OSIsoft for Federal Facilities

Meeting your Energy Management Mandates

The Value of a Data Infrastructure

24-August-2016

OSIsoft.

Speakers

Noah Goldstein
Director, Custom Research
Noah.Goldstein@navigant.com

David Doll
Industry Principal
ddoll@osisoft.com

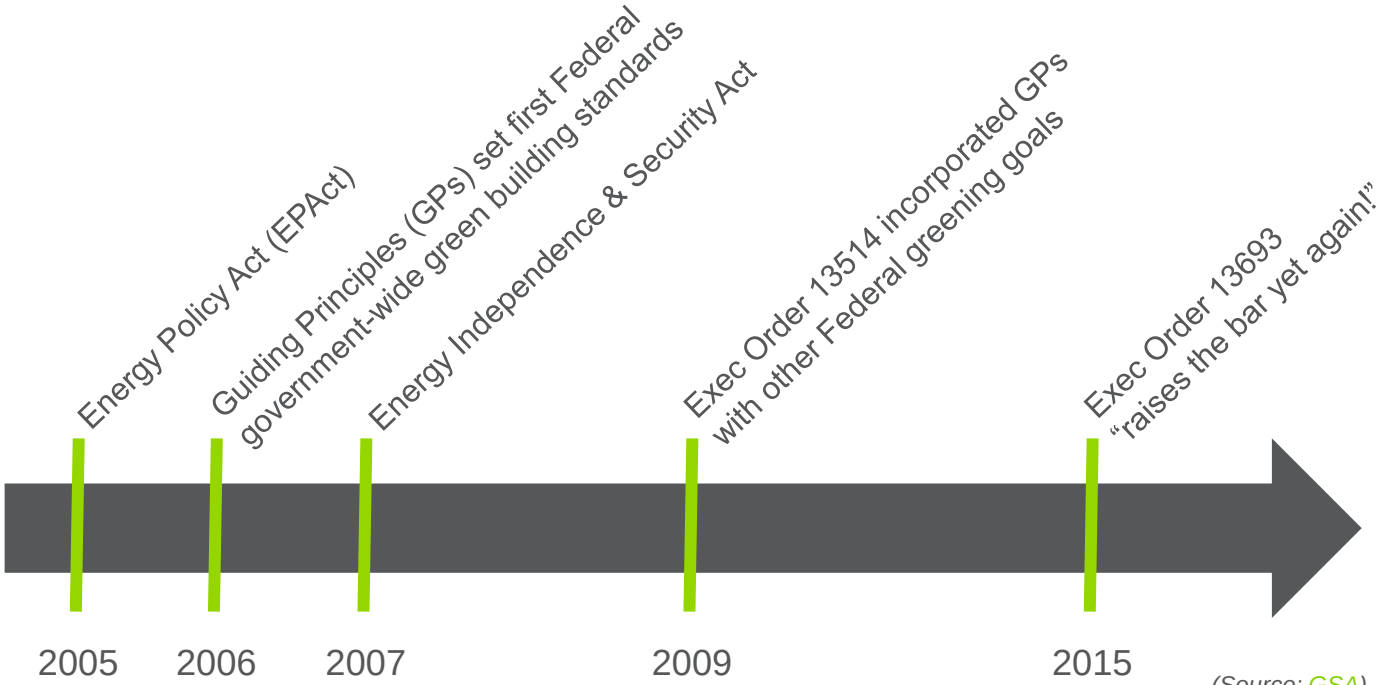
EVOLUTIONARY & DISRUPTIVE MARKET TRANSFORMATION

ENERGY AND SUSTAINABILITY

FEDERAL SECTOR IMPACTS

NAVIGANT

FEDERAL LEADERSHIP ON SUSTAINABILITY



(Source: GSA)

NAVIGANT

EXECUTIVE ORDER 13693
OVERARCHING POLICY & DIRECTIVES FOR IMPLEMENTATION

"To improve environmental performance and Federal sustainability, priority should first be placed on reducing energy use and cost, then on finding renewable or alternative energy solutions."
– Executive Order 13693

Data **Sensors** **Analytics**

Energy Conservation and Renewable Energy: ● ● ●

Climate Change Resiliency: ● ●

Greenhouse Gas (GHG) Emissions Reduction and Reporting: ● ●

Green Building Performance: ● ●

Water and Storm water Management: ● ●

Performance Contracting: ● ● ●

Strategic Sustainability Performance Plan: ●

THE DETAILS

Executive Order (EO) 13693 was signed March 19, 2015. EO 13693 introduces new requirements and expands upon requirements established by EO 13514, EO 13423, the Energy Policy Act of 2005 (EPAct 2005), and the Energy Independence and Security Act (EISA) of 2007

GOALS:

- Energy Conservation and Renewable Energy
  - Reduce energy intensity (measured in British thermal units per gross square foot) 2.5 percent annually through FY 2025, compared to a baseline year of FY 2015.
  - Use renewable electric energy for 30 percent of total building electricity use by FY 2025.
  - Use renewable electric energy and alternative energy for 25 percent of total building energy use by FY 2025.
- Climate Change Resiliency
  - Incorporate climate-resilient design and management elements into the operation, repair and renovation of existing buildings and design of new buildings.
- Greenhouse Gas (GHG) Emissions Reduction and Reporting
- Green Building Peformance
- Water and Stormwater Management
- Fleet Performance
- Employee Commuting and Workplace Travel
- Sustainable Acquisition
- Solid Waste Diversion and Pollution Prevention
- Performance Contracting
- Electronics Stewardship
- Strategic Sustainability Performance Plan

(Source: White House)

GSA GUIDANCE FOR EO IMPLEMENTATION
ILLUSTRATIVE CHANGES

Issue	Previous Goals	New EO Goals
Scope 1 and 2 GHG	Cut 28.7% (from FY08 base to FY20). (Set agency goal)	**Cut 40%** (from FY08 base to FY2025). (Set agency goal.)
Scope 3 GHG	Cut 14.6% (from FY08 base to FY20). (Set agency goal.)	**Will include leased space.** (Set agency goal.)
Energy Use Intensity (BTU/GSF)	Cut 30% (from FY03 base to FY15; 3% per year).	**Cut 25% more** (from FY15 baseline to FY25; 2.5% per year)
"Clean Energy" target for total building electric plus thermal energy	N/A	**Renewable electric plus alternative energy** from 10% of total building **electric plus thermal** energy in FY16 **to 25%** by FY25
Renewable Electricity target	From 10% of electric use in FY15 to 20% in FY20 (12/13 Pres. Memo)	From 10% in FY16 **to 30%** by FY25
Mandatory lease clauses	Energy Star label required (EISA)	Energy efficiency required plus **lessor to disclose CO2 emissions or energy consumption** for agency-occupied portion of building (10k+ RSF)

