale Trade (n = 7)	Banking (n = 25)	Insurance (n = 19)	Healthcare (n = 22)	Transportation (n = 20)	Utilities (n = 11)
Improved development environment (faster time to deployment, easy to develop, access to development tools)	44%	21%	50%	50%	53%	25%	18%	-	33%	-	-
Business advantage (revenue growth, customer growth, customer retention)	31%	21%	42%	19%	41%	50%	18%	40%	11%	38%	60%
Overall cost reduction	44%	43%	33%	25%	53%	75%	55%	100%	33%	31%	60%
Public cloud services are more environmentally friendly	19%	21%	25%	31%	35%	25%	45%	20%	22%	46%	40%
Financial considerations (moving from capital expenditure to operating expenditure, tax advantages, and so forth)	13%	14%	17%	31%	24%	25%	27%	-	22%	23%	-
Operational agility and scaling (ability to react quickly to opportunities)	50%	36%	42%	25%	12%	-	45%	20%	44%	23%	20%
Innovation to be gained from cloud services	50%	29%	42%	19%	24%	-	9%	80%	33%	54%	20%
Business units prefer public cloud models	25%	36%	17%	25%	6%	25%	27%	20%	-	15%	40%
Cloud computing is a more modern computing approach	25%	36%	33%	25%	41%	25%	27%	20%	78%	62%	20%

Next highest response Next highest response

Source : Gartner Survey, Cloud Adoption Across Vertical Industries , Feb 2015

Top inhibitors of public cloud adoption

The most significant inhibitor for cloud adoption is security and privacy concerns

	Manufacturing (n = 16)	Communications (n = 14)	Government (n = 12)	Education (n = 16)	Retail (n = 17)	Wholesale Trade (n = 4)	Banking (n = 11)	Insurance (n = 5)	Healthcare (n = 9)	Transportation (n = 13)	Utilities (n = 5)
Time to deployment	12%	17%	17%	13%	13%	29%	12%	11%	5%	5%	9%
Difficulty of development	12%	17%	6%	-	13%	14%	4%	11%	18%	25%	9%
Lack development tools and resources	16%	21%	6%	13%	6%	-	12%	5%	14%	15%	-
Dislike for release schedules and impact on my application life cycle management	12%	8%	11%	9%	6%	14%	4%	11%	9%	-	-
Data integration challenges	40%	21%	28%	35%	13%	14%	32%	11%	41%	25%	-
Lack of cloud service provider options	20%	8%	6%	13%	13%	14%	16%	-	9%	15%	-
Insufficient SLAs from cloud service providers	12%	13%	28%	9%	13%	-	4%	37%	14%	15%	18%
Security and/or privacy concerns	44%	63%	72%	57%	69%	86%	72%	68%	73%	50%	64%
Lack of internal skills to manage public cloud services	36%	42%	17%	26%	13%	-	12%	16%	14%	20%	45%
Compliance requirements prevent public cloud usage	16%	21%	39%	9%	25%	29%	24%	32%	27%	10%	45%
Concerns about government snooping	12%	21%	17%	39%	56%	14%	28%	47%	27%	30%	18%
Public cloud services are not environmentally friendly	20%	8%	6%	4%	13%	14%	4%	-	9%	-	9%
Data center locations don't meet data sovereignty requirements	12%	25%	17%	17%	19%	29%	24%	16%	5%	30%	18%
Others	-	-	-	4%	-	-	-	-	-	5%	-

Next highest response

Next highest response

Source : Gartner Survey, Cloud Adoption Across Vertical Industries , Feb 2015

Cloud storage is easy to use, durable, highly available, and secure...how can we leverage it?

- Data generated by grid devices and systems and used for operational decision making or is sensitive enough to expose the utility to increased risk of cyber attack must be protected in accordance with compliance and cyber security policies
- To meet this requirement:
 - Data should be encrypted outside of the protected control systems networks
 - The utility shall maintain key sovereignty (ability to manage, revoke, roll keys and access to encryption keys at all times)
 - Ability to use cybersecurity tools in the cloud to review access to the encrypted data
 - Audit and non-repudiation controls for data transfers and retrieval
 - Assurance from the cloud vendor that vulnerabilities and appropriate cyber controls are in place.

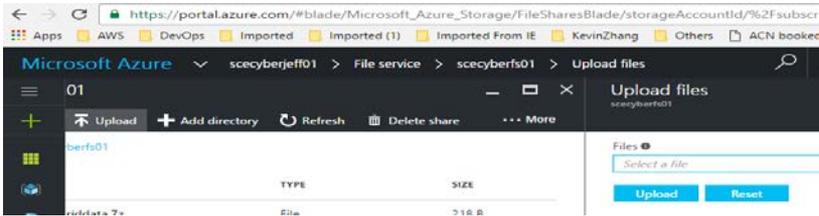
Encryption models provide various levels of assurance

Encryption Models

Server Encryption			Client Encryption
<p>Server Side Encryption using <u>service managed keys</u></p> <ul style="list-style-type: none"> Azure services can see decrypted data <u>Microsoft manages the keys</u> Full cloud functionality 	<p>Server side encryption using <u>customer managed keys</u> in Azure KeyVault</p> <ul style="list-style-type: none"> Azure services can see decrypted data <u>Customer controls keys via Azure Key Vault</u> Full cloud functionality 	<p>Server side encryption using on-prem customer managed keys</p> <ul style="list-style-type: none"> Azure services can see decrypted data <u>Customer controls keys On-Prem</u> Full cloud functionality 	<ul style="list-style-type: none"> Azure services cannot see decrypted data <u>Customer keep keys on-premises</u> <u>REDUCED cloud functionality</u>

Encrypt data with SCE keys, secure transfer and store the file in cloud storage

3 Using Azure portal to https the encrypted file to a cloud file share on Azure



dummygriddata - Notepad

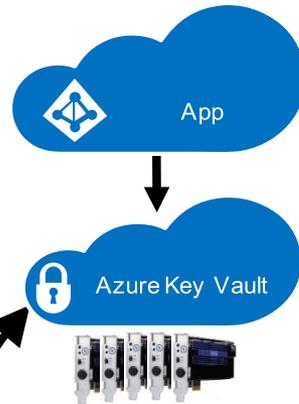
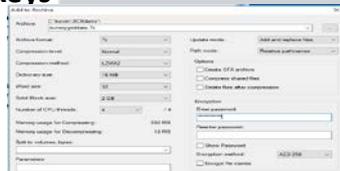
2 Encrypted content in flight and at rest denies access to data

```
File Edit Format View Help
|7z%~' 00^6@ z Ñ
+Áx Yz°SLü"°šÁâMÿp000 0 @
d u m m y g r i d d a t a
```

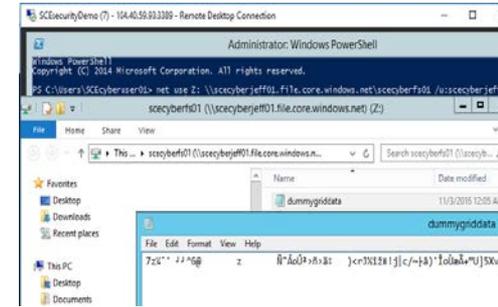
1 Encrypt data with SCE keys

dummygriddata - Notepad

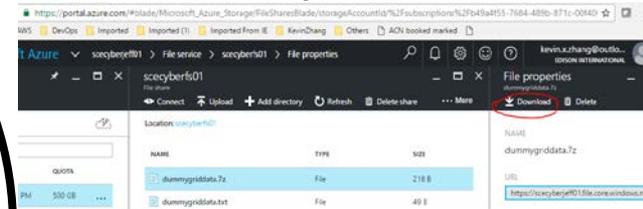
```
File Edit Format View Help
|This is dummy grid data for SCE
Grid circute 101
```



4 Display the encrypted file in a windows server on Azure, only encrypted content is displayed



5 Use Azure portal https to download the same data back to my Control Center



6 Use key to un-encrypt the data within the Control Center

On Your Premises

dummygriddata - Notepad

```
File Edit Format View Help
|This is dummy grid data for SCE
Grid circute 101
```

Beyond Cloud Storage – Using Cloud Services

All my data is in the cloud and many services are available to make it more valuable...how do I access services?

What is Azure Key Vault?

An Azure resource provider that lets you

1. Store & manage **SECRETS** (esp app config), and release them to authorized apps & users.
2. Store & manage **KEYS**, and perform cryptographic operations in isolated service.

Backed by Hardware Security Modules (HSM)

All secrets and keys are protected at rest with key chain terminating in HSMs.

Keys marked as 'HSM-protected' are protected even at runtime with HSMs.

Key Vault ≠ customer's dedicated HSM

Azure Key Vault is a multi-tenant service backed by Microsoft-managed HSMs.

Encryption – all choices

Case 1: Only your code needs to see data.

Encrypt on your own. Store keys in either Azure Key Vault, external hoster, or on-premises.

Case 2: You pass data to one or more Microsoft PaaS/SaaS services

<i>PaaS/SaaS service →</i>	<i>Azure Storage</i>	<i>SQL DB & SQL Server</i>	<i>O365 at rest</i>	<i>O365 w/ RMS</i>	<i>VMs</i>	<i>ML</i>
MS service can see decrypted data. Microsoft manages your keys. Full cloud functionality.		Transparent Database Encryption	Bitlocker, File level encryption	Azure RMS	Azure Disk Encryption	
MS service can see decrypted data. You control keys via Azure Key Vault. Full cloud functionality.			Advanced Encryption	Azure RMS w/ BYOK	Azure Disk Encryption	
MS service cannot see decrypted data. You keep keys on-premises. REDUCED cloud functionality.	Client-side Encryption	AlwaysEncrypted		ADRMS + AzureRMS	N.A.	N.A.

Questions?





Application of Cloud Computing at ISO New England

NERC Emerging Technology Roundtables

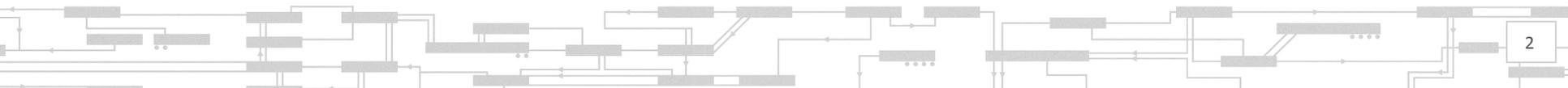
Xiaochuan Luo

TECHNICAL MANAGER

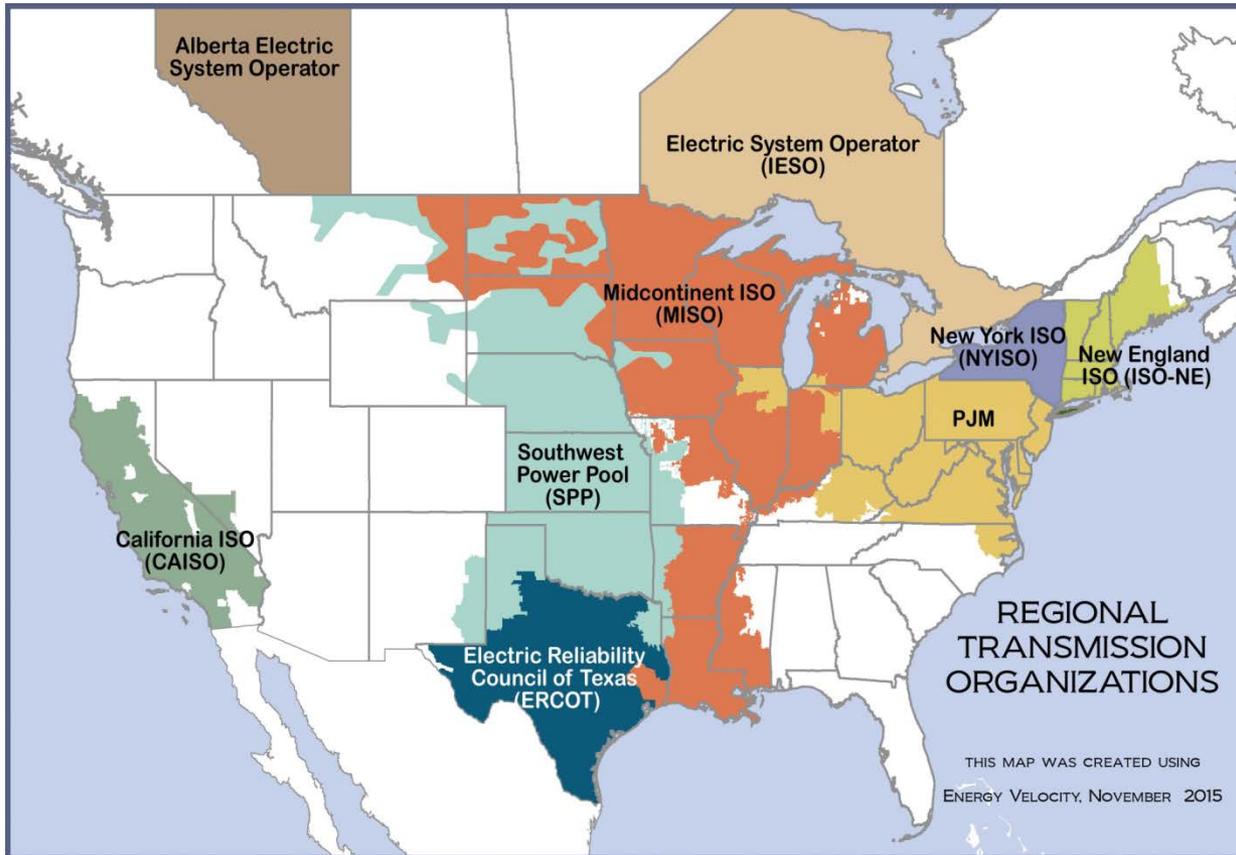


Outline

- Overview of ISO New England
- Cloud computing and new opportunities
- Application 1:
 - High performance computing needs in power system modeling and simulations
 - Deploy power system analysis software in the cloud
- Application 2:
 - Synchrophasor technology, wide area monitoring and situational awareness
 - Cloud-hosted wide area monitoring
- Conclusions



Overview of ISO New England



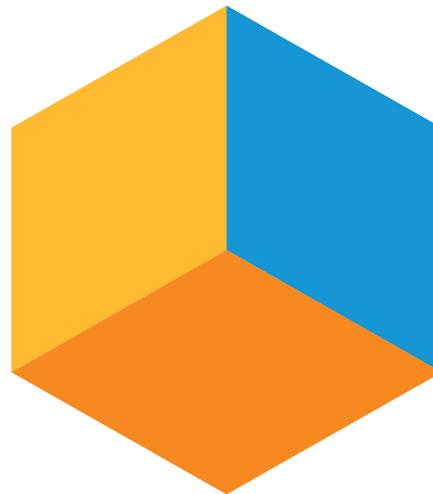
- **350** Generators
- **31,000** MW of generating capacity
- **8,600** miles of high voltage transmission lines (115 kV and above)
- **13** transmission interconnections to New York and Canada
- 6.5 million households and business; 14.7 million population
- **28,130** MW all-time summer peak demand set on August 2, 2006

Reliability Is the Core of ISO New England's Mission

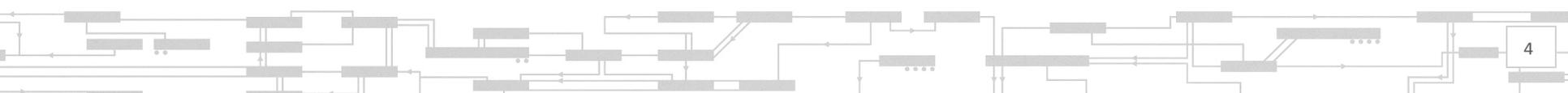
Fulfilled by three interconnected and interdependent responsibilities

Overseeing the day-to-day, reliable **operation** of New England's electric power generation and transmission system

Managing comprehensive regional power **system planning**

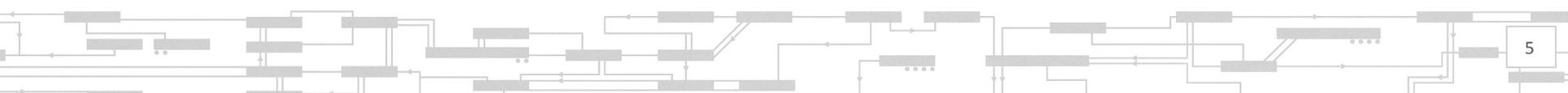


Developing and administering the region's competitive **wholesale electricity markets**



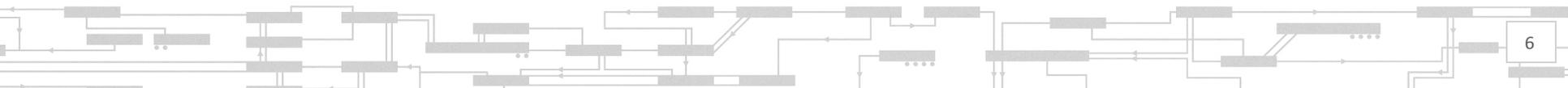
Cloud Computing and New Opportunities

- Cloud computing technology has matured and been adopted in many industries
 - On-demand self-service
 - Broad network access
 - Resource pooling
 - Rapid elasticity
 - Measured service
- New opportunities
 - High performance computing
 - Big data capture, processing and storage
 - Data sharing and exchange
 - Shared applications for regional collaboration

