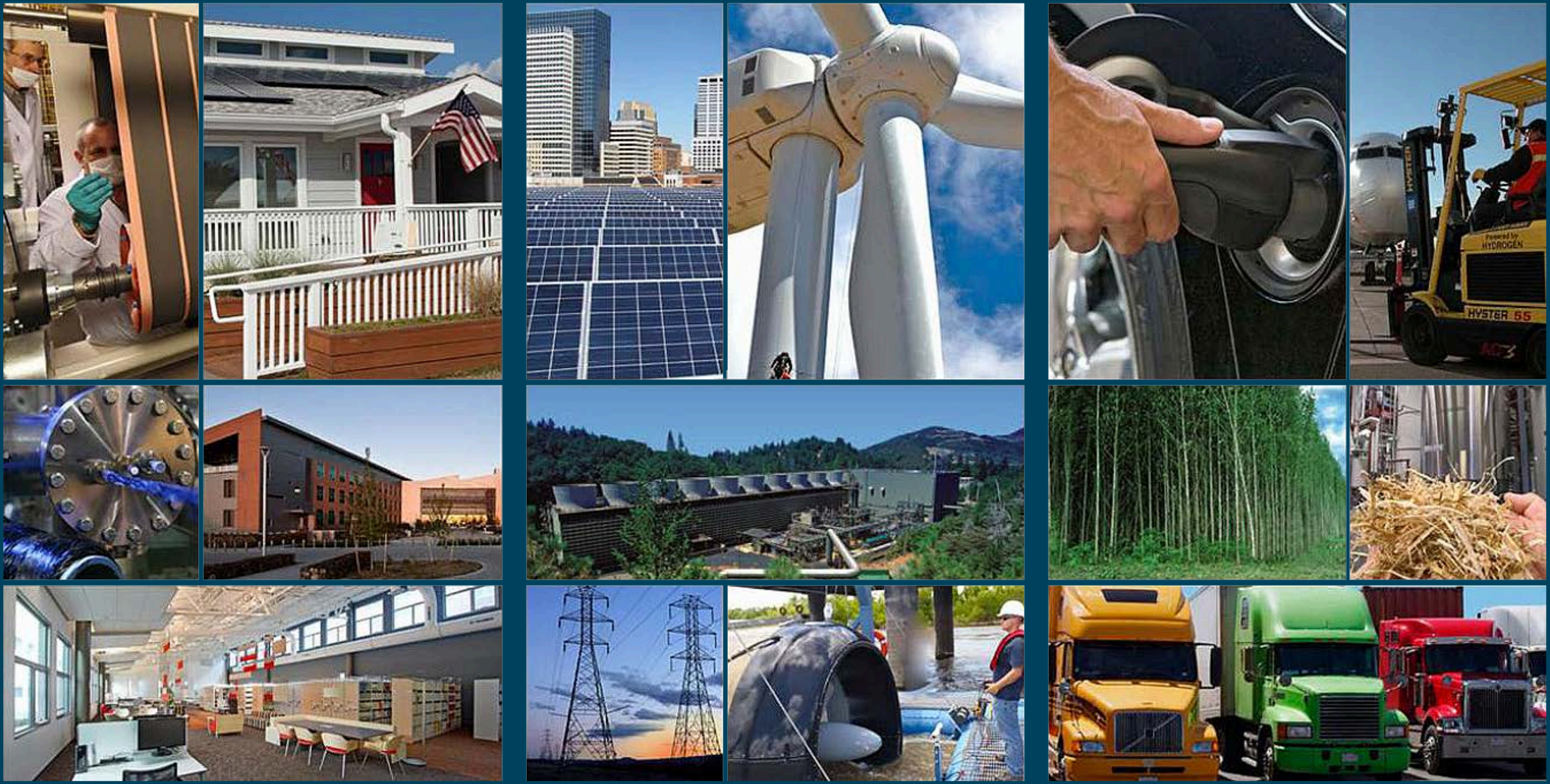
DOE/EERE Buildings Cybersecurity Project