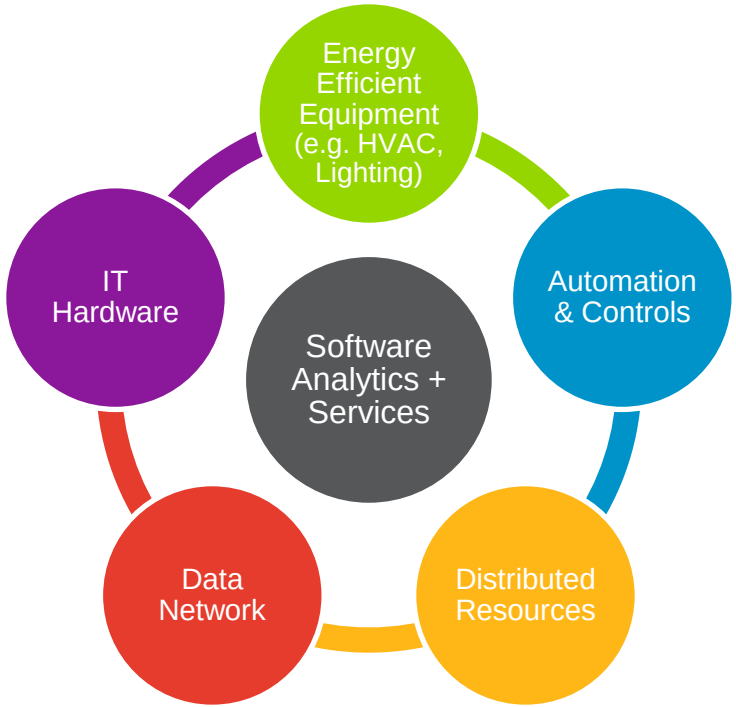
(Source: GSA)

FEDERAL CUSTOMER PRESSURES

Facility Class	Key Priority	Applications & Functionality
Mission Critical (Data Centers, DoD)	Uptime/Reliability, Resilience	Optimization, Services
Mixed Use (Campus, Portfolio)	Operational Efficiency, Cost Containment	Predictive Analytics, Services
Leased Space (Office)	Occupant Satisfaction, Sustainability	Visualization, Reporting, FDD

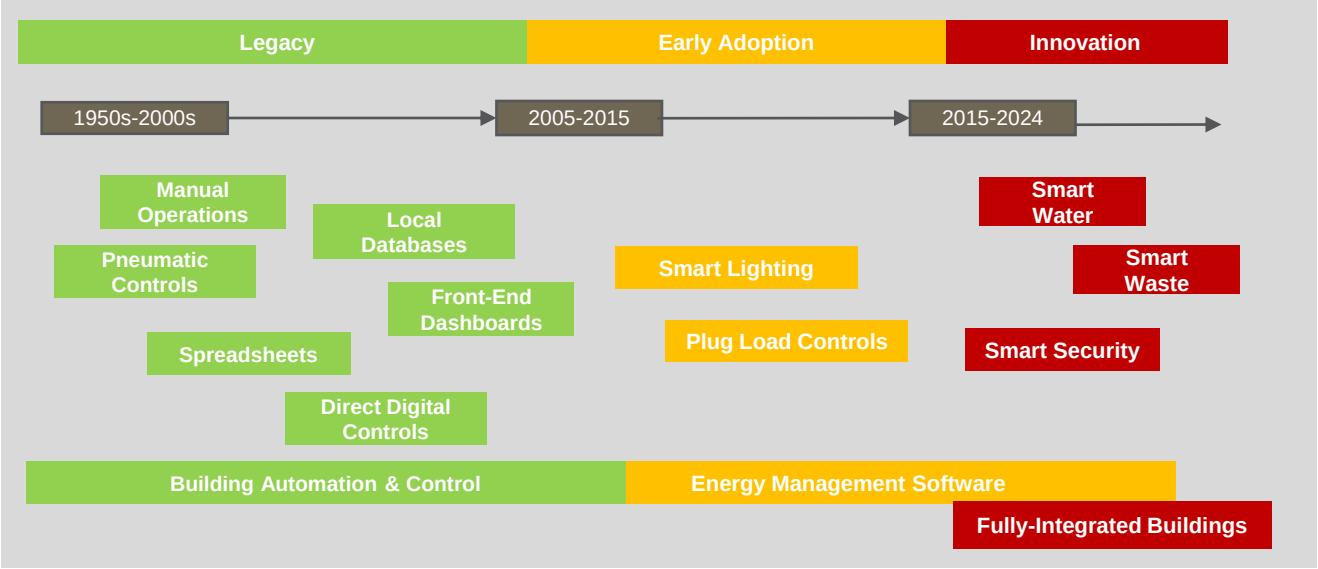
DEFINITION | Software Analytics Drive Performance Improvement

An intelligent building is a facility optimized by continuous, automated performance improvement in the operations of building systems as directed by software analytics.