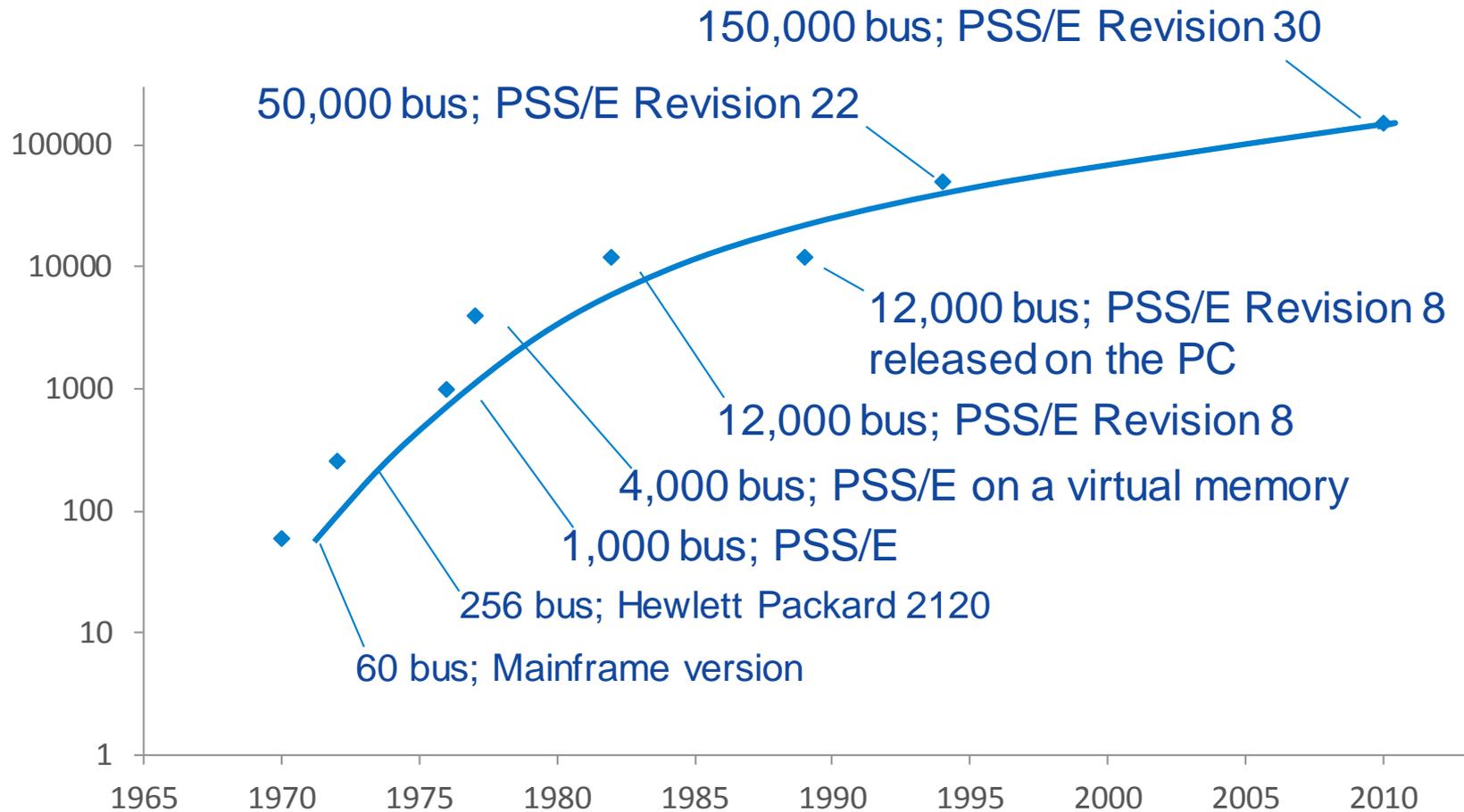


Outline

- Overview of ISO New England
- Cloud computing and new opportunities
- **Application 1:**
 - High performance computing needs in power system modeling and simulations
 - Deploy power system analysis software in the cloud
- **Application 2:**
 - Synchrophasor technology, wide area monitoring and situational awareness
 - Pilot cloud-hosted wide area monitoring
- Conclusions



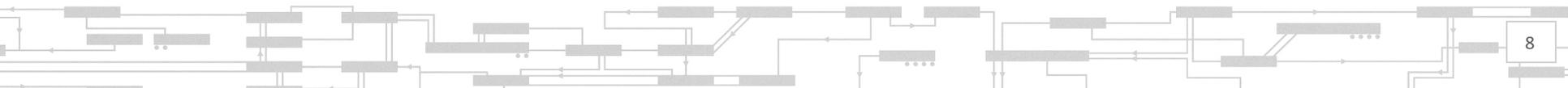
Evolution of Network Model Size in PSS/E



Evolution of Network Model

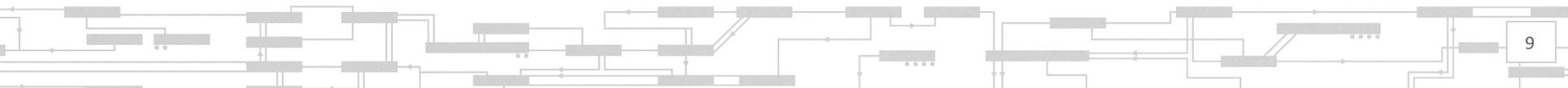
High Performance Computing Needs

- Transmission Planning
 - Needs assessment, solutions studies, economic studies
 - Long range time horizon (1 to 10+ years) with many scenarios
 - N-1, N-1-1 contingency analysis (NERC TPL-001-4)
 - Thermal, voltage, and dynamic stability simulations
- Examples:
 - Southeast Massachusetts and Rhode Island assessment
 - 36 power flow cases, 295 first level contingencies, 2,122 second level contingencies
 - $36 * 295 = 10,620$ scenarios; each takes about 6 minutes
 - $10,620 * 6 = 63,720$ minutes = 1,062 hours
 - Maine Power Reliability Program (MPRP) stability study
 - 11 power flow cases, 477 dynamic contingencies
 - One 30-second dynamic simulation takes about 15 minutes in PSS/E
 - $11 * 477 * 15 = 78,705$ minutes = 1,312 hours
- Expected increase in penetration of wind/solar generation will further increase the computational requirements



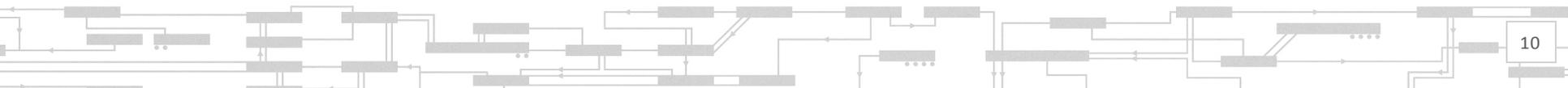
High Performance Computing Needs (Cont.)

- NPCC Bulk Power System (BPS) testing
 - Performance-based test which determines whether an event at a specific location on the transmission system would have a significant adverse impact outside of the local area
 - A substation's BPS status must be re-examined after any major transmission or generation addition or retirement
 - Any interface transfer limit increase requires BPS testing across the entire New England system
- A full BPS assessment involves simulation of a fault on every transmission bus in New England, across at least four to six generation dispatches
 - A recent re-assessment tied to a transfer limit increase in Northern New England involved over 7000 fault simulations
- NPCC Document *A-10 Classification of Bulk Power System Elements*



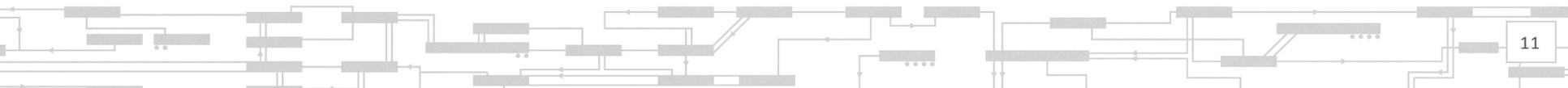
High Performance Computing Needs (Cont.)

- Resource adequacy studies
 - Probabilistic study using Monte Carlo simulation to determine installed capacity requirements, tie benefits, etc.
 - Typically users run 1000 replication years, which takes around 10 hours
 - Number of sensitivities
 - Each replication is independent and can be parallelized
- Operations Planning
 - Line and generation outage conditions
 - Different load levels (peak, shoulder and light load)
 - Different stress conditions (generation dispatch) at each load level
 - Hundreds of contingencies (N-1)
 - Close to two hundred stability operating guides



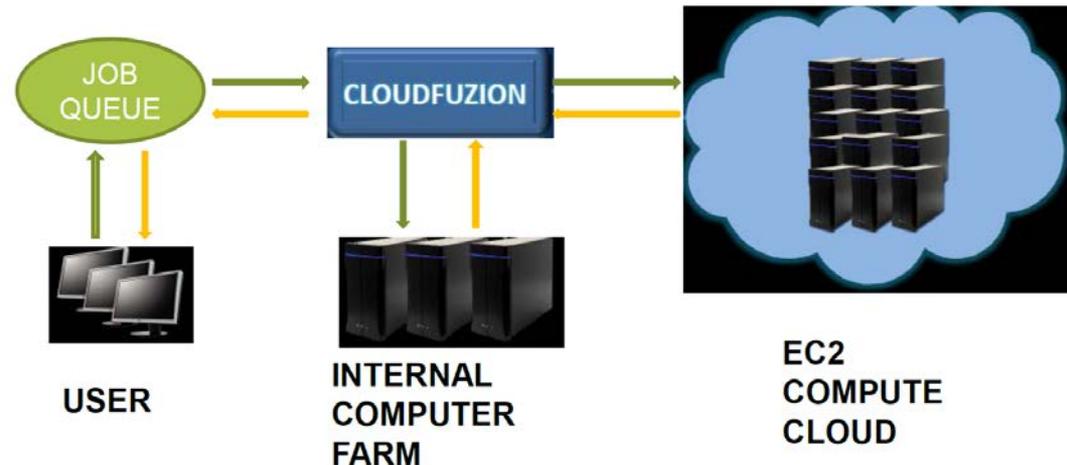
High Performance Computing Needs (Cont.)

- Other computation challenges:
 - ElectroMagnetic transient simulations
 - Stochastic Unit Commitment
 - Security constrained AC OPF
 - Unit commitment and economic dispatch with corrective actions (N-1 and N-1-1 security constraints)
 - Long-term market simulations (DAM-RTM-AGC)
 - Mid-term and long-term generation and transmission outage coordination
 -

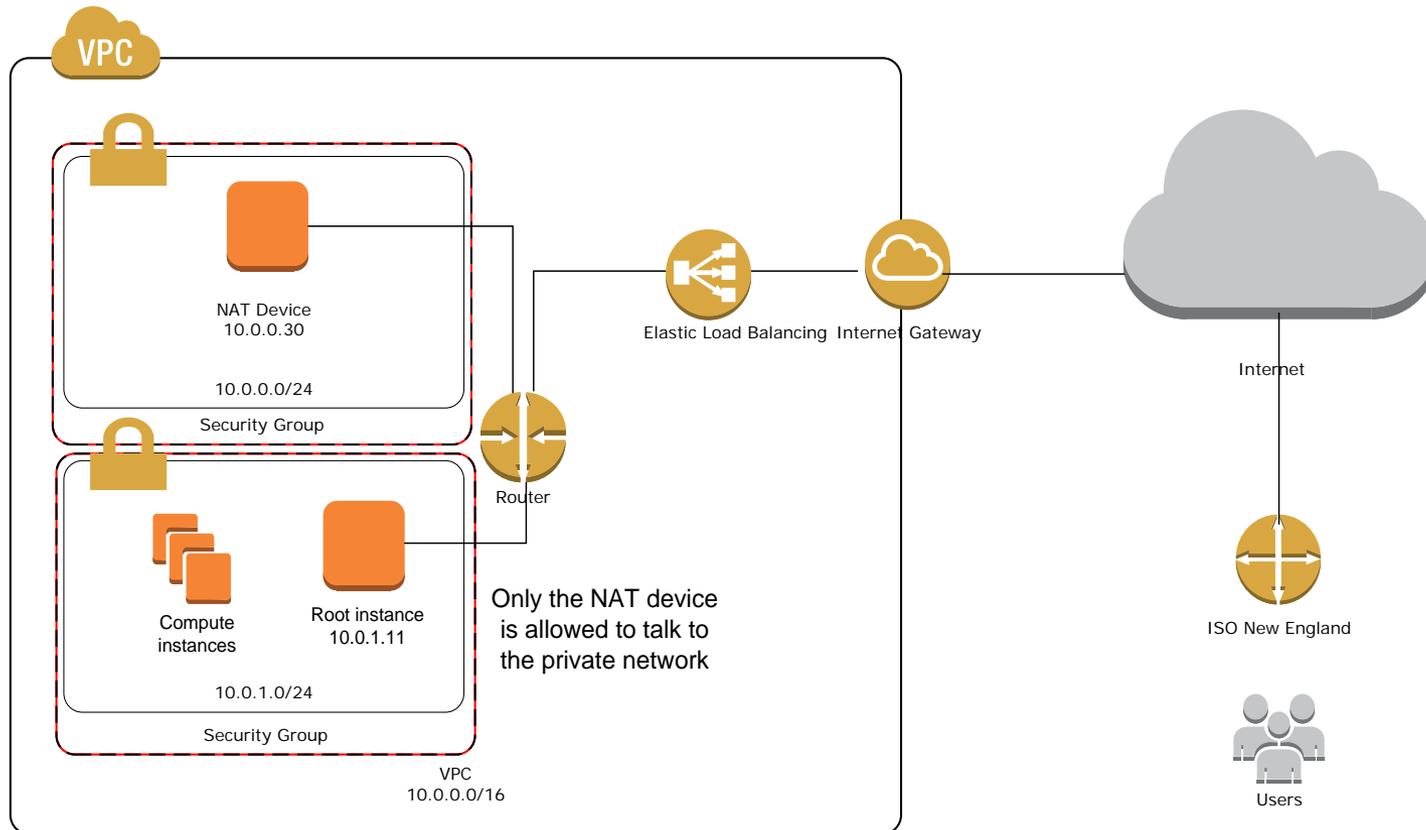


Deploy Power System Simulations in the Cloud

- Internal computing clusters are insufficient to meet our engineers' computational needs
- Use cloud as the HPC platform for large scale power system simulations
 - Amazon Web Services
 - CloudFuzion
- Power system software:
 - TARA
 - GE MARS
 - PSS/E
 - TSAT



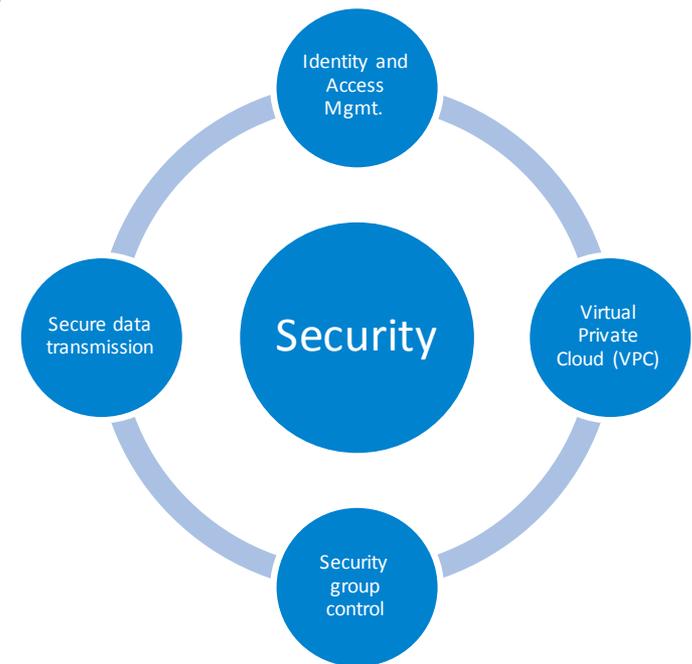
Deploy Power System Simulations in the Cloud - Architecture