Presentation to the Federal Facilities Council Workshop: Cyber Resilience of Building Control Systems, Nov. 17, 2015



U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy

Joseph Hagerman
Senior Policy Advisor
Building Technologies Office

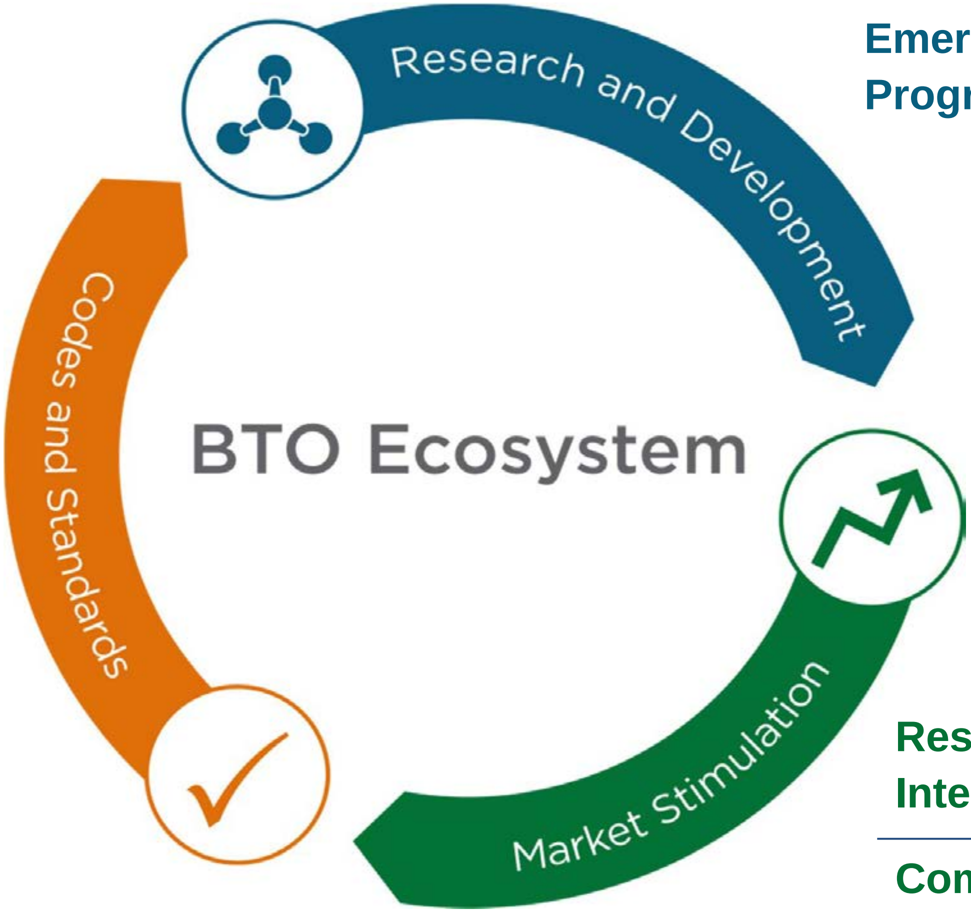
DOE/EERE: Building Technologies Office

Tech-to-Market → Speed Adoption → Scale Savings

Emerging Technologies Program

Building Energy Codes Program

Appliance Standards Program



Residential Buildings Integration Program

Commercial Buildings Integration Program

The energy savings potential in homes and buildings is 50%.

U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy

PNNL and Cybersecurity

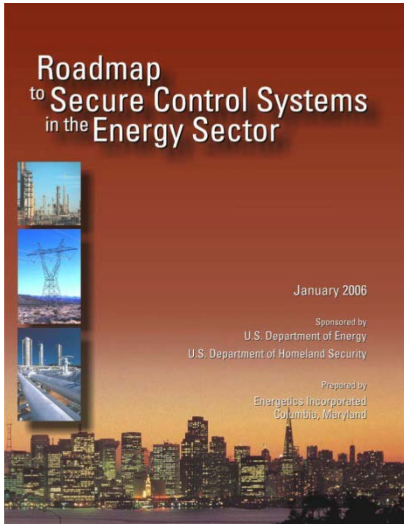
Extensive capability and experience protecting cyber infrastructure.