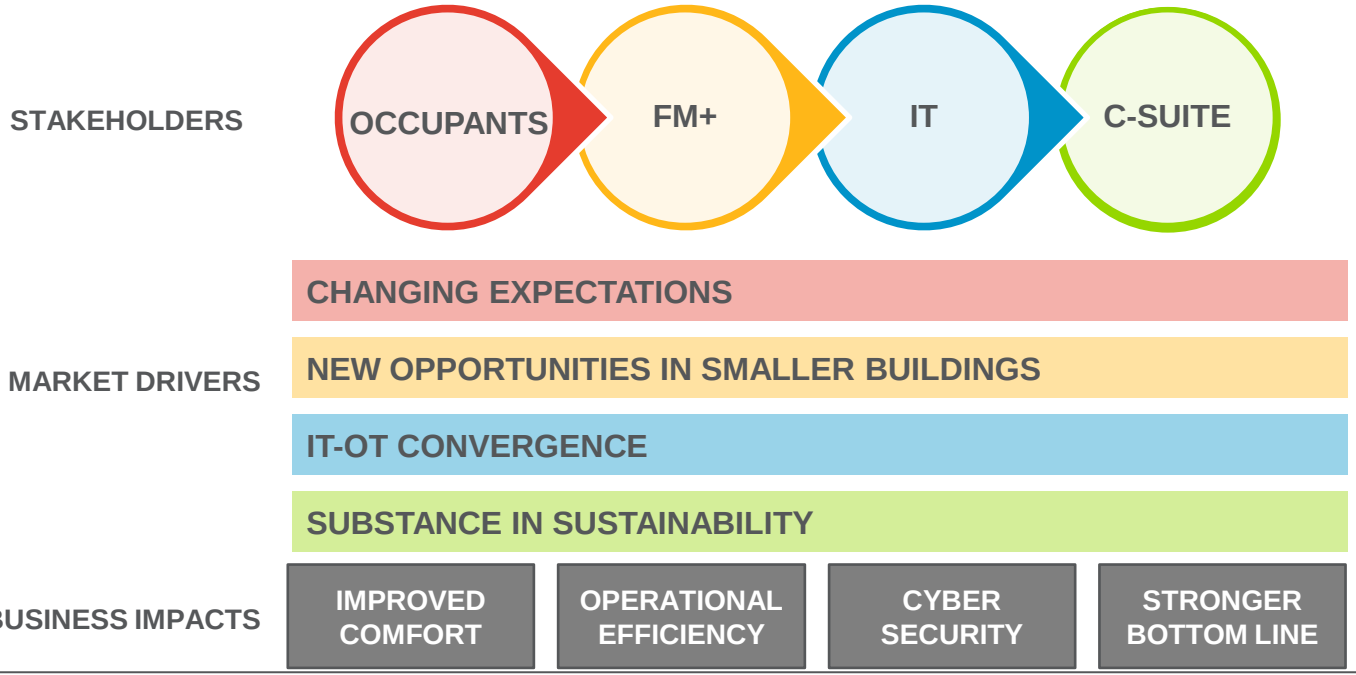


NAVIGANT

DEFINITION | Technology Roadmap to Fully-Integrated Intelligent Buildings



NAVIGANT



NAVIGANT

How to move forward

MANDATES…

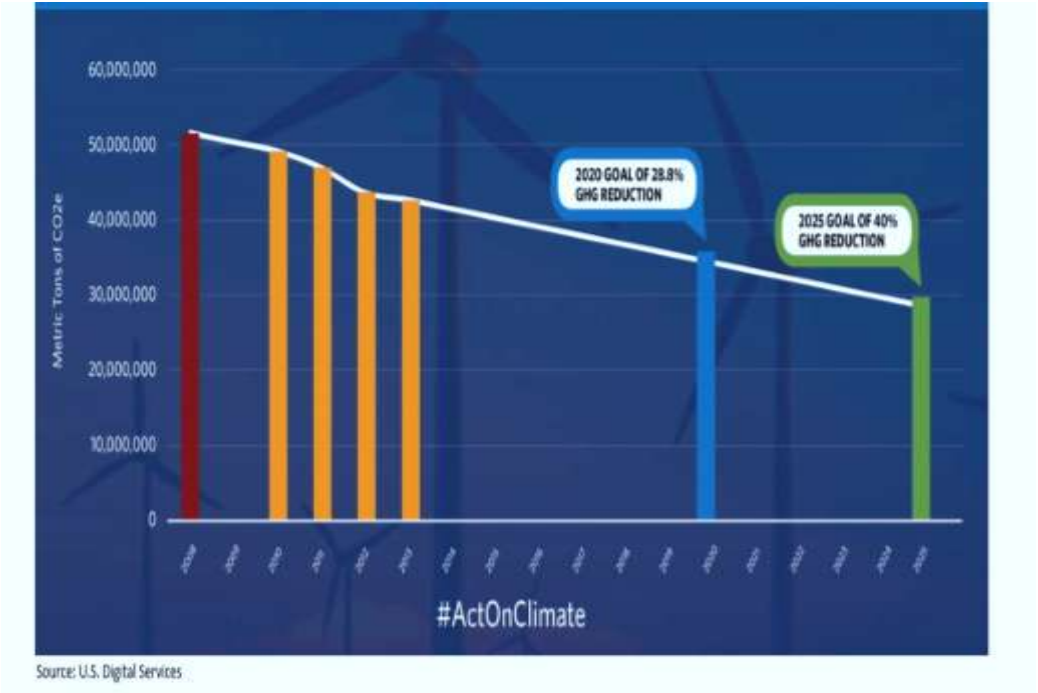
Executive Order 13693 (2015)

By 2018 (data centers)

- Install *and monitor* energy meters in all data centers
- New DC PUE ≤ 1.4
- Existing DC PUE ≤ 1.5

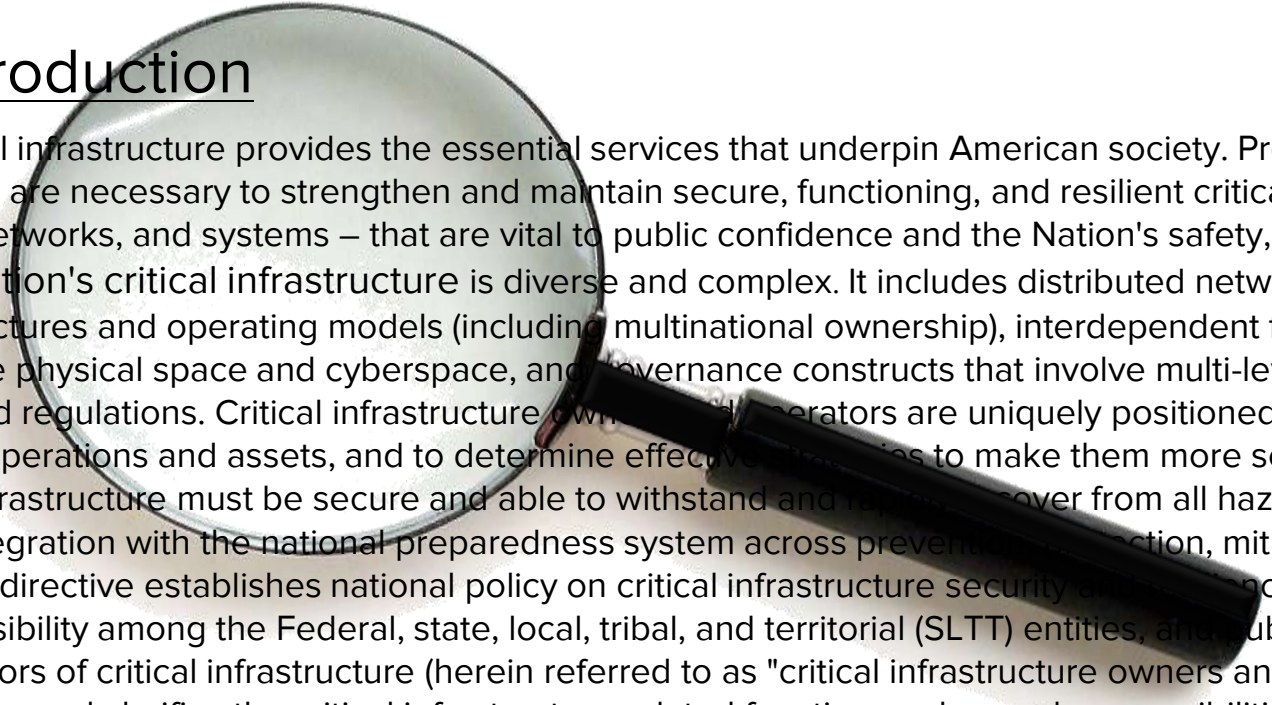
By 2025 (all facilities)