Deploy Power System Simulations in the Cloud

– Security

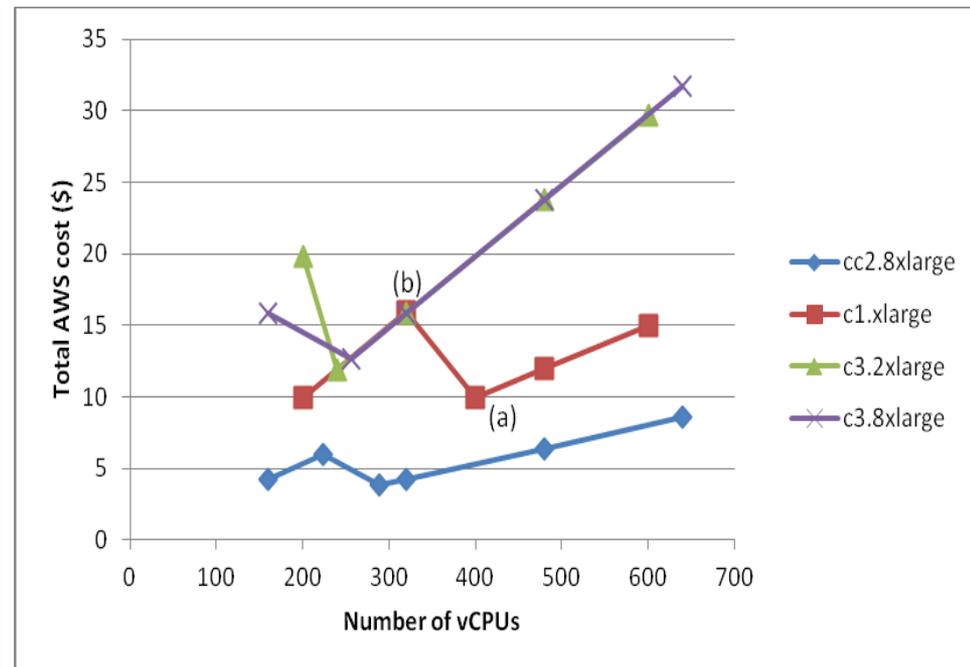
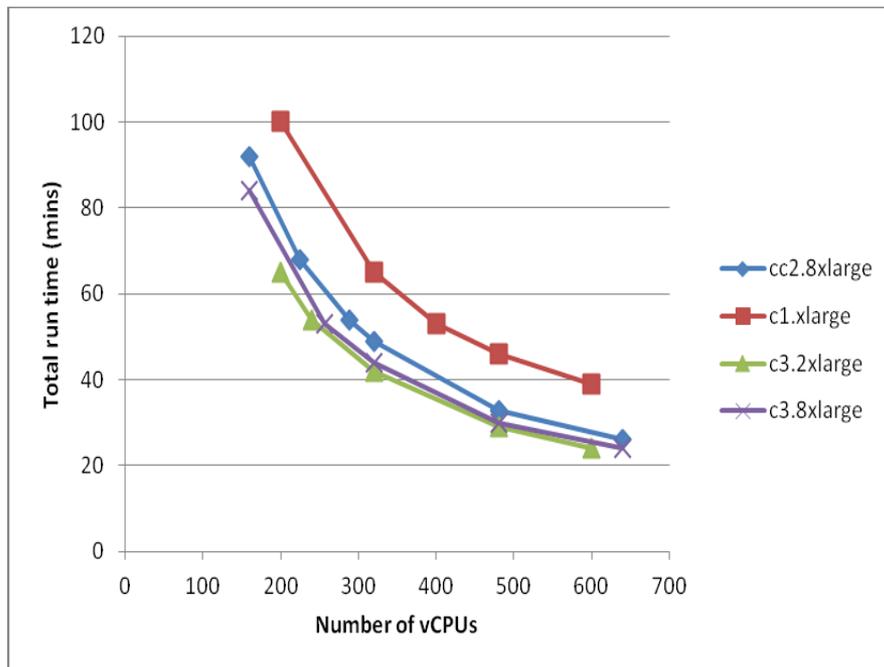
- Identity and Access Management (IAM)
 - Users' credentials, permissions, etc.
- Virtual Private Cloud (VPC)
 - A logically isolated section of AWS under users' complete control
- Security Group Control
 - Virtual firewall
 - Specify allowable inbound and outbound traffics (protocol, source, port, etc.)
- Secure data in transit and at rest
 - SSL certificates are created for data encryption using HTTPS protocol
 - EBS volume encryption for data at rest



Deploy Power System Simulations in the Cloud

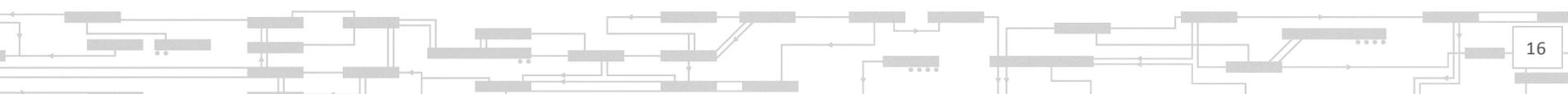
– Case Study

- 7,090 TARA N-1-1 simulations in Greater Boston Reliability Study
- 470 hours on engineer's desktop and 8 hours in internal clusters
- Nine CC2.8xlarge instances (32 cores/instance @ 2.60 GHz, 60.5 GB memory)
- Completed in less than one hour and AWS cost is about \$5.00



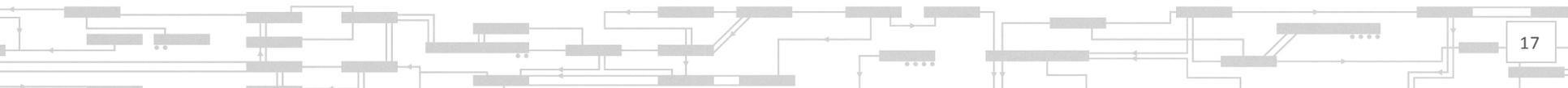
Deploy Power System Simulations in the Cloud

Run ID	Name	Status	User	Account	Submitted	Completed	Uptime	Total Time	Waiting	Done	Failed	Rescheduled	Length	Done	Length	Nodes
0000000299	cloud_Master_N_1_1_A34a	failed	anonymous	None	Fri Nov 4 17:06:24 2016	Fri Nov 4 17:14:11 2016	00:07:47	00:00:00	1824	0	0	0	0.000	0	0.000	0
0000000298	cloud_Master_N_1_1_A34a	done	anonymous	None	Fri Nov 4 16:02:44 2016	Fri Nov 4 17:33:21 2016	01:30:37	8d,10:05:20	0	1824	0	121	00:06:38	0	0.000	29
0000000296	cloud_Master_N_1_1_A34a	done	anonymous	None	Fri Nov 4 15:33:28 2016	Fri Nov 4 15:37:03 2016	00:03:35	01:37:27	0	48	0	0	00:02:01	0	0.000	10
0000000294	cloud_Master_N_1_1_A24a	done	anonymous	None	Fri Nov 4 13:53:35 2016	Fri Nov 4 15:15:43 2016	01:22:08	8d,05:17:51	0	1824	0	480	00:06:29	0	0.000	25
0000000293	cloud_Master_N_1_1_A24a	done	anonymous	None	Fri Nov 4 13:29:45 2016	Fri Nov 4 13:36:51 2016	00:07:06	02:59:48	0	48	0	0	00:03:44	0	0.000	1
0000000289	cloud_Master_N_1_1_A14a	done	anonymous	None	Fri Nov 4 12:32:11 2016	Fri Nov 4 13:10:54 2016	00:38:43	10d,07:46:19	0	1872	0	0	00:07:56	0	0.000	15
0000000285	cloud_Master_N_1_1_A14a	done	anonymous	None	Fri Nov 4 10:52:23 2016	Fri Nov 4 10:59:27 2016	00:07:04	02:57:56	0	48	0	0	00:03:42	0	0.000	1
0000000284	cloud_Master_N_1_1_A34b	done	anonymous	None	Thu Nov 3 18:11:58 2016	Thu Nov 3 19:04:17 2016	00:52:19	9d,21:18:30	0	1824	0	0	00:07:48	0	0.000	10
0000000282	cloud_Master	done	anonymous	None	Thu Nov 3 18:03:29 2016	Thu Nov 3 18:05:28 2016	00:01:59	01:13:48	0	48	0	0	00:01:32	0	0.000	10
0000000279	cloud_Master_N_1_1_A24b	done	anonymous	None	Thu Nov 3 16:56:37 2016	Thu Nov 3 17:49:09 2016	00:52:32	9d,20:18:34	0	1824	0	0	00:07:46	0	0.000	10
0000000276	cloud_Master_N_1_1_A24b	done	anonymous	None	Thu Nov 3 14:49:08 2016	Thu Nov 3 14:51:04 2016	00:01:56	01:12:21	0	48	0	0	00:01:30	0	0.000	9
0000000275	cloud_Master_N_1_1_A14b_nr	done	anonymous	None	Thu Nov 3 13:06:56 2016	Thu Nov 3 13:54:19 2016	00:47:23	9d,02:50:28	0	1824	0	0	00:07:11	0	0.000	15
0000000274	test_nr	done	anonymous	None	Thu Nov 3 12:26:27 2016	Thu Nov 3 12:31:22 2016	00:04:55	00:04:42	0	1	0	0	00:04:42	0	0.000	2
0000000272	cloud_Master_N_1_1_A14b	done	anonymous	None	Thu Nov 3 12:18:42 2016	Thu Nov 3 13:01:50 2016	00:43:08	9d,01:04:50	0	1824	0	0	00:07:08	0	0.000	15
0000000269	cloud_Master_N_1_1_A14b	done	anonymous	None	Thu Nov 3 11:14:00 2016	Thu Nov 3 12:04:59 2016	00:50:59	9d,13:53:13	0	1824	0	32	00:07:33	0	0.000	16
0000000268	cloud_Master_N_1_1_A14b	done	anonymous	None	Thu Nov 3 11:04:44 2016	Thu Nov 3 11:06:40 2016	00:01:56	01:13:26	0	48	0	0	00:01:31	0	0.000	10
0000000265	cloud_MasterA13	done	anonymous	None	Wed Nov 2 18:43:57 2016	Wed Nov 2 19:45:50 2016	01:01:53	8d,22:22:39	0	1824	0	0	00:07:03	0	0.000	15
0000000263	cloud_MasterA13	done	anonymous	None	Wed Nov 2 16:47:05 2016	Wed Nov 2 17:45:39 2016	00:58:34	8d,02:47:45	0	1824	0	0	00:06:24	0	0.000	14
0000000259	cloud_Master	done	anonymous	None	Wed Nov 2 15:10:56 2016	Wed Nov 2 16:26:36 2016	01:15:40	7d,04:02:38	0	1824	0	0	00:05:39	0	0.000	14



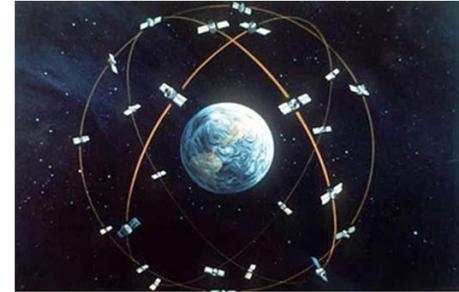
Outline

- Overview of ISO New England
- Cloud computing and new opportunities
- Application 1:
 - High performance computing needs in power system modeling and simulations
 - Deploy power system analysis software in the cloud
- **Application 2:**
 - Synchrophasor technology, wide area monitoring and situational awareness
 - Cloud-hosted wide area monitoring
- Conclusions



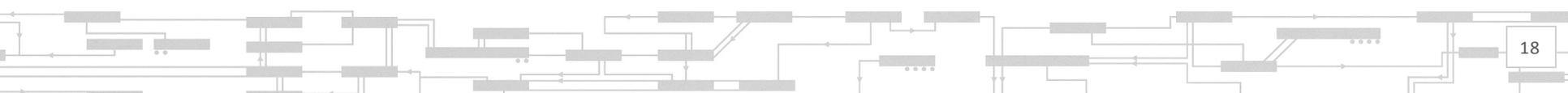
Synchrophasor Technology

- Synchrophasor:
 - Phasor (magnitude and angle)
 - Precise GPS time stamp
 - High sampling rates
 - 30 to 120 samples per second

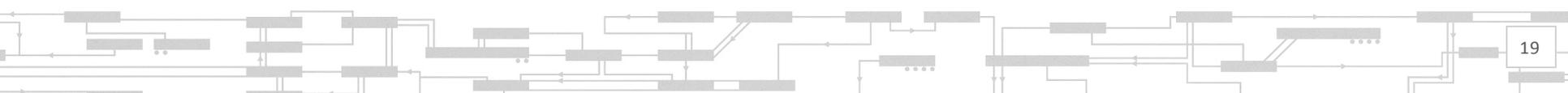
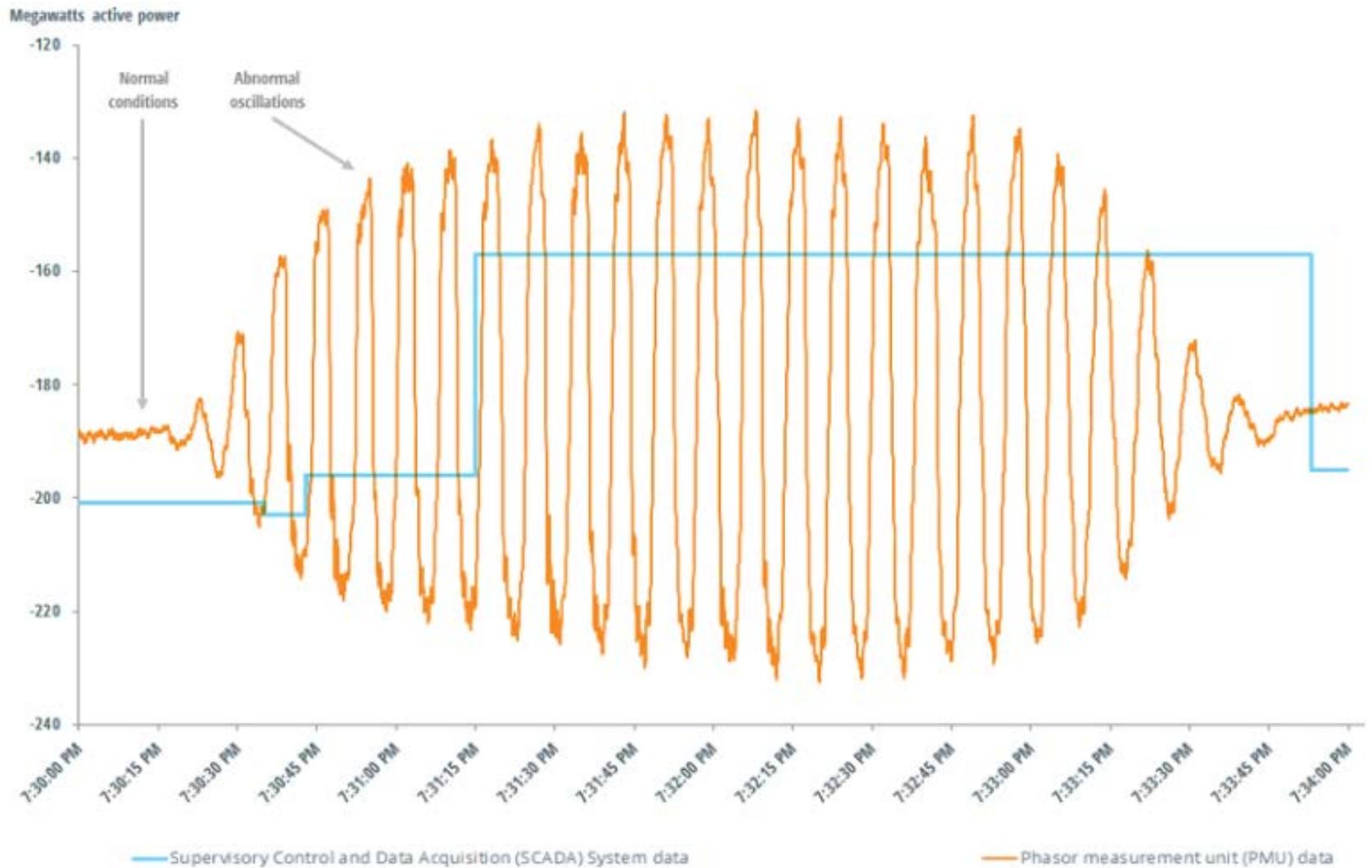


Synchrophasor = Phasor + GPS + high sampling rate

- PMU - Phasor Measurement Unit
 - Synchrophasor is created in the substation by PMU



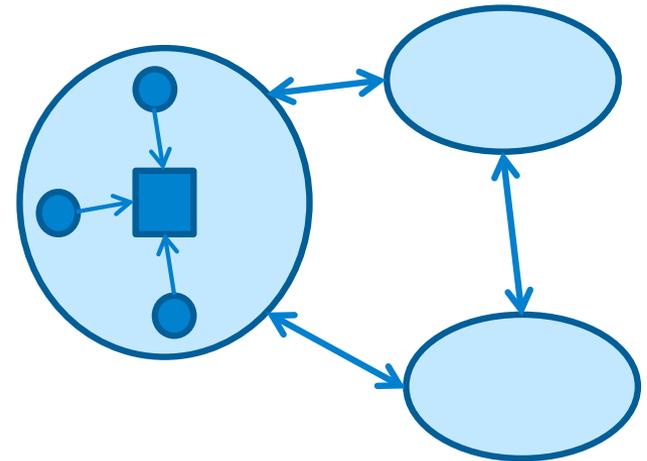
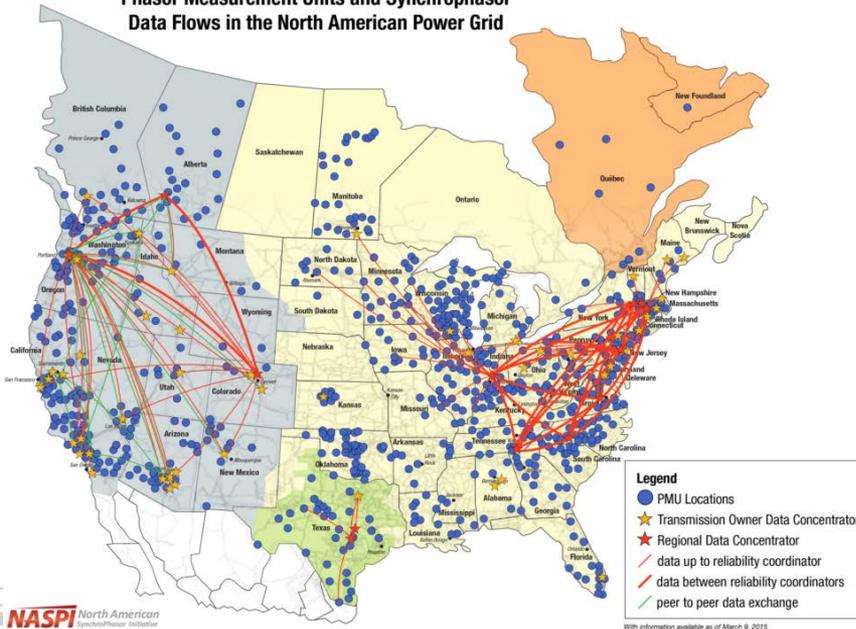
Example of Traditional SCADA Data vs New PMU Data in Power Grid Condition Monitoring



Wide-Area Monitoring System (WAMS)