- -40% total GHG
- -25% total energy
- 30% renewables
- 15% net-zero buildings



And more MANDATES

PPD-21 Introduction



The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being. The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient. Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery. This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators").This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively

So what problems are getting in the way?

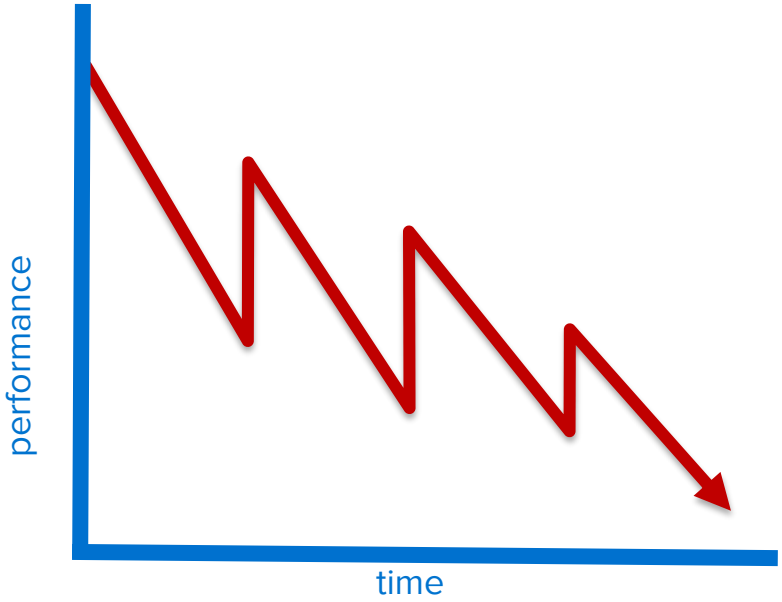
Problem: Lots of infrastructure to monitor

- Federal owns and leases over 275K+ buildings*
  - Over 2.8B sq ft
  - Many different systems (data sources) and many without any
- Existing data centers:
  - 2010: Est 3100 (>500 sq ft)
  - 2013: Est 7000 (after 420 closed)
  - 2015: Est 6000 (after closing 3800)

Federally owned cabin in Great Smoky Mountains National Park. Listed in the FRPP database as being in excellent condition.

*USA only, Federal Real Property Profile

Problem: The Inevitability of Failure



Problem: Understanding IT versus OT

IT Systems

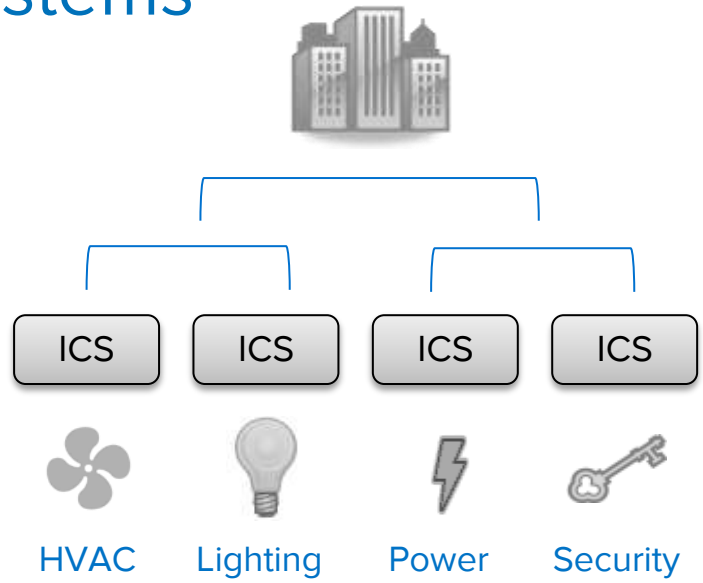
Business Systems
Rows and columns
Relational
Record-based
Clean schema

OT Systems

Meters, ICS, IoT
Sensor values
Streaming
Time-based
Unpredictable

Problem: The Limits of Control Systems

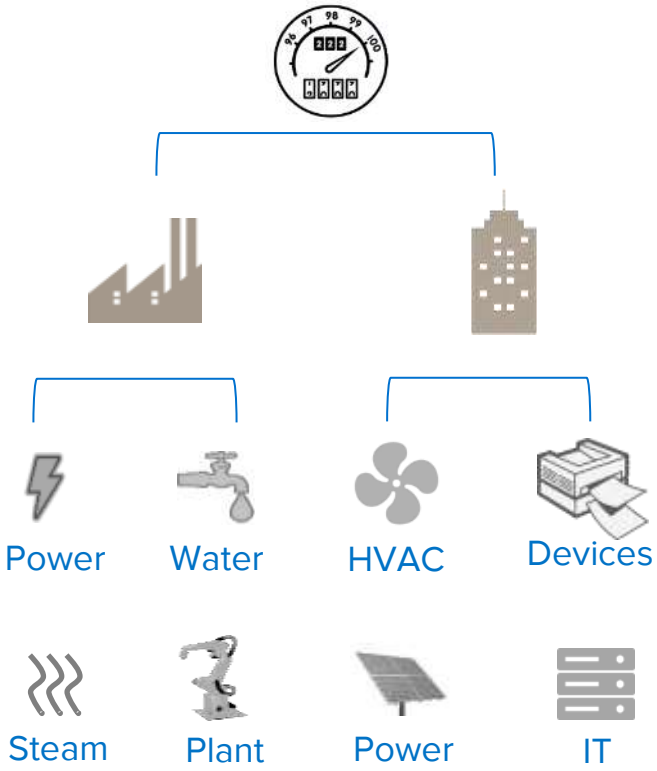
- Any Control System is myopic
  - Only knows about assets it controls
  - Only as good as its programming
  - Doesn't include energy usage
- What should it be doing?
  - How to validate programming?
  - How to compare other systems or sites?
  - Limited history, analytics, and fault detection
  - How to normalize data to give context?



ICS = Industrial Control System

Problem: The Limits of Meters

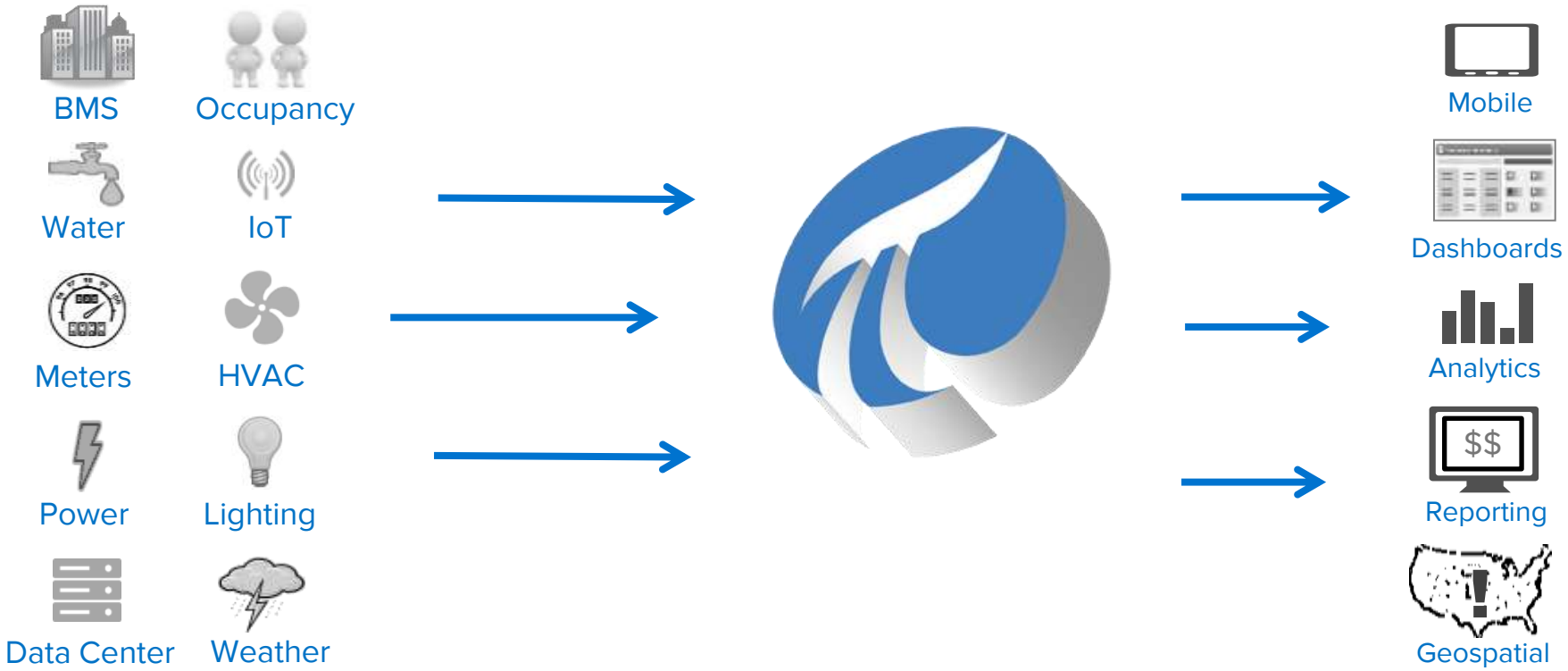
- How much energy am I using?
  - How frequently do I get the data?
  - Monthly? Daily? Hourly? Today? Yesterday?
- Where am I using energy?
  - One meter for multiple buildings/assets
  - Can't see below the meter
- What can I do about it?
  - No visibility on my impact
  - No insight on how to improve



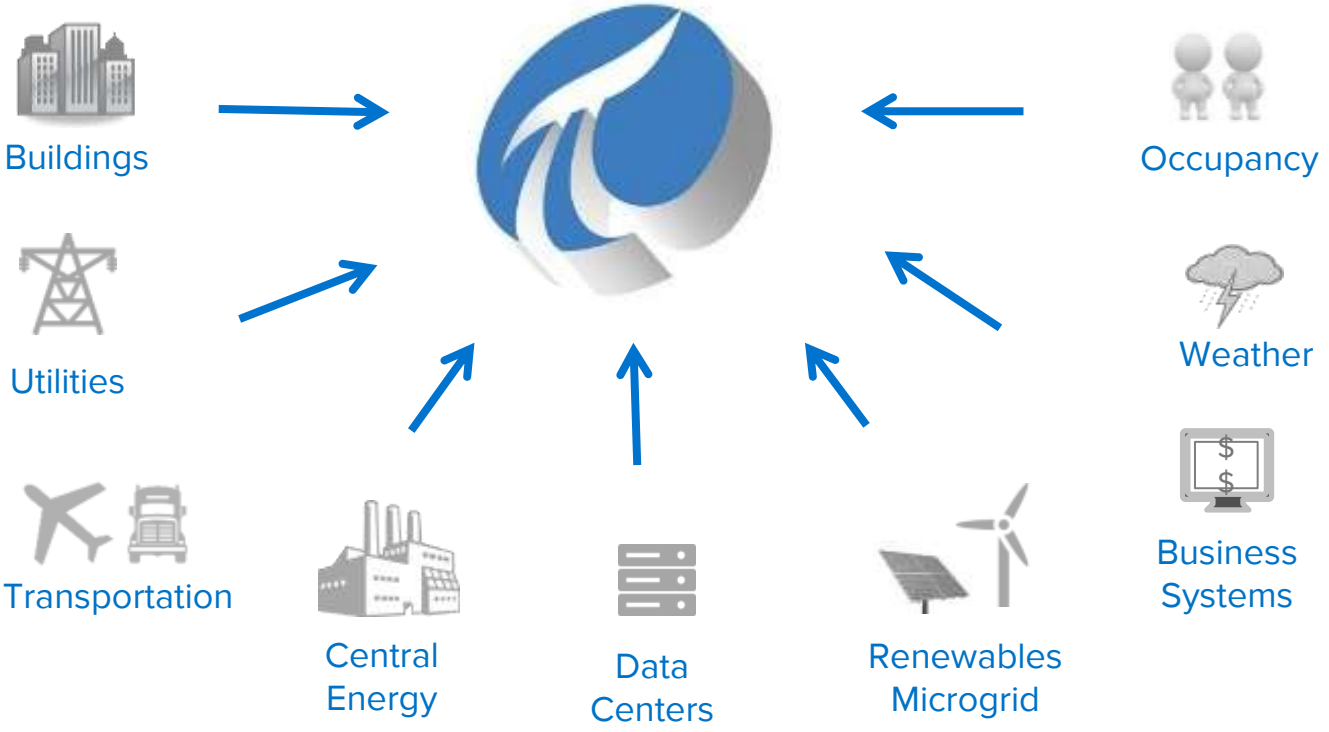
Problem: Tomorrow's Technology

The PI System as your Data Infrastructure

Collect from multiple systems. Store ALL of your data. Use ALL of your data.