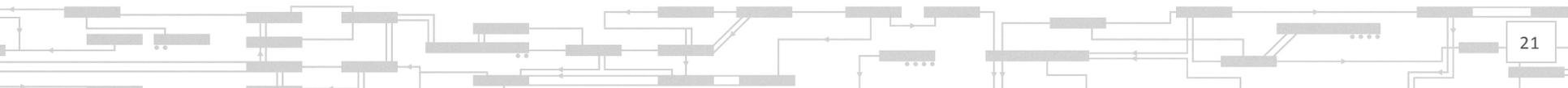
- Monitoring wide-area power system conditions in real time is key to operational situational awareness
 - Large scale PMU deployment in Eastern Interconnection due to SGIG
 - Information beyond the operational region is crucial
 - Current practice
 - ISOs collecting data from Transmission Owners
 - PMU data exchange among regions

Phasor Measurement Units and Synchrophasor Data Flows in the North American Power Grid



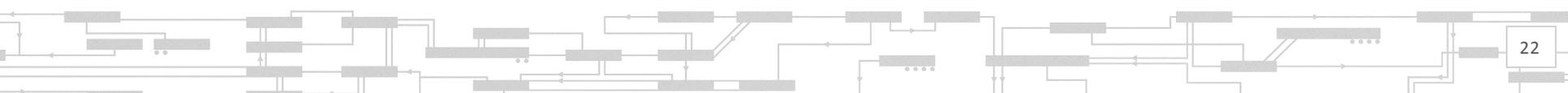
Challenges of Current PMU Data Exchange Scheme

- Raw PMU data exchange only
 - Large volumes of data
 - Bandwidth: cost, performance
 - High maintenance
 - Each entity has to model and maintain its own and other region's PMU data
 - There is no central PMU Registry
 - No data quality information or outage status
 - Lacks coordination
 - Each entity processes and analyzes data separately
 - Operators in different entities see different results and displays
 - Interpretation discrepancy
- Point-to-point data exchange structure
 - Multiple bilateral data streams: network cost, maintenance
- Latency
 - Bottom-up tree structure
 - Chained PDC network which accumulates time delays

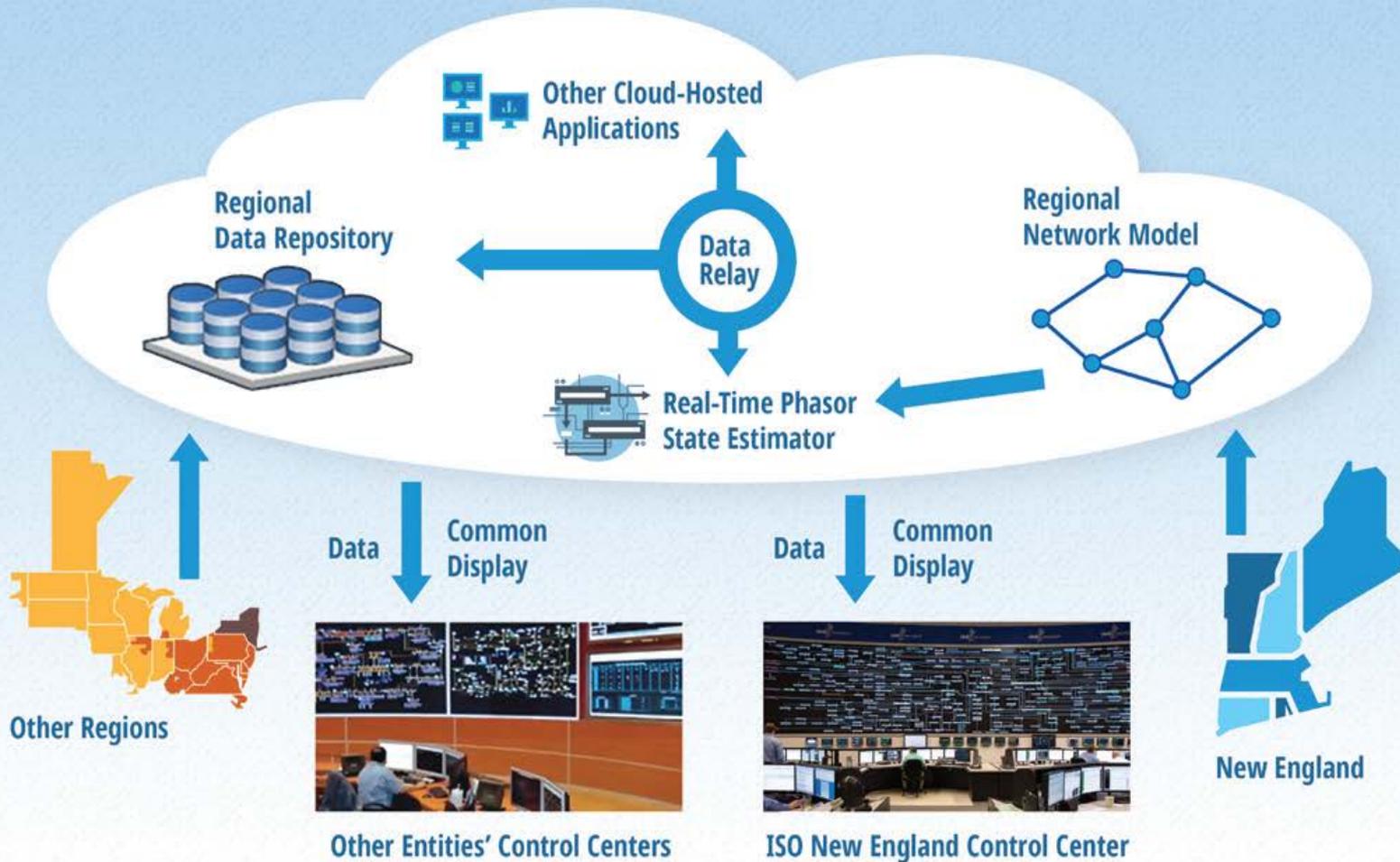


Proof-of-Concept Cloud Hosted WAMS

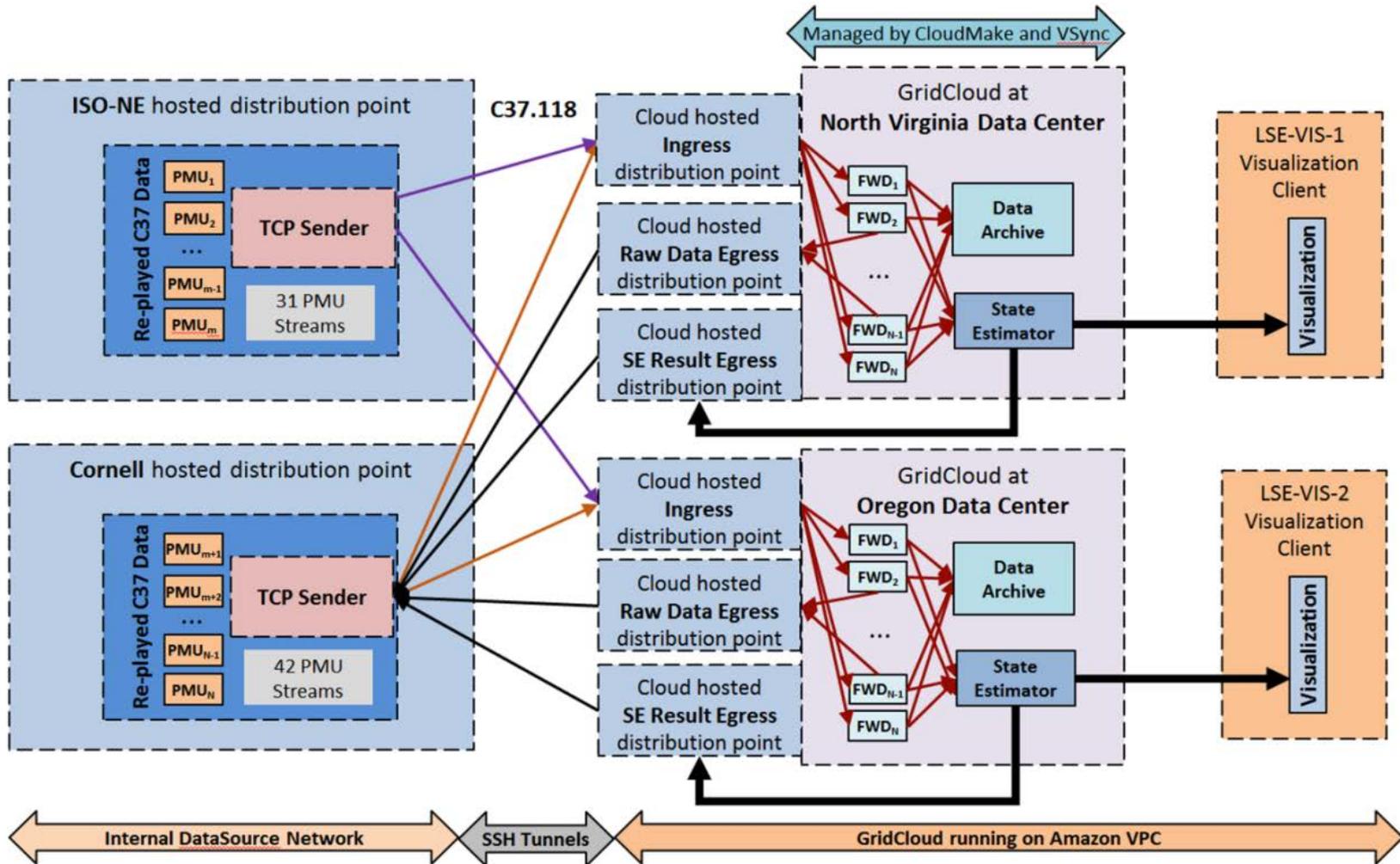
- Objective: demonstrate a cloud-hosted distributed platform for real-time PMU data collection, storage, processing and dissemination to achieve wide-area monitoring
 - Security
 - Network latency
 - Fault tolerance
 - Data consistency
 - Cost
- Project collaborations among
 - ISO New England Inc.
 - Cornell University
 - Washington State University



Overview of the Concept of Cloud Hosted WAMS



Cloud Hosted WAMS Deployment



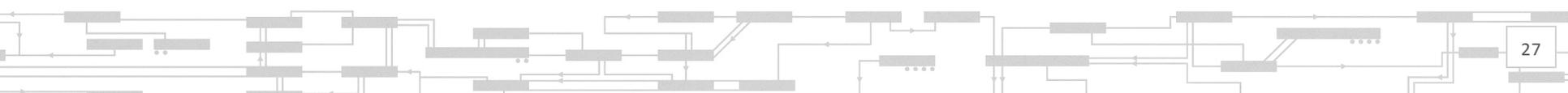
Key Findings

- The latency due to encryption of data in transit and at rest (cloud archive) was satisfactory
 - Around 15ms between EC classic and VPC
 - SSH tunnels added less than 2ms
 - AES 256 encryption has no impact on performance (noise level)
- The average round-trip time from the ISO-NE in Massachusetts to the Phasor State Estimator in the cloud and back to Cornell was 350 milliseconds via the Virginia data center and 425 milliseconds via the Oregon data center
- Data consistency (PMU raw data and state estimator results) was confirmed between the two data centers
- Each data center had 13 cloud instances, with a total average cost of \$2.47 per hour per data center
- Full back-up redundancy was restored within 5 minutes after data center shutdowns.

Conclusions

- The rapid proliferation of new technologies is transforming how electricity is produced, delivered, and consumed.
- While offering many benefits, these changes are also increasing the complexity of power systems and requiring innovative approaches to keeping the lights on.
- Cloud Computing has offered many new opportunities that the power industry could take advantage of.
- Strong business cases are key to the decisions.
- Security concerns shall not discourage adopting cloud computing; it is necessary to understand responsibilities and adapt security practices to this new environment.

Questions





NERC Emerging Technology Roundtable Cloud Offerings Architecture

Stevan D. Vidich, Principal Program Manager
Microsoft Corporation

NIST SP 800-145 definition of cloud computing

Service Models

Infrastructure as a Service (IaaS)

Platform as a Service (IaaS)

Software as a Service (IaaS)

Deployment Models

Private cloud

Community cloud

Public cloud

Hybrid cloud

Hyper-scale cloud

200+ cloud services,
100+ datacenters,
\$15B+ infrastructure investment

1+ billion customers,
20+ million businesses,
90+ countries worldwide

500+ million
users in Azure
Active Directory
Microsoft Azure

3.5 million
active users

Microsoft Dynamics CRM Online

50+ billion
minutes of connections
handled each month

skype

7+ billion
worldwide queries
each month³

bing

1.2+ billion
worldwide users

Office 365

48+ million
members in 57 countries

XBOX

450+ million
unique users each month

msn



Security & Management

- Security Center
- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Store/Marketplace
- VM Image Gallery & VM Depot

Platform Services

Media & CDN

- Media Services
- Media Analytics
- Content Delivery Network

Integration

- API Management
- BizTalk Services
- Logic Apps
- Service Bus

Compute Services

- Container Service
- VM Scale Sets
- Batch
- RemoteApp
- Dev/Test Lab

Application Platform

- Web Apps
- Mobile Apps
- API Apps
- Cloud Services
- Service Fabric
- Notification Hubs
- Functions

Developer Services

- Visual Studio
- Mobile Engagement
- VS Team Services
- Xamarin
- Application Insights
- HockeyApp

Data

- SQL Database
- SQL Data Warehouse
- DocumentDB
- SQL Server Stretch Database
- Redis Cache
- Storage Tables
- Azure Search

Intelligence

- Cognitive Services
- Bot Framework
- Cortana

Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Catalog
- Data Lake Analytics Service
- Data Lake Store
- IoT Hub
- Event Hubs
- Data Factory
- Power BI Embedded

Hybrid Cloud

- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Log Analytics
- Import/Export
- Azure Site Recovery
- StorSimple

Infrastructure Services

Compute

- Virtual Machines
- Containers

Storage

- Blob
- Queues
- Files
- Disks

Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

Datacenter Infrastructure



patterns & practices

proven practices for predictable results

This poster depicts common problems in designing cloud applications and patterns that offer solutions. The information applies to Microsoft Azure as well as other cloud platforms. The icons at the top of each item represent the problem areas that the pattern relates to. Patterns that include code samples are indicated by this icon: </>

Visit <http://aka.ms/Cloud-Design-PatternsSample> to download.

Problem areas in the cloud

Availability

Availability defines the proportion of time that the system is functional and working. It will be affected by system errors, infrastructure problems, malicious attacks, and system load. It is usually measured as a percentage of uptime. Cloud applications typically provide users with a service level agreement (SLA) which means that applications must be designed and implemented in a way that maximizes availability.

<http://aka.ms/Availability-Patterns>

Data Management

Data management is the key element of cloud applications, and influences most of the quality attributes. Data is typically hosted in different locations and across multiple servers for reasons such as performance, scalability or availability, and this can present a range of challenges. For example, data consistency must be maintained, and data will typically need to be synchronized across different locations.

<http://aka.ms/DataManagement-Patterns>

Design and Implementation

Good design encompasses factors such as consistency and coherence in component design and deployment, maintainability to simplify administration and development, and flexibility to allow components and subsystems to be used in other applications and in other scenarios. Decisions made during the design and implementation phase have a huge impact on the quality and the total cost of ownership of cloud hosted applications and services.

<http://aka.ms/Design-and-Implementation-Patterns>

Messaging

The distributed nature of cloud applications requires a messaging infrastructure that connects the components and services, ideally in a loosely coupled manner in order to maximize scalability. Asynchronous messaging is widely used and provides many benefits, but also brings challenges such as the ordering of messages, poison message management, identity, potency, and more.

<http://aka.ms/Messaging-Patterns>

Management and Monitoring

Cloud applications run in a remote datacenter where you do not have full control of the infrastructure or, in some cases, the operating system. This can make management and monitoring more difficult than an on-premises deployment. Applications must expose runtime information that administrators and operators can use to manage and monitor the system, as well as supporting changing business requirements without requiring the application to be stopped or redeployed.

<http://aka.ms/Management-and-Monitoring-Patterns>

Performance and Scalability

Performance is an indication of the responsiveness of a system, while scalability is the ability to gracefully handle increases in load, perhaps through an increase in available resources. Cloud applications, especially in multi-tenant scenarios, typically encounter variable workloads and unpredictable activity peaks and should be able to scale out within limits to meet demand, and scale in when demand decreases. Scalability concerns not just compute instances, but other items such as data storage, messaging infrastructure, and more.

<http://aka.ms/Performance-and-Scalability-Patterns>

Resiliency

Resiliency is the ability of a system to gracefully handle and recover from failures. The nature of cloud hosting, where applications are often multi-tenant, use shared platform services, compete for resources and bandwidth, communicate over the Internet, and run on commodity hardware means there is an increased likelihood that both transient and more permanent faults will arise. Detecting failures, and recovering quickly and efficiently, is necessary to maintain resiliency.

<http://aka.ms/Resiliency-Patterns>

Security

Security is the capability of a system to prevent malicious or accidental actions outside of the designed usage, and to prevent disclosure or loss of information. Cloud applications are exposed on the Internet outside trusted on-premises boundaries, are often open to the public, and may serve untrusted users. Applications must be designed and deployed in a way that protects them from malicious attacks, restricts access to only approved users, and protects sensitive data.

<http://aka.ms/Security-Patterns>

Cache-aside

Load data on demand into a cache from a data store. This pattern can improve performance and also helps to maintain consistency between data held in the cache and the data in the underlying data store.



For more info, see <http://aka.ms/Cache-Aside-Pattern>

Event Sourcing

Use an append-only store to record actions taken on data, rather than the current state, and use the store to materialize the domain objects. In complex domains this can avoid synchronizing the data model and the business domain, improve performance, scalability, and responsiveness provide consistency, and provide audit history to enable compensating actions.



For more info, see <http://aka.ms/Event-Sourcing-Pattern>

Leader Election

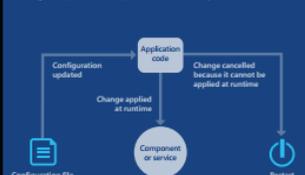
Coordinate the actions performed by a collection of collaborating task instances in a distributed system by electing one instance as the leader that assumes responsibility for managing the other instances. This pattern can help to ensure that task instances do not conflict with each other, cause contention for shared resources, or inadvertently interfere with the work that other task instances are performing.



For more info, see <http://aka.ms/Leader-Election-Pattern>

Runtime Reconfiguration

Design an application so that it can be reconfigured without requiring redeployment or restarting the application. This helps to maintain availability and minimize downtime.



For more info, see <http://aka.ms/Runtime-Reconfiguration-Pattern>

Circuit-aside

Handle faults that prevent a service or application from reaching a target service or application.



For more info, see <http://aka.ms/Circuit-Aside-Pattern>

Externalized Configuration

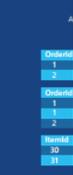
Move configuration data out of the application code and into a separate, externalized configuration store. This helps to maintain consistency between the application code and the configuration data.



For more info, see <http://aka.ms/Externalized-Configuration-Pattern>

Materialized View

Generate pre-populated data for a specific query to support a specific use case. This helps to improve performance and reduce the load on the underlying data store.



For more info, see <http://aka.ms/Materialized-View-Pattern>

Scheduler

Coordinate a set of tasks, attempt to start the work, and maintain resiliency to a data to transient exceptions.



For more info, see <http://aka.ms/Scheduler-Pattern>

Cloud Design Patterns

PRESCRIPTIVE ARCHITECTURE GUIDANCE FOR CLOUD APPLICATIONS

**Alex Homer
John Sharp
Larry Brader
Masashi Narumoto
Trent Wanson**

patterns & practices

Command and Query Responsibility Segregation (CQRS)

Segregate operations that read data from operations that update data by using separate interfaces. This pattern can maximize performance, scalability, and security support evolution of the system over time through higher flexibility, and prevent update commands from causing merge conflicts at the domain level.

Index Table

Create indexes over the fields in data stores that are frequently referenced by query criteria. This pattern can improve query performance by allowing applications to more quickly locate the data to retrieve from a data store.

Primary Key	Customer Data	Customer Data
CustomerID	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
1	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
2	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
3	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
4	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
5	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
6	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
7	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
8	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
9	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate
10	CustomerID, Name, Address, Birthdate	CustomerID, Name, Address, Birthdate

Retry

Enable an application to handle anticipated, temporary failures when it attempts to connect to a service or network resource by transparently retrying an operation that has previously failed in the expectation that the cause of the failure is transient. This pattern can improve the stability of the application.

Valet Key

Use a token or key that provides clients with restricted direct access to a specific resource or service in order to offload data transfer operations from the application code. This pattern is particularly useful in applications that use cloud-hosted storage systems or queues, and can maximize cost and maximize scalability and performance.

Cloud Design Patterns: Prescriptive Architecture Guidance for Cloud Applications

Azure IoT architecture



Event Hubs



Stream Analytics

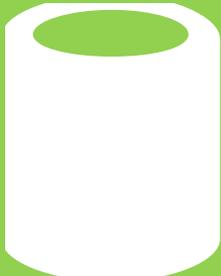
Microsoft Azure

Client or Device

Apps	IoT Devices + Sensors
IP-capable devices	Low-power devices

Azure Services

- Storage
- Relational DB
- NoSQL
- Hadoop
- Machine Learning



Power BI



The next generation solution for energy companies

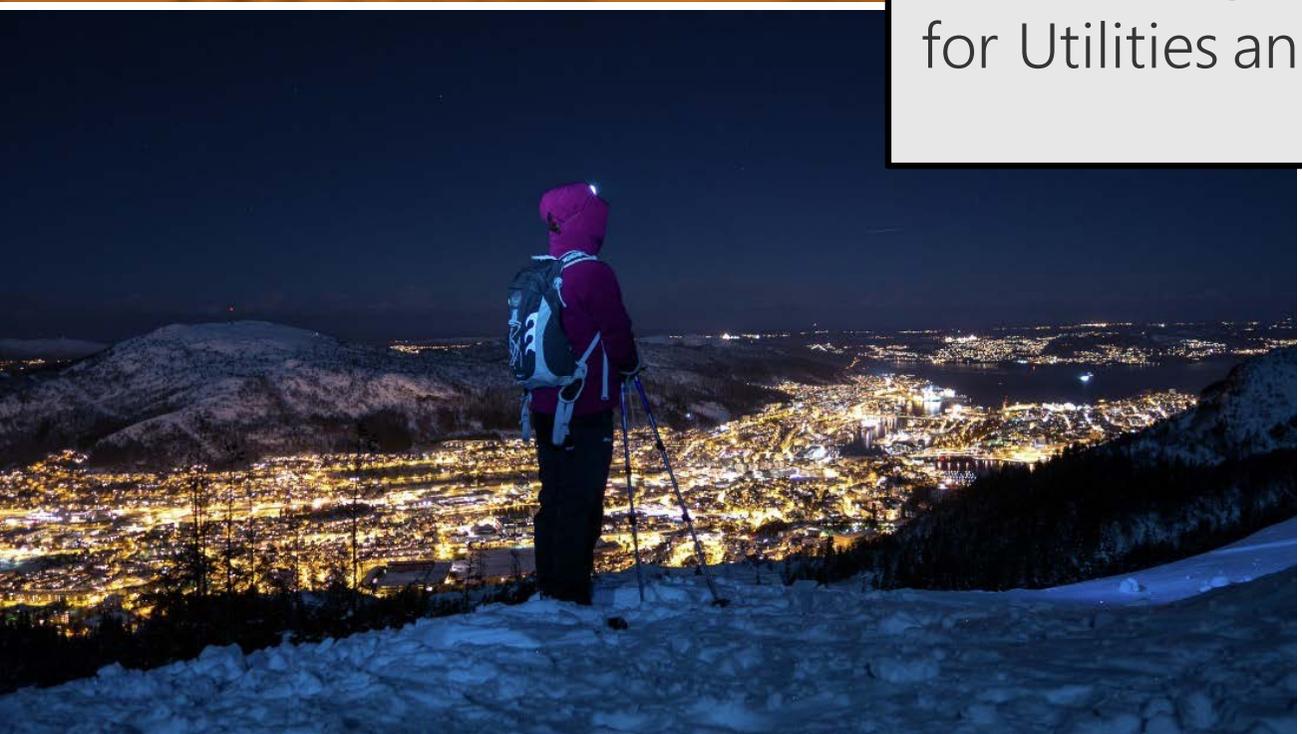
 Connected Grid

The icon consists of a white stylized tower or antenna symbol inside a blue square.

Is your company seeking to capitalize on smart metering system investments? Are you looking to create smart grids and more efficient network operations?



IoT and Big Data Analytics
for Utilities and Smart Cities

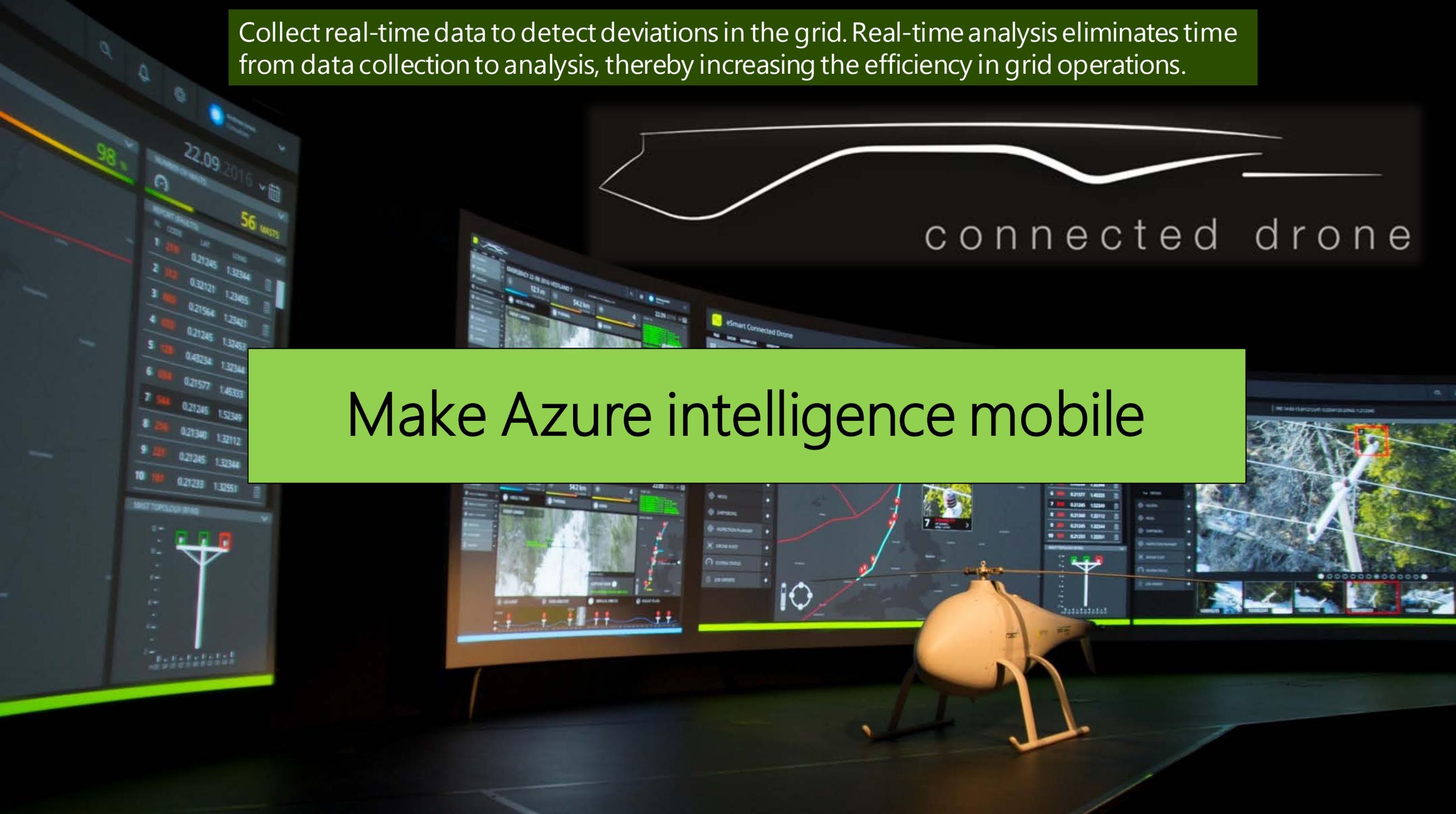


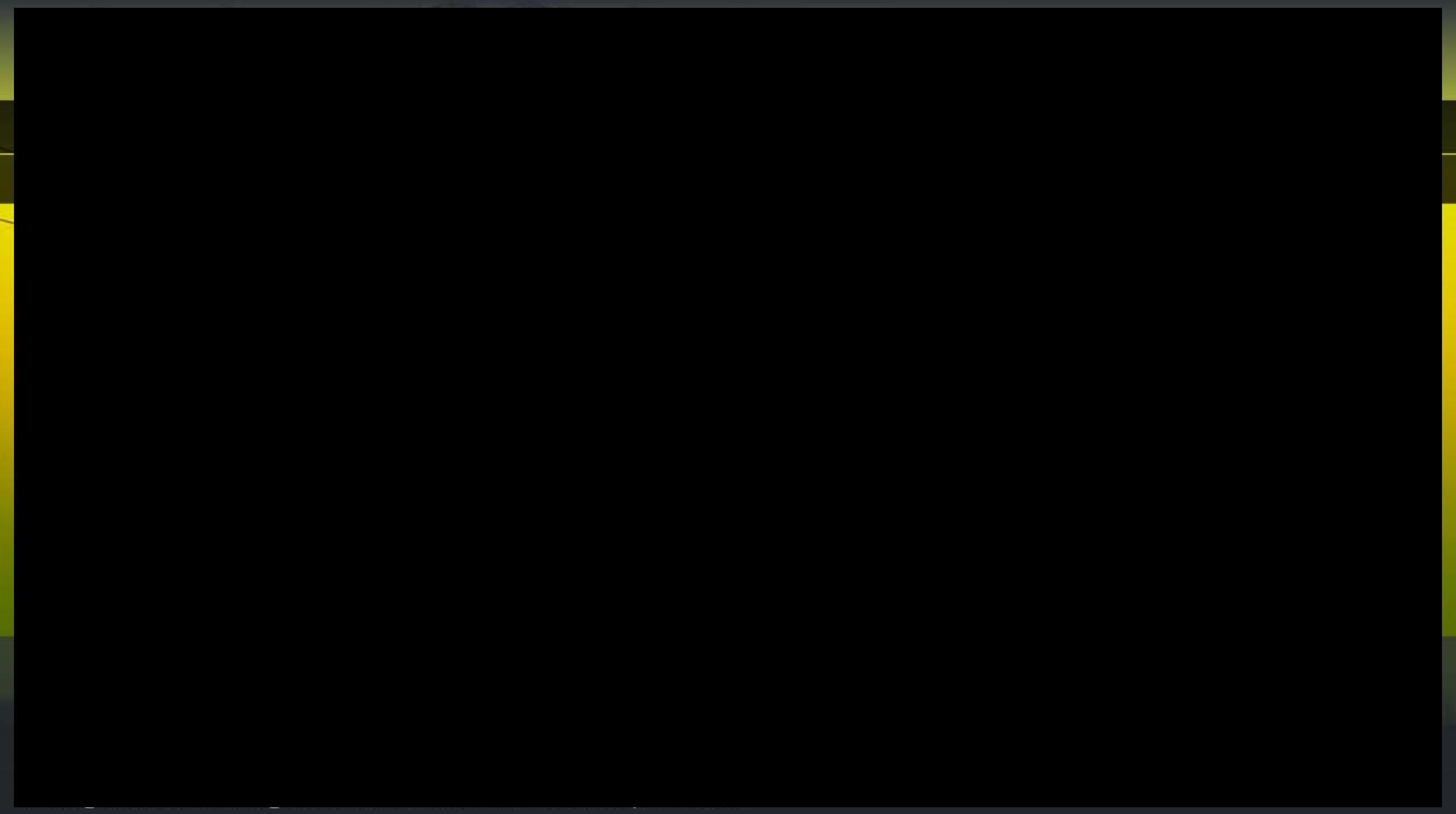
Collect real-time data to detect deviations in the grid. Real-time analysis eliminates time from data collection to analysis, thereby increasing the efficiency in grid operations.