Common Data Infrastructure: Campus / Base



The Need for a Data Infrastructure

Connecting data and insight to multiple users and roles

IT Operations

Engineering

Management

Facility Operations

Users/Occupants

Maintenance

Reliability **Compliance** **Energy Surety**

Innovation **Efficiency** **Performance**

Cyber Risk Management

Critical Systems

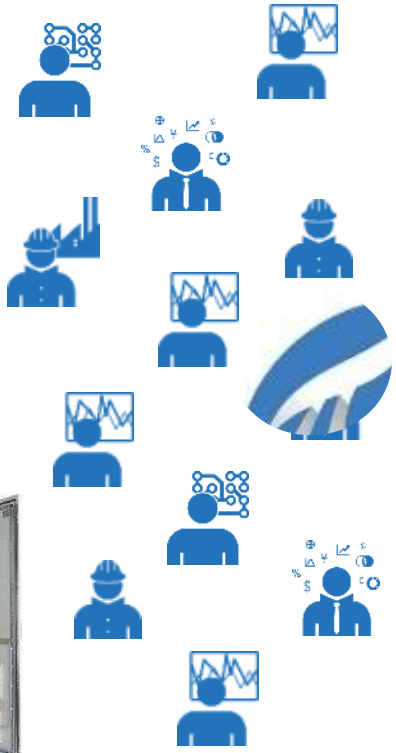
Power and Utilities Systems

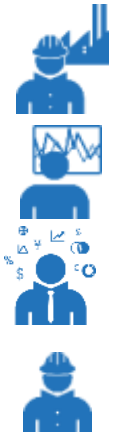
IoT Systems

PLCs

Building Control Systems

Other critical operations systems





Success Stories

A wide range of customers in the energy space

THE UNIVERSITY OF IOWA

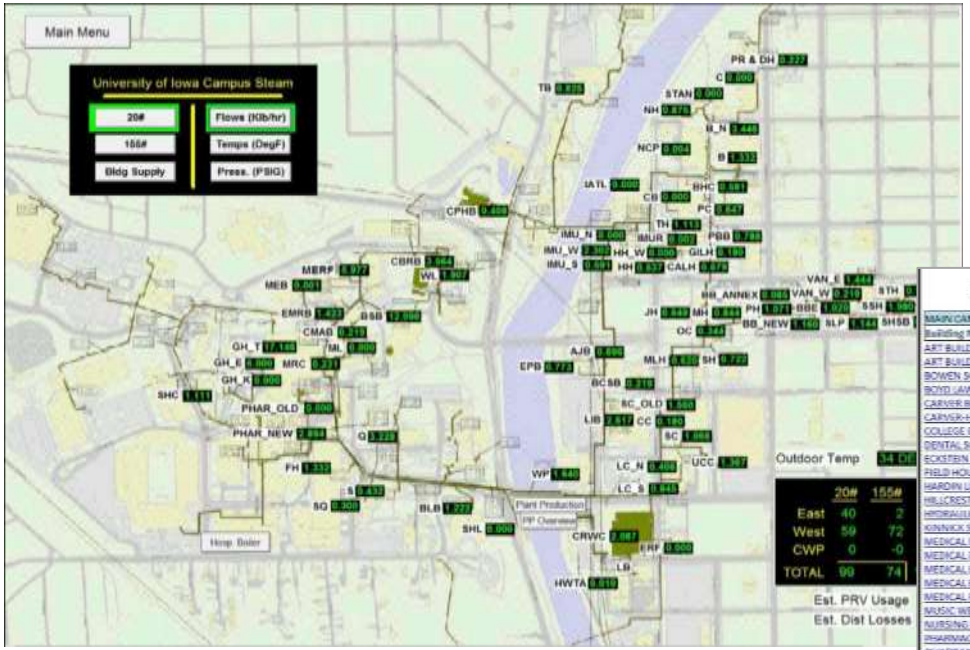
Students: 31K

120 major buildings

15M sq ft

GOAL: Maintain 2010 baseline despite a billion dollars in new construction

Real-time energy dashboards



facilitiesnet

Bringing Energy Understanding to Occupants, Tenants

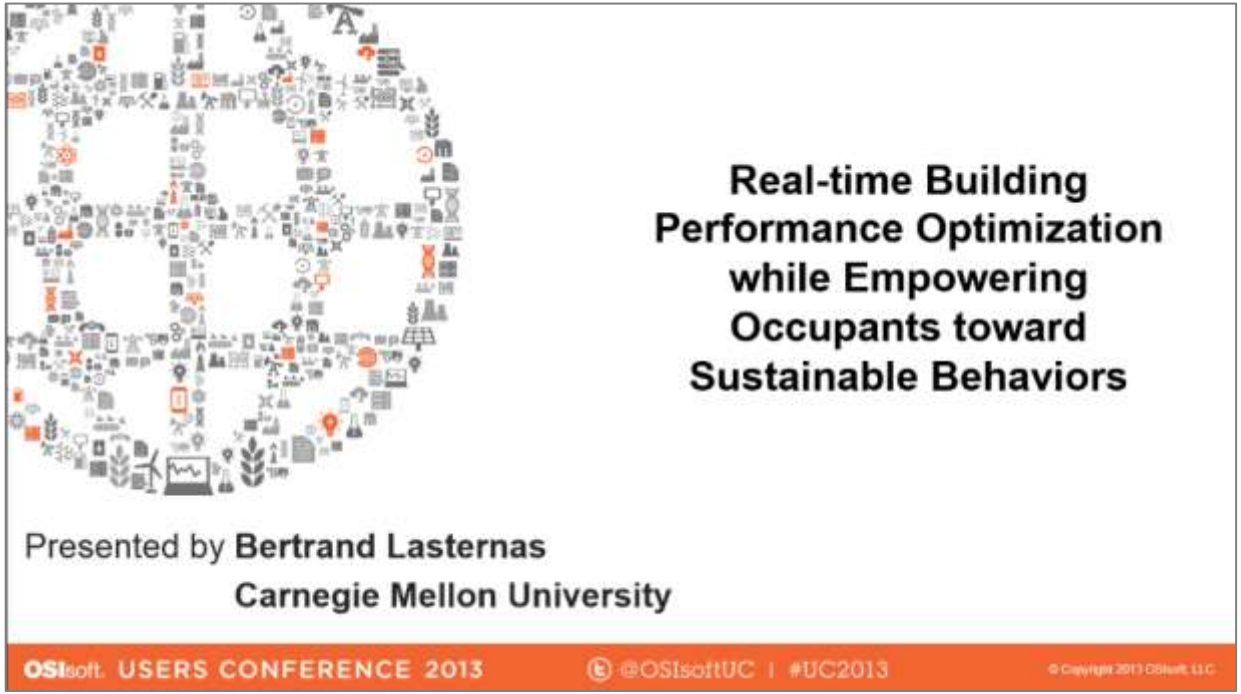
"The end goal for any real-time energy monitoring system might look like what's in place at the University of Iowa. There, a system of thousands of meters and at least 100,000 data points is constantly monitored and analyzed to identify problems and opportunities for greater efficiency....