connected drone

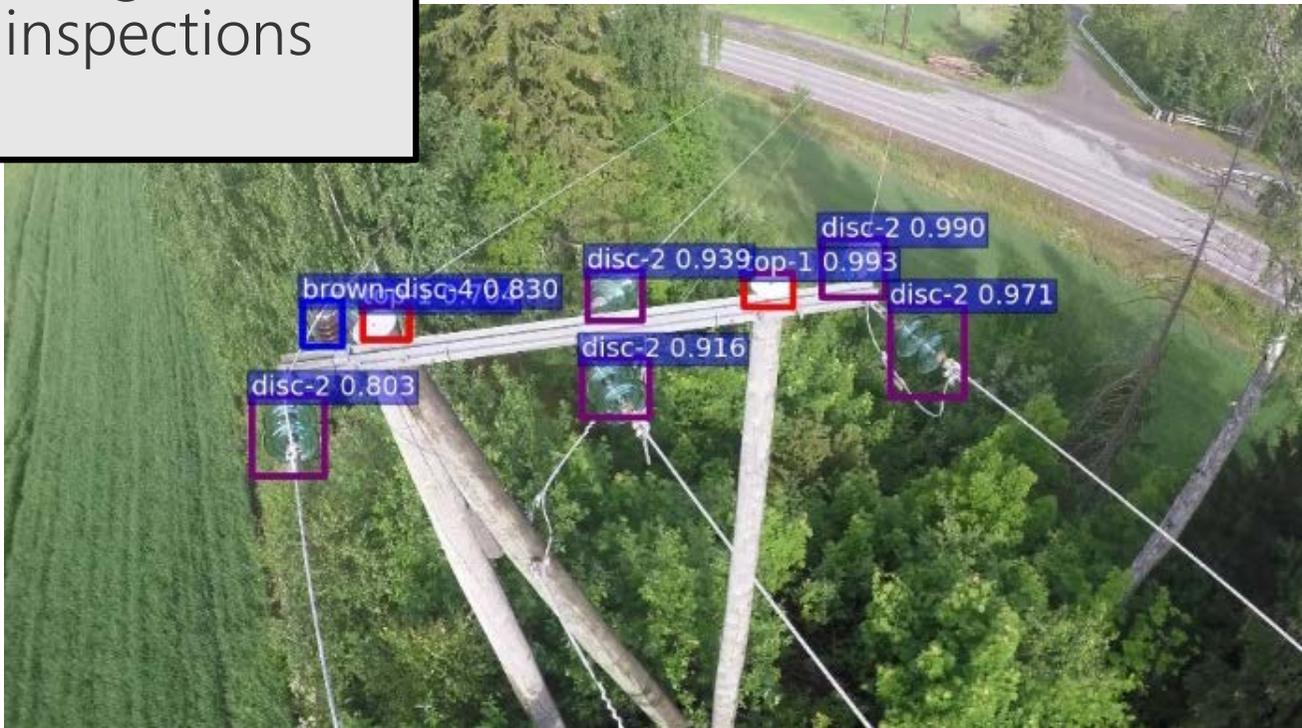
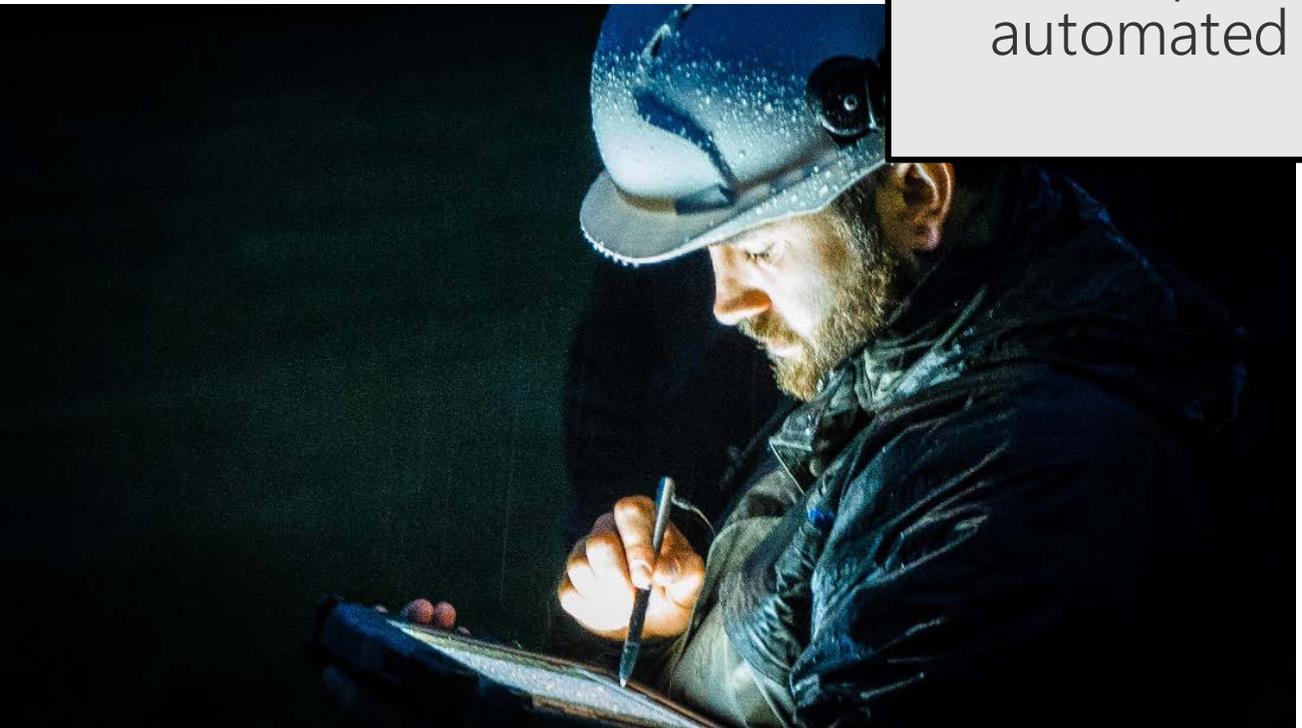
Make Azure intelligence mobile

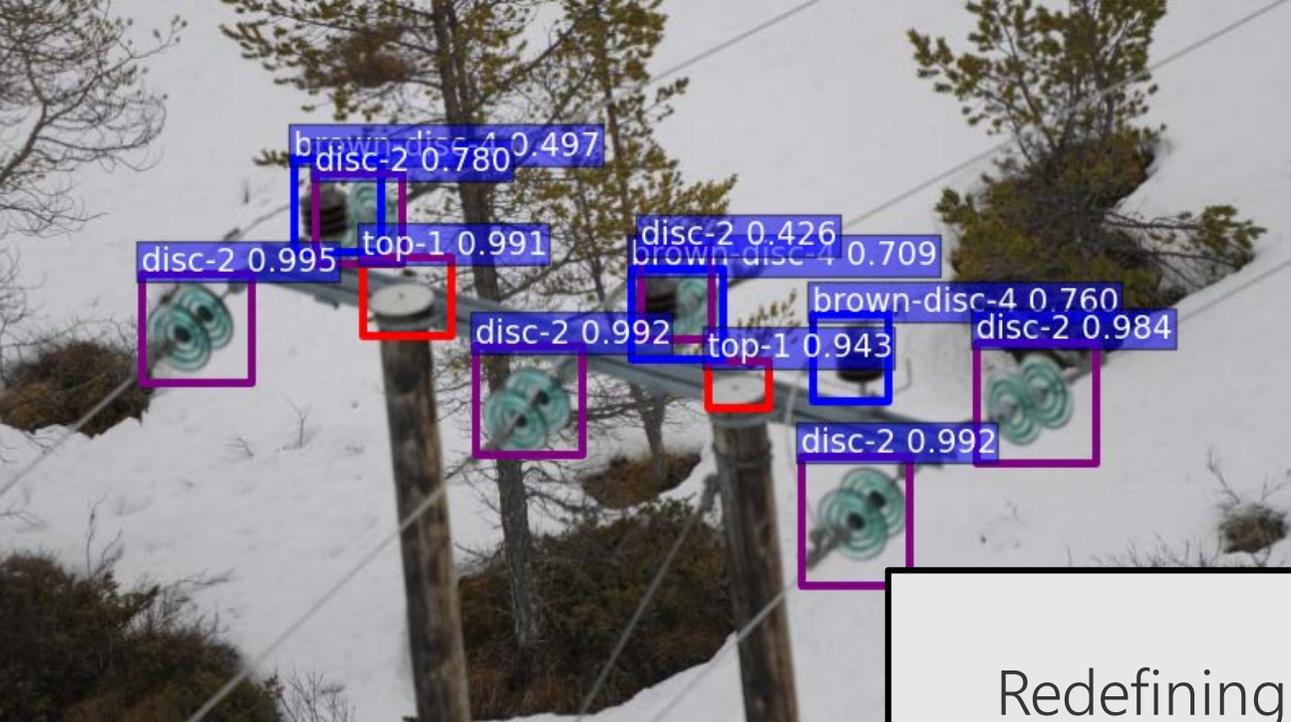




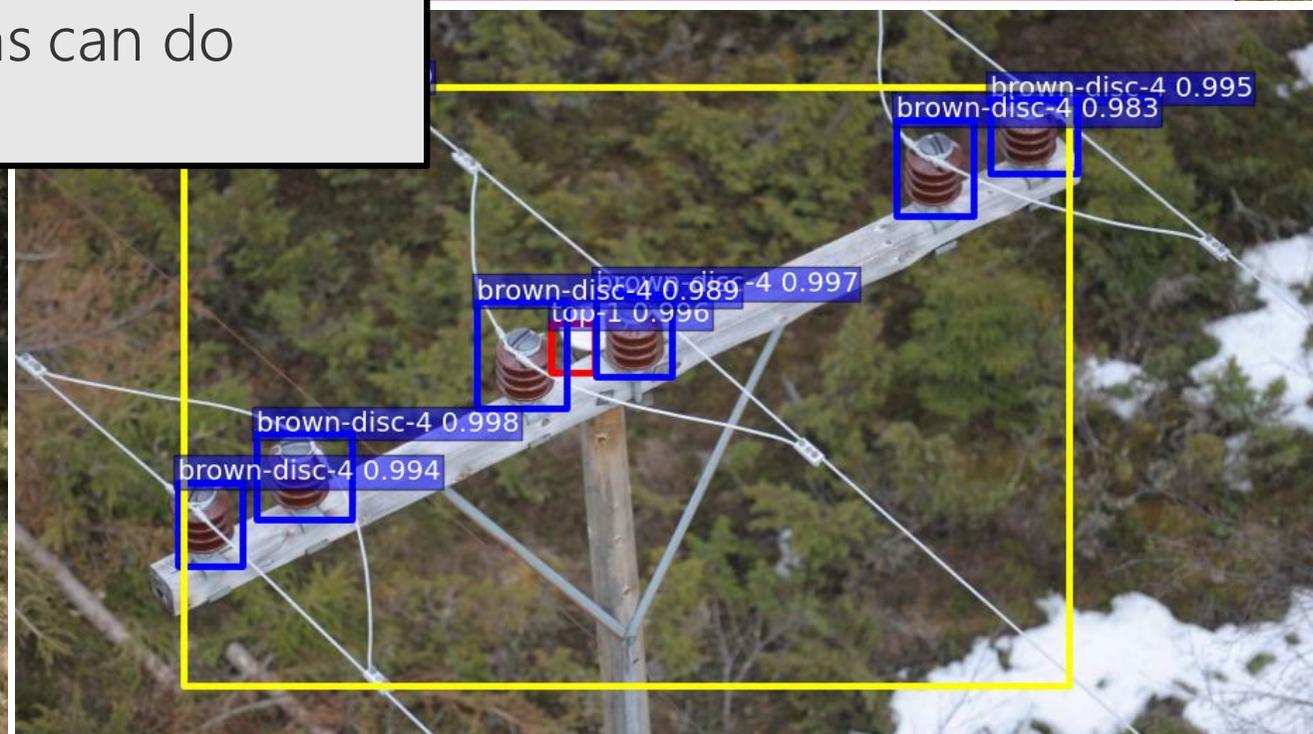
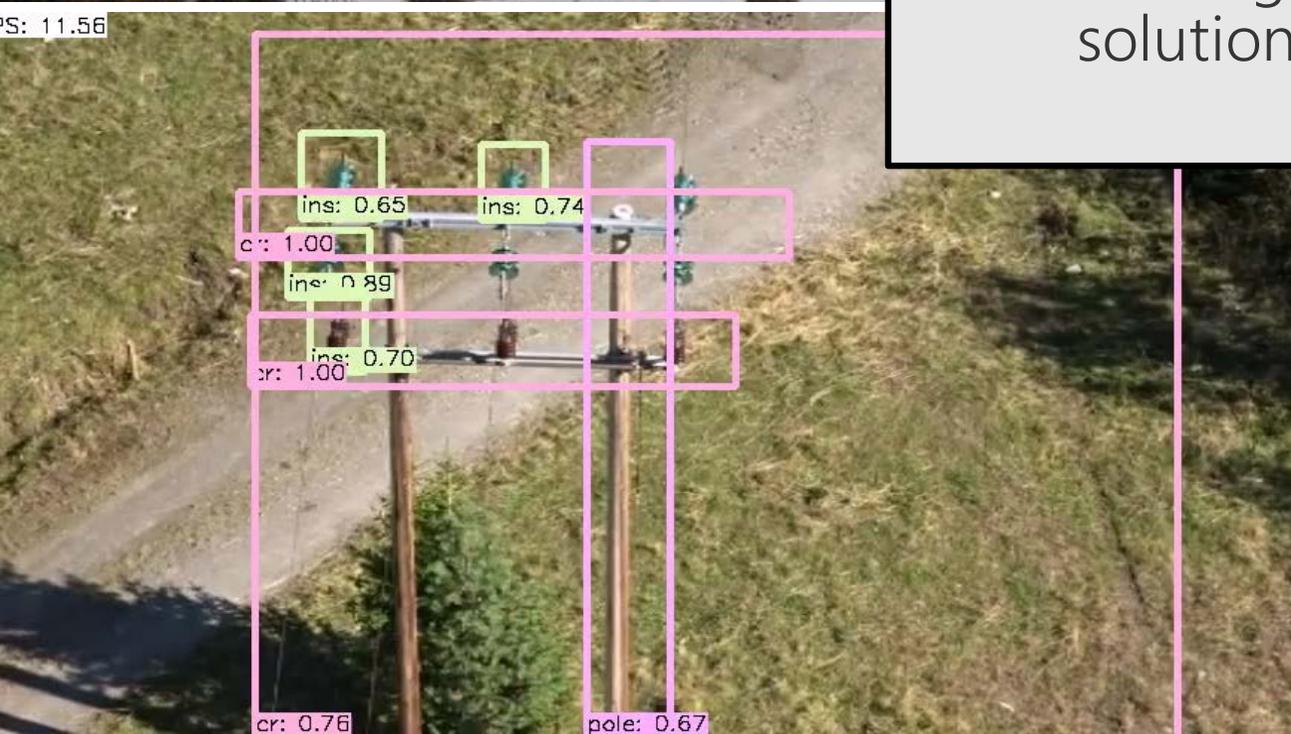


Deep learning for automated inspections

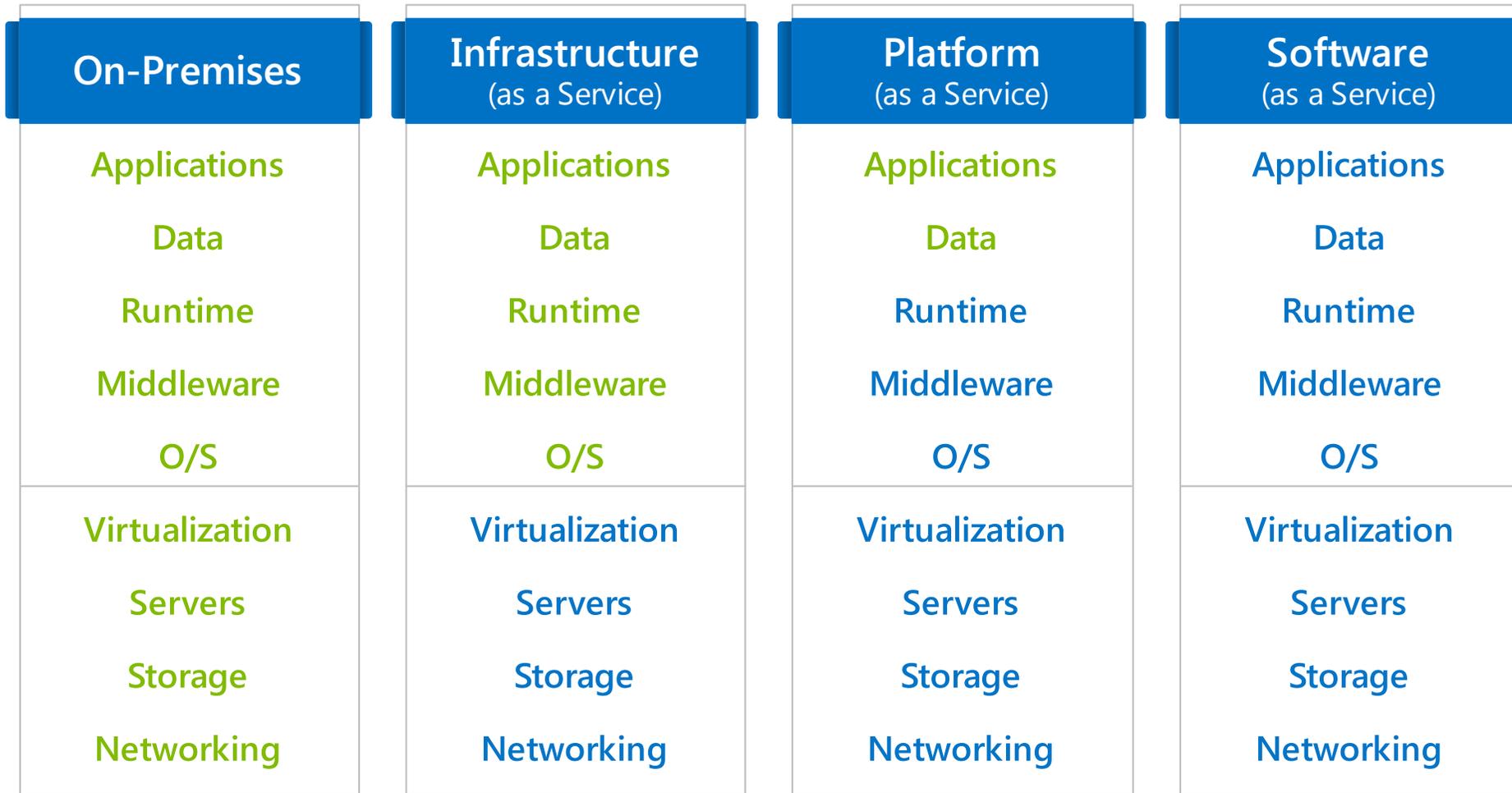




Redefining what cloud solutions can do



Cloud services – shared responsibility



← Microsoft Azure →

Office 365 →

Each customer environment is isolated on top of Azure's Infrastructure

Shared Physical Environment

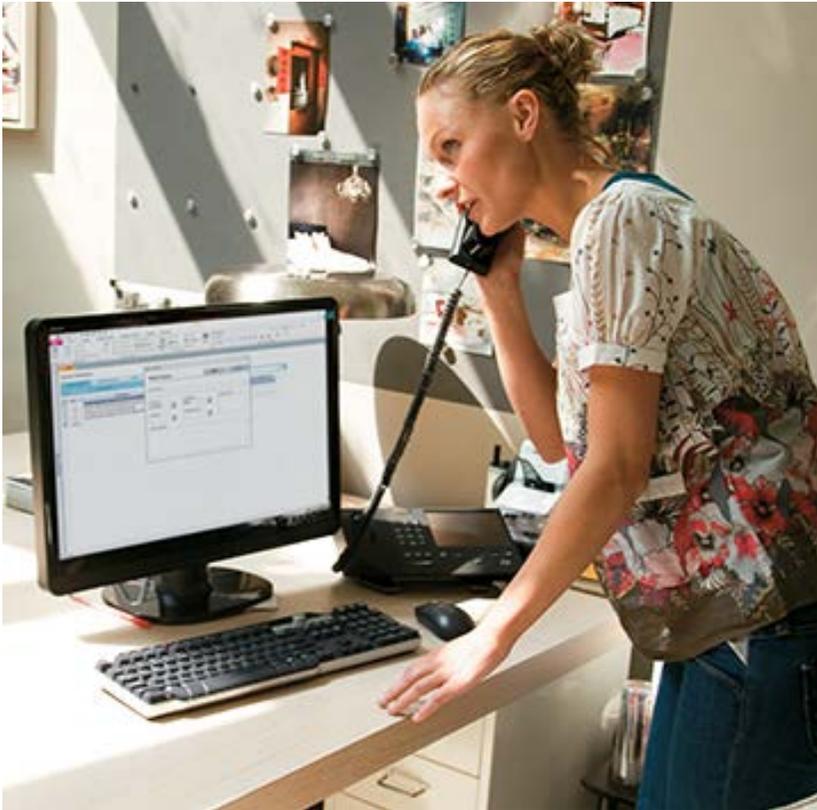
Managed by:

Customer

Vendor

Certification dependencies

Infrastructure protection



24 hour monitored physical security

System monitoring and logging

Patch management

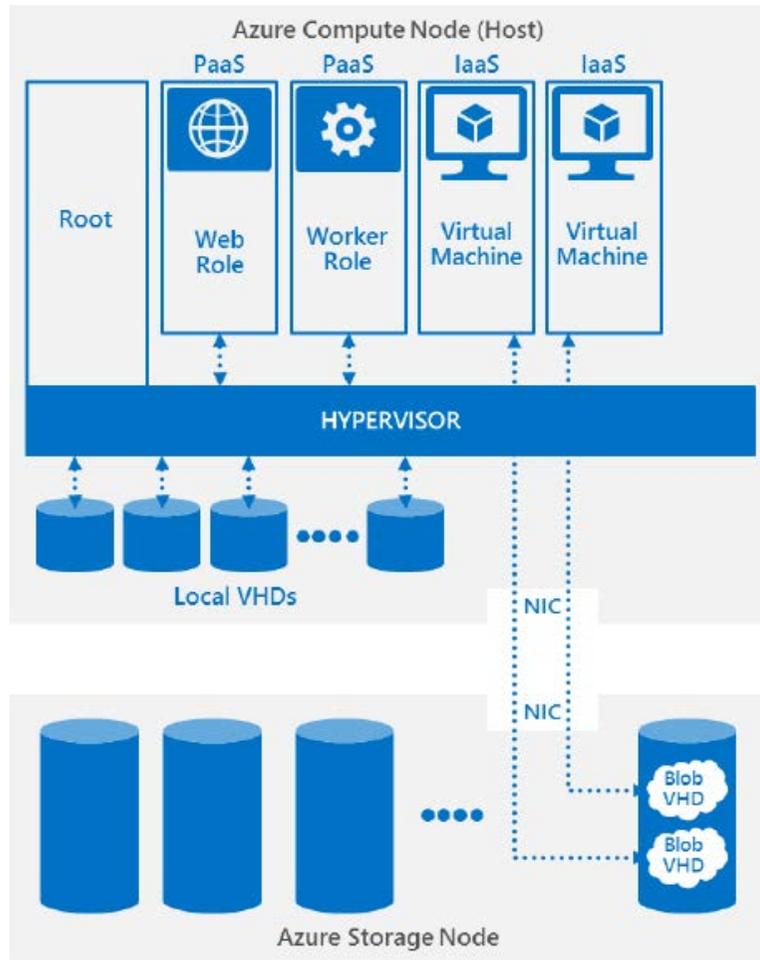
Anti-Virus/Anti-Malware protection

Intrusion detection/DDoS

Penetration testing, vulnerability scanning

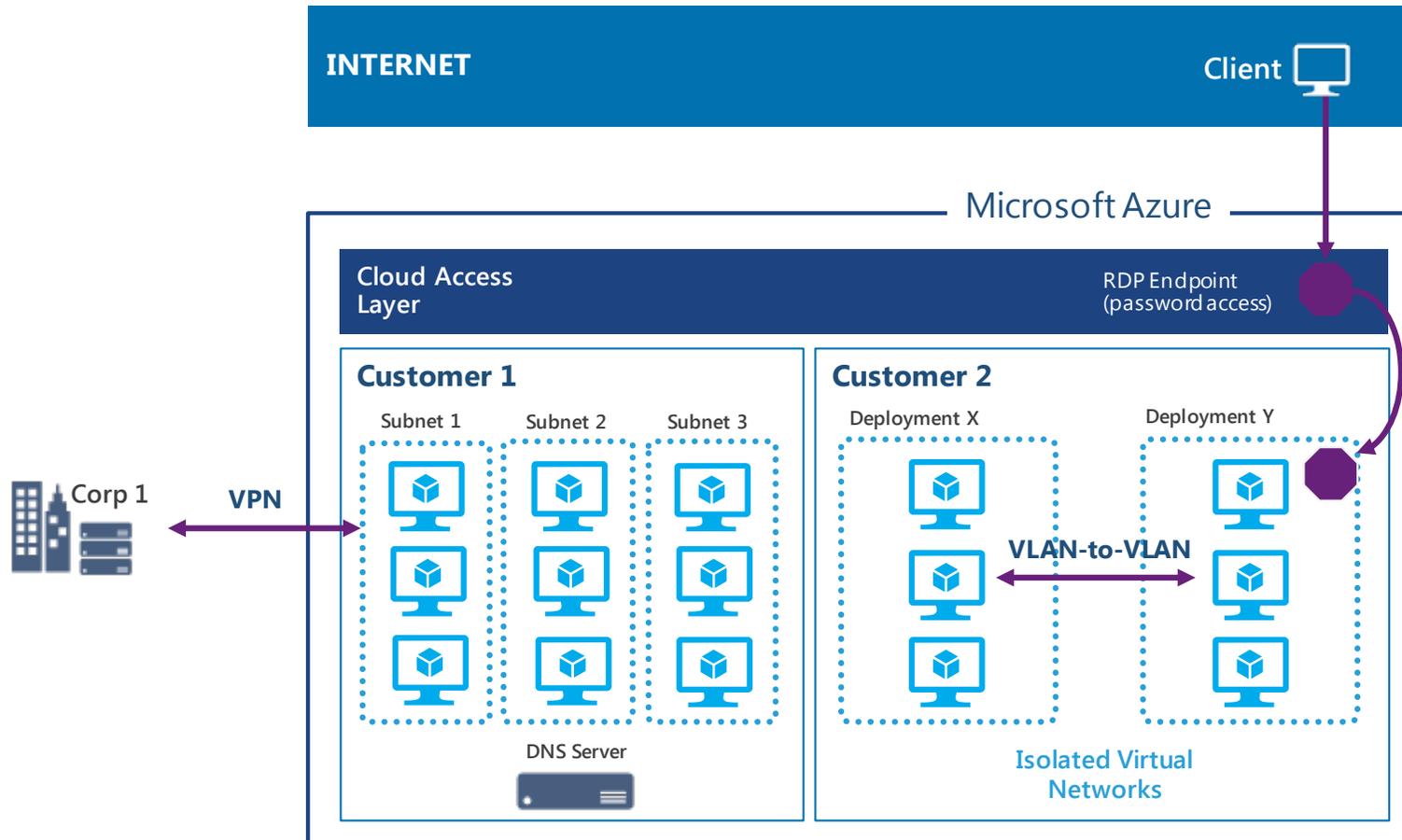
Security incidents and breach notification

Secure multi-tenancy



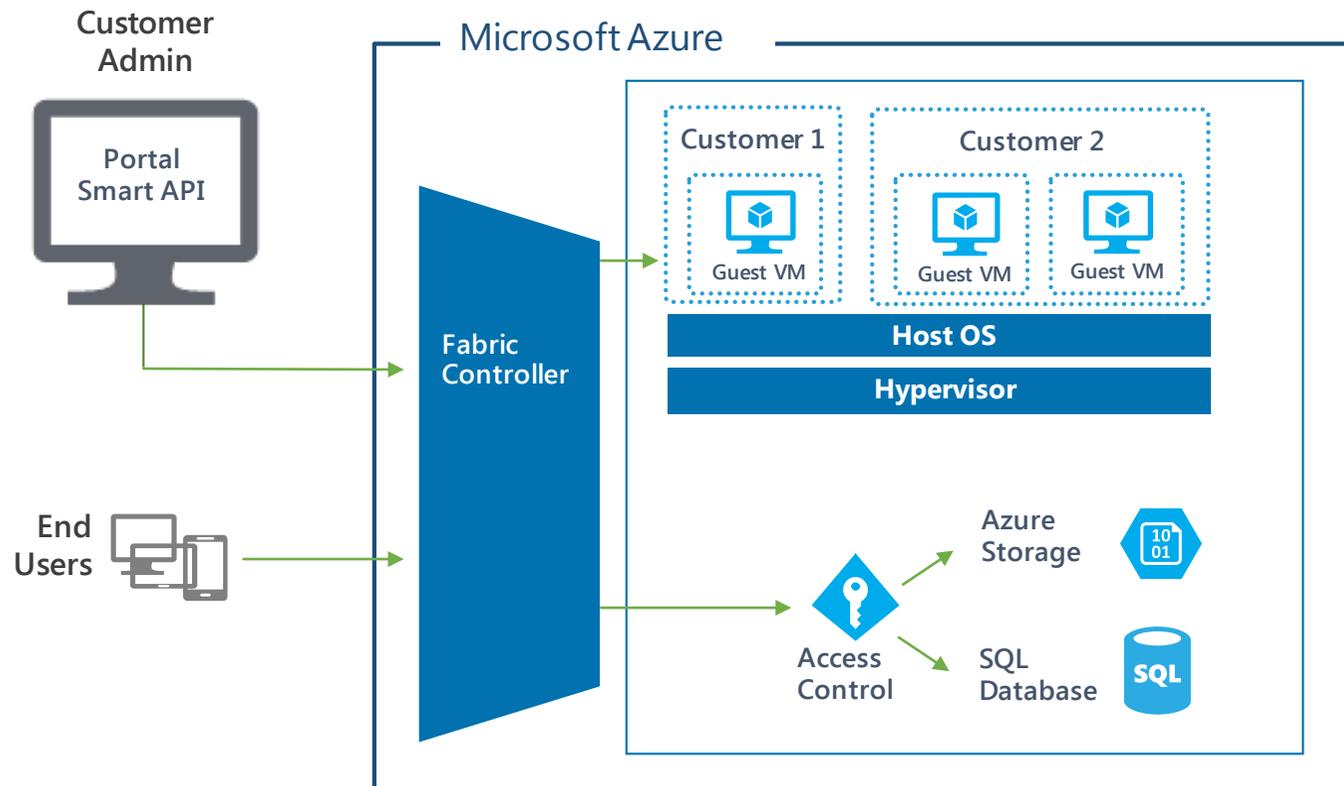
- ✓ Uses Hyper-V, a battle tested and enterprise proven hypervisor
- ✓ Runs a configuration-hardened version of Windows Server as the Host OS
- ✓ Isolates Root VM from Guest VMs and Guest VMs from one another

Network isolation



- ✓ Provides logical isolation while enabling customer control
- ✓ Private IP addresses are isolated from other customers
- ✓ Firewalls limiting traffic to VMs
- ✓ Encrypted communications

Data segregation



- ✓ Storage is allocated sparsely
- ✓ Storage Access Key controls all access to storage account
- ✓ SQL Azure isolates separate account database
- ✓ Customer A cannot read active or deleted data belonging to Customer B

Data protection

Data segregation

Logical isolation segregates each customer's data from that of others.

At-rest data protection

Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection

Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Encryption

Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data redundancy

Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.

Data destruction

When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer's data inaccessible.



Connect on-premises servers to cloud

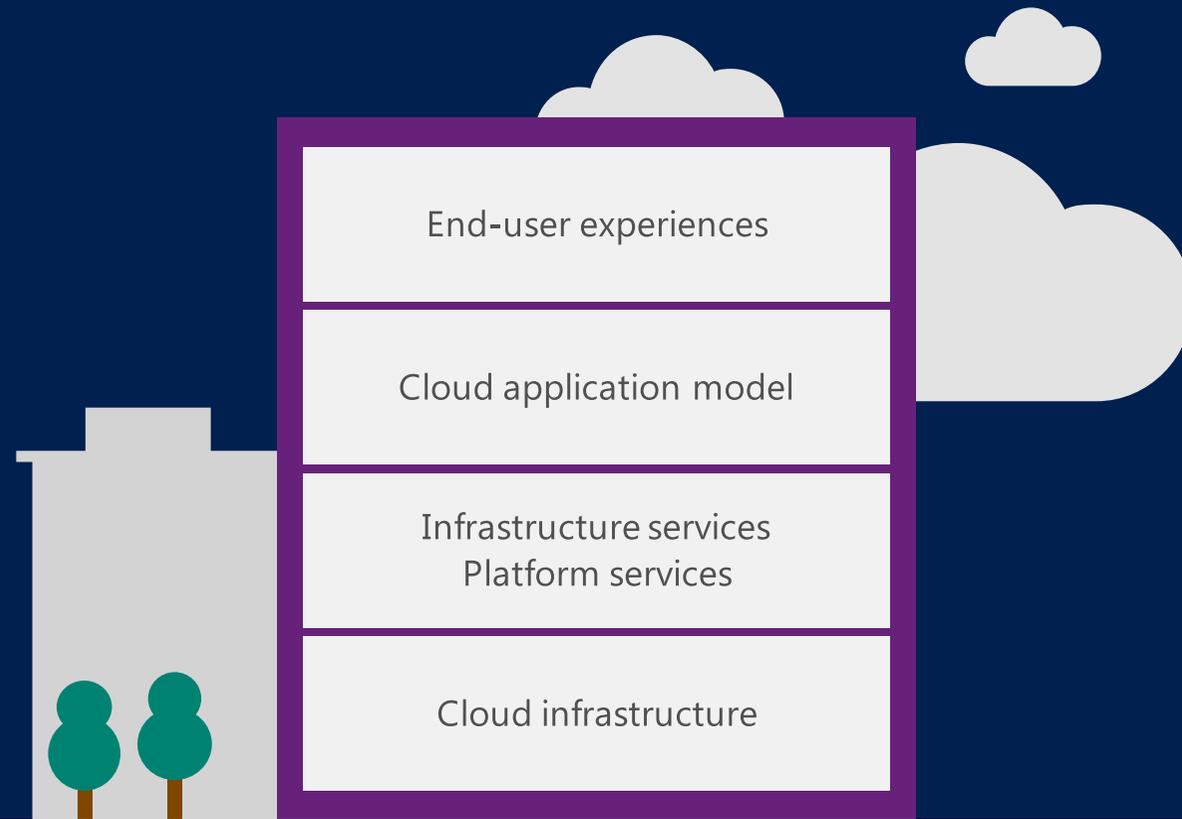


- Storage
- Backup
- Disaster recovery
- Identity
- Networking

On-Premises Datacenter



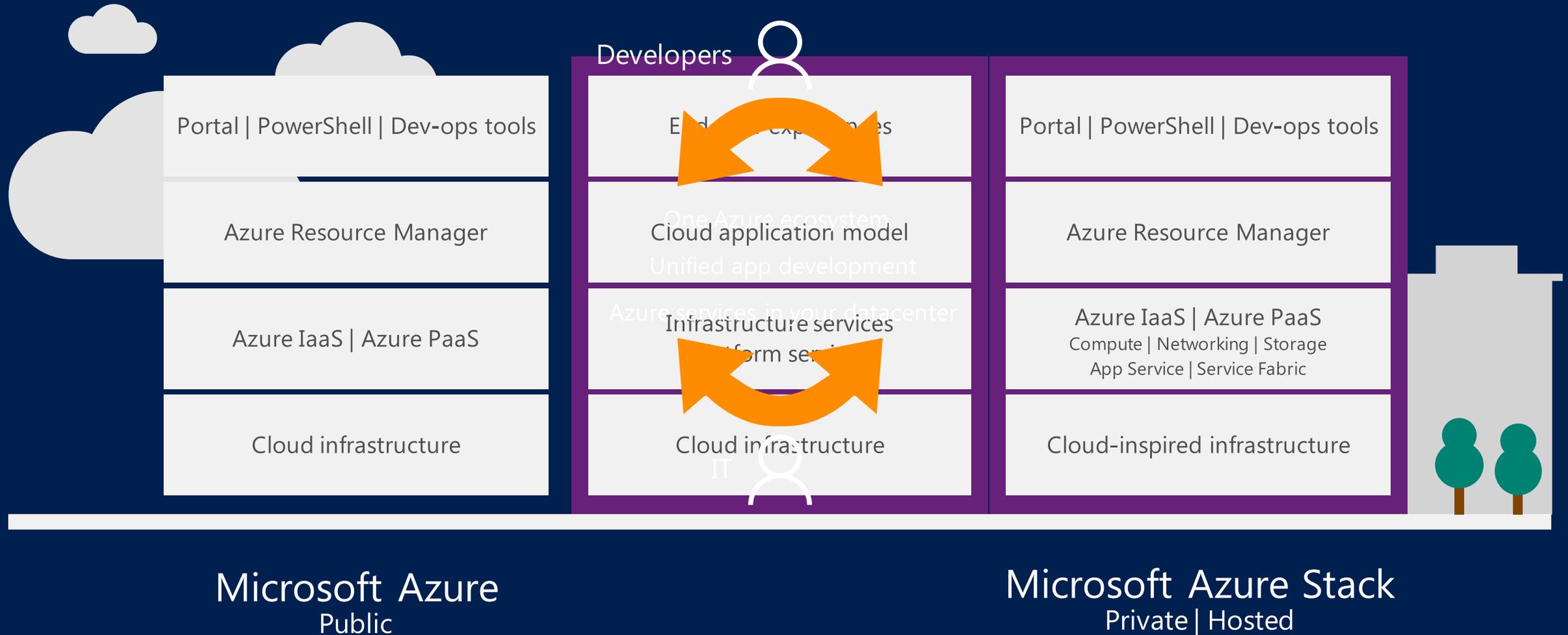
What does a hybrid cloud platform look like?



Private | Hosted | Public

Microsoft's hybrid cloud platform

Power of Azure in your datacenter





NERC CIP Implications of Cloud Computing

Tobias Whitney, Senior Manager of CIP Compliance, NERC
Reliability Assurance

RELIABILITY | ACCOUNTABILITY



NERC Standards apply to the Bulk Electric System (BES)

- Generally, 100kV and above, but with some exceptions, primarily for radial lines
- 20MVA and above generating units, 75MVA and above generating plants, with some exceptions for wholly behind-the-meter generation
- Includes Control Centers that monitor and control the BES

NERC Standards *do not* apply to distribution (i.e., non-BES)

- With several exceptions, primarily UFLS, UVLS, Blackstart Resources (generation), Cranking Paths

Cyber Asset: Programmable electronic devices, including the hardware, software, and data **in those devices.**

BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

BES Cyber System (BCS): One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

- Components of the BCS also include “glue” infrastructure components (e.g., networking infrastructure) necessary for the system to perform its reliability tasks, like network switches
- Tremendous flexibility is built into the definition – BCS could be the entire control system, or a subset based on function (HMI, server, database, FEP, etc)

Electronic Security Perimeter (ESP): The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Protected Cyber Asset (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

Electronic Access Point (EAP): A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Access Control or Monitoring Systems (EACMS): Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes intermediate Systems.

Control Center: One or more facilities **hosting operating personnel that monitor and control** the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities **at two or more locations**, or 4) a Generator Operator for generation Facilities at two or more locations.

- Includes rooms and equipment where power system operators sit, as well as rooms and equipment containing the “back office” servers, databases, telecommunications equipment, etc.
- They may all be in the same room, or be located in different buildings or in different cities.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

- i.e., “wide-area communications”

Energy Management/SCADA/AGC/Economic Dispatch – would most likely be considered a BCS (BES Cyber System).

Other considerations:

Would you support taking all transmission substation data and storing it in a cloud based HIS – including substation equipment status, P&C settings, and substation topology?

Would transmission network planning using a cloud based application and cloud based storage be considered a BCS?

If used to reduce the risk of outages, would Contingency Analysis in the cloud be considered a BCS?

If utility asset management and predictive maintenance for transmission assets be considered a BCS?

3rd Party Access CIP Applicability



Information Access

- Data classification
- Information Protection

CIP-011 – Information Protection



Temporary Access

- Escorted Access
- Periodic On-site

CIP-004 – Training and Awareness
CIP-005 – Interactive Remote Access
CIP-006 – Escorted Access



Operational Support

- Decision Support
- Data Analytics
- Interface to Cyber Assets
- Access to CEII

CIP-004 – Training and Awareness
CIP-004 – Personnel Risk Assessment
CIP-005 – Interactive Remote Access
CIP-011 – Information Protection



Real-time Operations

- Dedicated Interface to BES Cyber Assets
- Operations & Maintenance of EACMS
- Cloud Control Center Operations

All applicable standards and requirements associated with the Cyber Assets used to:

- perform the Registered Entity's reliability tasks
- Manage or operate the Registered Entities applicable systems.

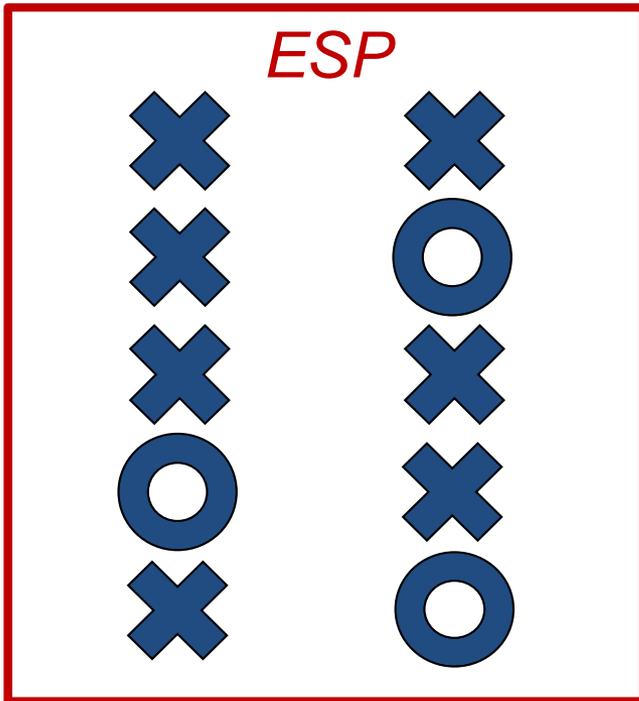
CIP definitions are “**device**” centric

- I.e., the physical computers that make up the cloud computing infrastructure

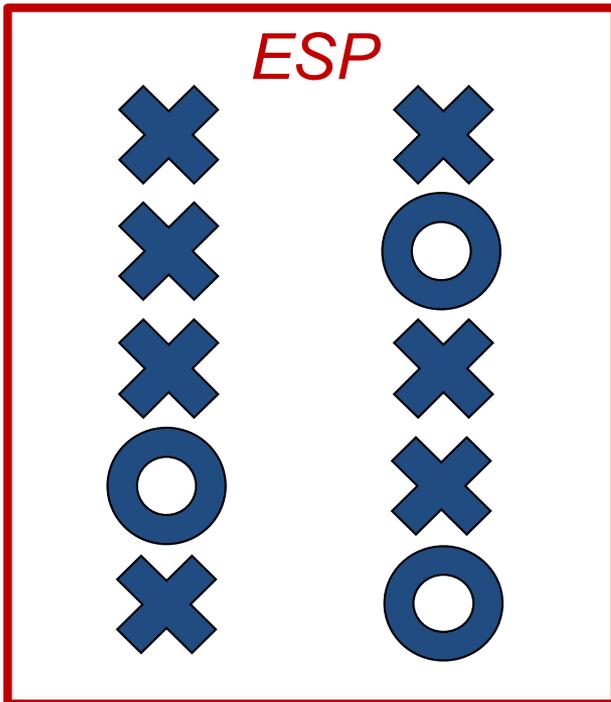
BCAs / BCSs perform “**real-time**” functions of monitoring or controlling the BES

- Includes core networking infrastructure and network attached storage necessary to perform functions
- Since the cloud implementation allows application processing to occur on different compute nodes depending on availability, virtually all computers in the cloud would be considered BES Cyber Assets

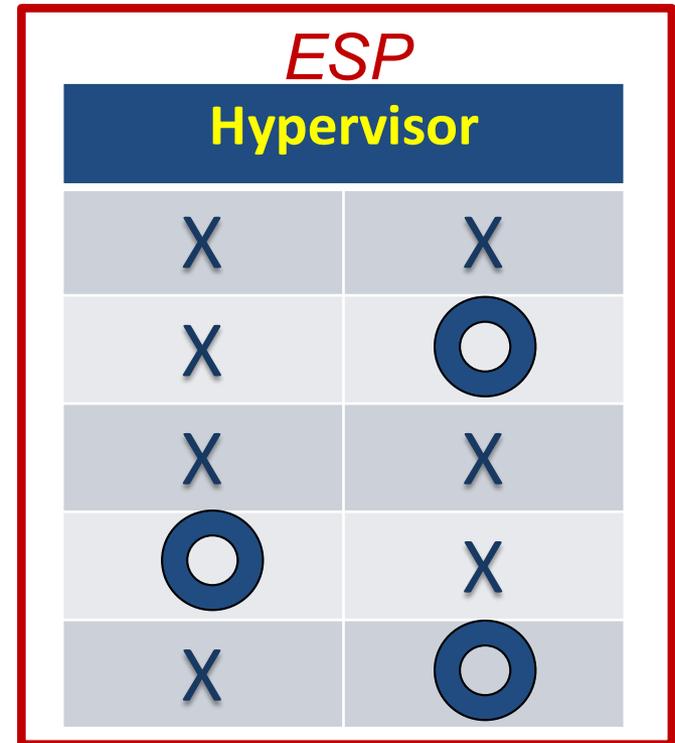
X = BCA, O = PCA



X = BCA, O = PCA

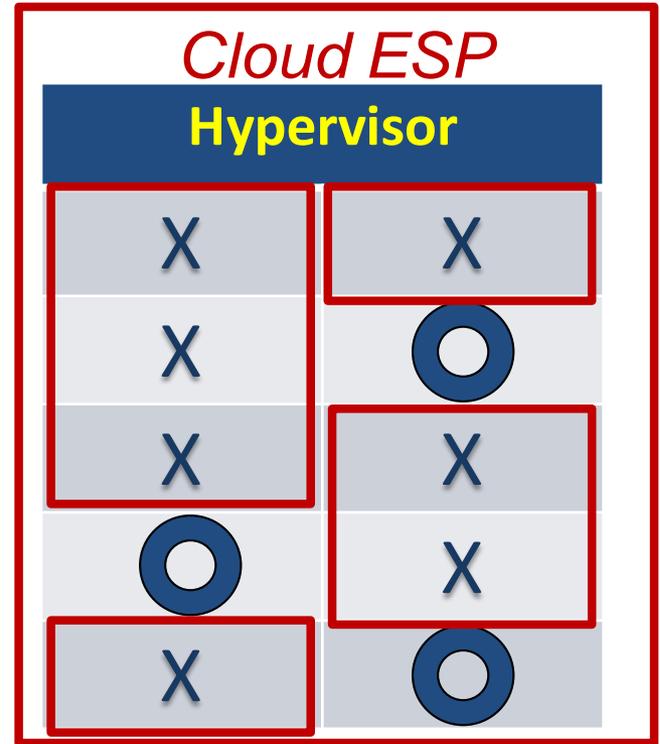
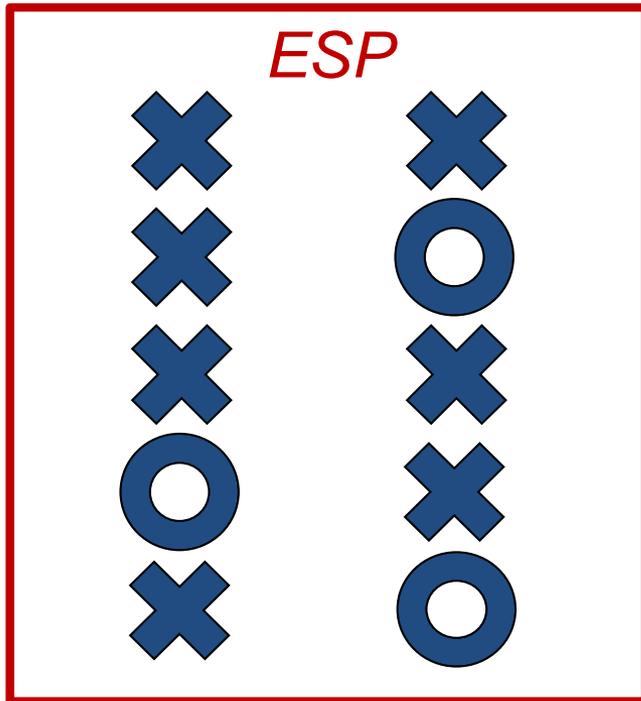


X = BCA, O = PCA



X = BCA, O = PCA

X = BCA, O = CAs



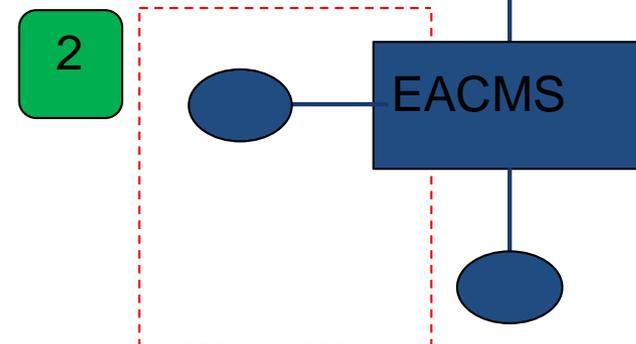
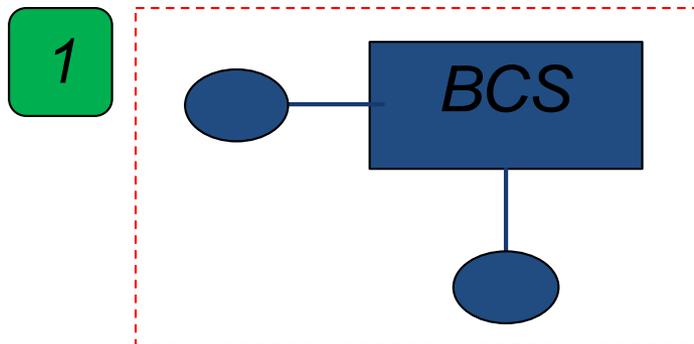
Can other Cyber Assets (O) be securely operated within one logically separated virtual environment? Is this concept supported by the standard? No it is not.

Network VLANs (mixed trust) – 2 Options

1. Network device can be considered a BCS or PCA and fully enclosed within an ESP with no connection outside the ESP.
2. Categorize the network interface as an Electronic Access Point (EAP) and treat the whole device as an EACMS. Separate, non-ESP related interfaces are permitted.

Technical discussions:

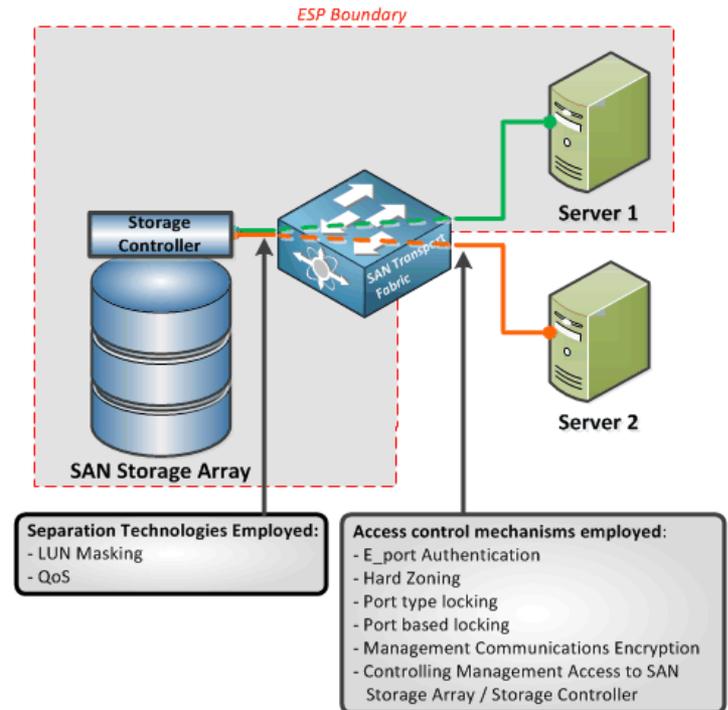
- Adequacy of layer 2 controls in CIP environment



Can virtual storage be considered BCS, PCAs, or non-impactful systems in regards to CIP?

Are real-time decisions being made?

What are the mixed-trust considerations?



BCAs / BCSs in the cloud performing Control Center functions
makes the cloud part of the defined the Control Center

BCAs / BCSs connected to a network must be surrounded by an
ESP

- Cloud border infrastructure (routers, firewalls, etc) would be considered EACMS devices, and contain EAPs

Other Cyber Assets inside the ESP are at minimum, PCAs

- All the other computers in the cloud (i.e., inside the ESP / cloud boundary) – even if configured to not execute your applications

There is no exclusion consideration for location, ownership, or other use of Cyber Assets

- All computers, network access points, users, etc. of the cloud, regardless of who owns them or uses them, are therefore subject to the Registered Entity compliance obligations

CIP-004-6, R2 (formal training), R3 (personnel risk assessments) and R4 (access authorization)

- All personnel with electronic or physical access to BES Cyber Systems and EACMS must undergo entity specific training, entity defined PRA, and be individually authorized by the entity
- The standards do not restrict these requirements to only entity employees – they are specifically broad to include vendors and contractors

CIP-005-5 Requirement 1 (ESP and border protections)

- All traffic crossing the ESP in either direction must be authorized, with rationale for granting access, and traffic must be inspected for known or suspected malicious activities
- Not just your traffic, or traffic to your site

CIP-006-6 Requirement R1 (physical security perimeters)

- All medium impact BES Cyber Systems with External Routable Connectivity must utilize at least one physical access control to restrict access to personnel individually authorized by the entity
- All high impact BES Cyber Systems with External Routable Connectivity must utilize at least two physical access control to restrict access to personnel individually authorized by the entity
- Monitoring and alarming required

CIP-007-6 R2 (patching)

- All high and medium impact BES Cyber Systems, PCAs, and EACMS must have a patch management program to analyze patches at least every 35 days, and install or mitigate all patched vulnerabilities within 35 days of the completion of the analysis

CIP-007-6 R4 (event monitoring)

- All high and medium impact BES Cyber Systems, PCAs, and EACMS must have security event monitoring, including alerting, log retention, and a process to identify undetected Cyber Security Incidents (high)

Standard Drafting Team currently working on a number of issues, including virtualization

- Looking at modifying definitions to accommodate “virtual” environments – moving away from strict “device centric” approach
- Current reading of standard appears to not support “mixed-mode” (i.e., combining BES Cyber System and non-BES Cyber System environments on common hardware)