In total, with the support of the Energy Hawks and the Energy Control Center, the University of Iowa is saving more than $1.5 million per year on energy costs, against its 2010 baseline."

building operating management

http://www.facilitiesnet.com/energyefficiency/article/Bringing-Energy-Understanding-to-Occupants-Tenants--16177

Carnegie Mellon University



Overview

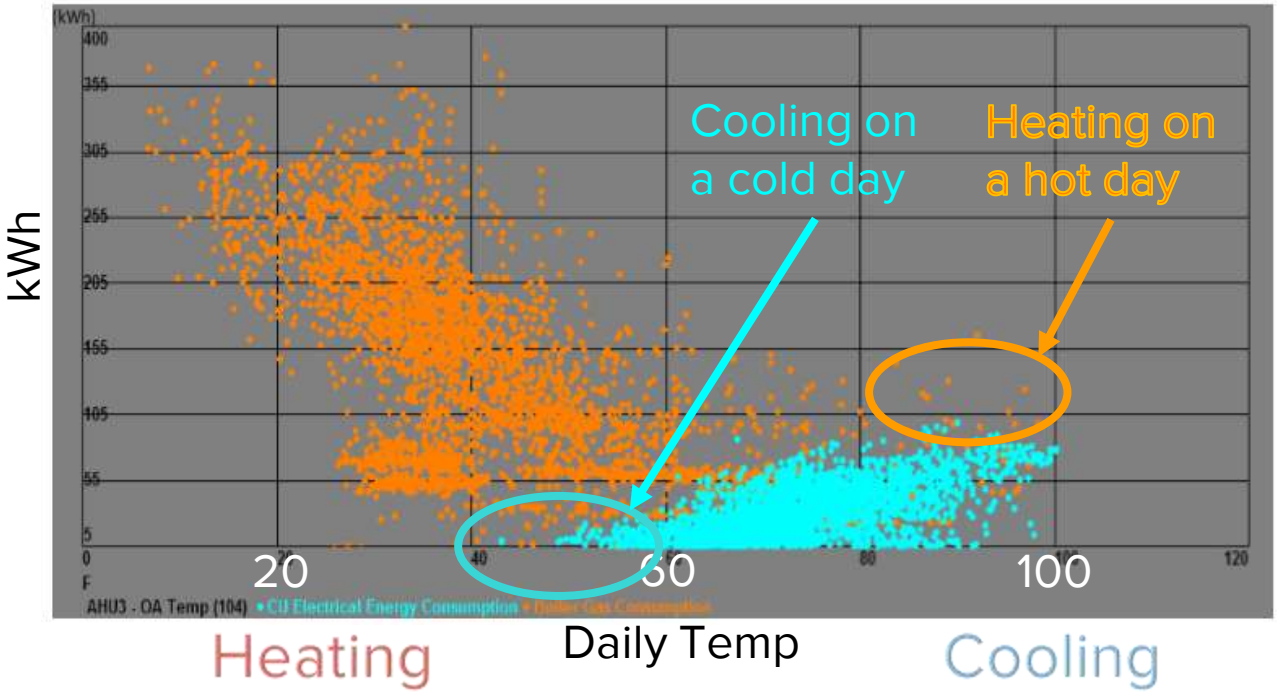
- 12,991 Students (6223 undergrad)
- CMU annual energy budget over $20M
- MANDATE: Improve by 30%

Visibility into Heating and Cooling

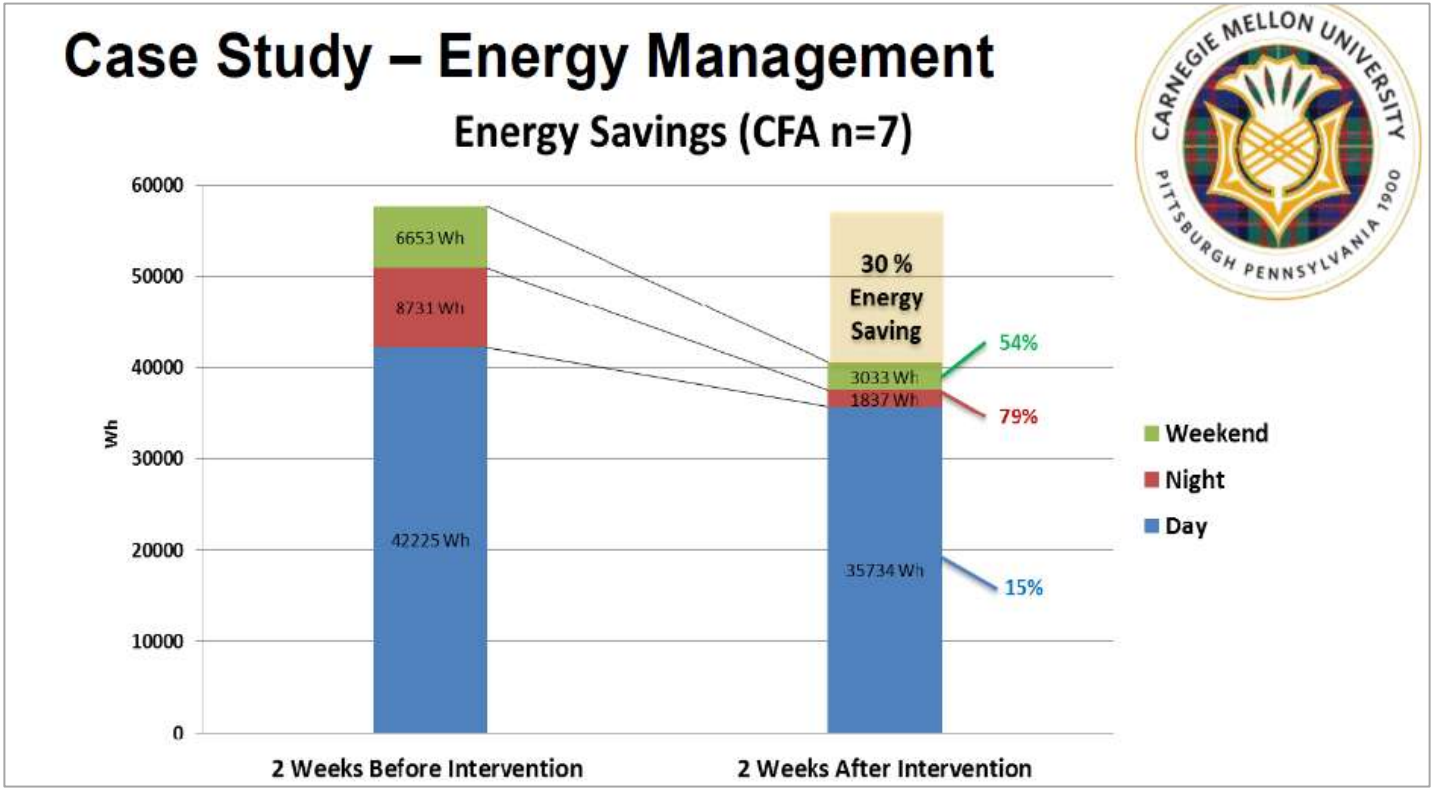
Carnegie Mellon

Avoiding heating when it's 98° outside… Or cooling when it's 40°

- Visibly into when and why heating and cooling systems were actually running
- Found accidental heating on hot days and cooling on cold days



Carnegie Mellon University



NIST National Cyber Center of Excellence

Energy Sector Situational Awareness Use Case

- “Standards-based cybersecurity”
- Deploy a “secure, practical, and scalable” architecture
- Adopt “state-of-the-art cyber technologies that meet and promote NIST’s mission”

INTELLIGENCE COMMUNITY NEWS

OSIsoft's PI system deployed by NIST National Cyber Center of Excellence

January 27, 2016 by Loren Blinde Leave a Comment

OSIsoft, LLC, of San Leandro, CA announced on January 26 that The National Institute of Standards and Technology's (NIST) National Cyber Center of Excellence (NCCoE) is deploying the PI System to accelerate integration and adoption of standards-based cybersecurity tools. OSIsoft's ability to manage data from diverse operations technology (OT) and information technology (IT) sources will help ensure that secure, practical and scalable technologies are implemented throughout the nation's cyber infrastructure. NIST's selection is representative of the deployment of the PI System throughout critical infrastructure and key resource sectors.

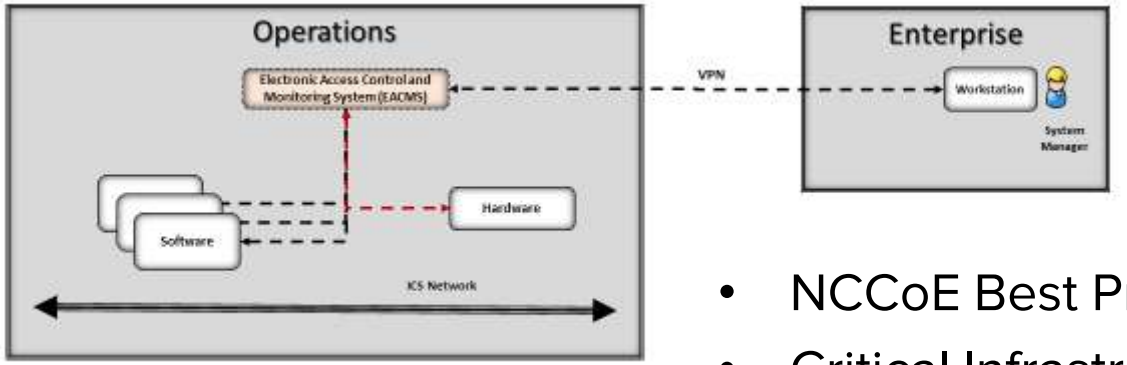
Project Performance Company (PPC), a longstanding NIST service provider and OSIsoft integration partner, is managing the implementation and configuration of the PI System, which includes testing of its varied data sources.

"The PI System is well positioned to help NIST accomplish its mission at the NCCoE," said Steven Sarnecki, vice president of federal and public sector at OSIsoft. "By utilizing our deep bench of almost 500 interfaces to different industrial control systems and data sources, U.S. cybersecurity management systems can be transformed from disconnected silos of information to an integrated, near-real-time situational awareness platform."

The vast majority of the nation's energy and industrial companies are already using the PI System to improve the security of their OT by detecting emerging anomalous conditions and taking corrective action before problems arise.

"A key benefit of deploying the PI System at the NCCoE is the ability to share findings in a collaborative environment that will help accelerate adoption of state-of-the-art cyber technologies in line with NIST's mission," said Paul Straasser, chief executive officer at PPC. "We are looking forward to realizing results."

NIST NCCoE Architecture at Univ Maryland



- NCCoE Best Practice architecture
- Critical Infrastructure security (PPD-21)
- Ensure data can only flow OUT
- OSIsoft Services

"Provide converged situational awareness across Operations and Business systems as well as physical security of buildings and other facilities."

What did we cover?

- Many overlapping mandates; single solutions not enough
- Requires continuous monitoring to improve over time
- OT monitoring needs the right tools (different than IT)
- Combining today's disparate systems and tomorrow's technologies needs a Data Infrastructure approach

The PI System provides unmatched capabilities for scalability, flexibility, security, and empowerment

OSIsoft Federal Contacts

Steve Sarnecki	VP, Federal Sales	ssarnecki@osisoft.com
Stephen Bates	Director, Advanced Analytics	sbates@osisoft.com
Bob Conroy	Account Executive	rconroy@osisoft.com
Paul Geraci	Senior Director, Intelligence and National Security	pgeraci@osisoft.com
Richard Goode	Federal Account Manager	rgoode@osisoft.com
Jeremiah Carroll	Federal Partner Manager	jcarroll@osisoft.com

Thank You

www.osisoft.com/federal

www.osisoft.com/corporate/facilities