- More than 300 hundred scientists, engineers, computing and software professionals engaged in the field
- Since the 1990's, have deployed solutions for DOE, DHS, DoD and other agencies
- PNNL work includes
  - Cyber-physical vulnerability assessments
  - Development of new analytic methods for threat prediction, detection and defense
  - Forensic analysis
  - Development of component security solutions
  - Outreach to key commercial sectors (classified and non-classified)

PNNL recognized leader in cyber-physical systems and cyber-security for both utility sector and other critical facilities (as well as for other agencies' needs).

PNNL Cybersecurity Support to DOE's Office of Electricity

Vulnerability Assessment & Research Roadmap



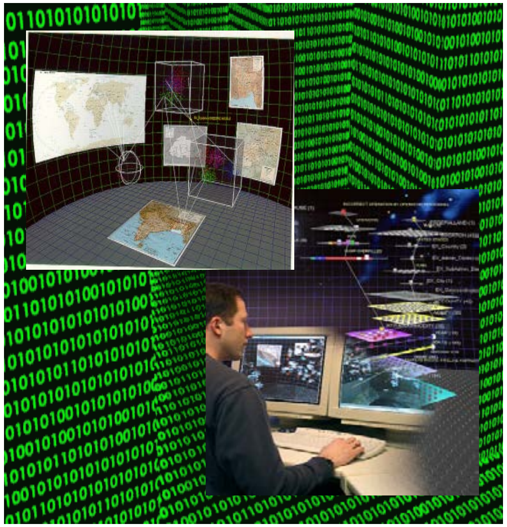
Roadmap to Secure Control Systems in the Energy Sector

January 2006

Sponsored by
U.S. Department of Energy
U.S. Department of Homeland Security

Prepared by
Energetics Incorporated
Columbia, Maryland

Threat Prediction, Detection, Early Warning



Component Solution Research, Development & Deployment

Electricity Subsector—Cybersecurity Capability Maturity Model

Established as a result of the Administration's efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the energy sector.

www.whitehouse.gov/blog/2012/01/09/protecting-nation-s-electric-grid-cyber-threats

BTO-FEMP project builds on extensive cybersecurity completed by DOE, PNNL and other national labs focusing energy systems and infrastructure. However, this is one of the first buildings cybersecurity projects for DOE.   We're using previous work as a benchmark – let's not reinvent the wheel!

“Smart” Buildings Present New Opportunities and Challenges

- **Buildings have a large role** in helping to enhance grid reliability and enabling rapid integration of renewable energy and storage.

BUT

- **Buildings today limited** by existing controls systems that can’t easily transact at speed or scale required by grid
  - High cost to “get it right” with existing technology and economics
  - Currently only implemented in large buildings w/ building automation systems
  - Components emerging with greater capabilities of control
  - Cyber-security is a looming issue

- **Building solutions must “think across the meter”**
  - Energy Efficiency is at the core, but are additional value streams to/from 3rd party entrepreneurs
  - Better load control has other benefits

- **Cyber solutions for buildings also need to be “Smart” as the threat is complex and rapidly evolving**
  - Cyber-physical security threats to buildings are complex, non-linear and rapidly evolving as cyber and physical systems converge and connectivity increases in our buildings and critical infrastructures (CI).
  - Therefore, DOE is examining cybersecurity threats to smart, connected buildings equipment to mitigate any threats to realizing the significant energy, economic and efficiency opportunity.

Scaling Transaction Based Controls

Vision

- Buildings operating at optimum energy efficiency over their lifetimes, interoperating effectively with the electric power grid.
- Buildings that are self-configuring, self-commissioning, self-learning, self-diagnosing, self-healing, and self-transacting to enable continuous optimal performance.
- Lower overall building operating costs and higher asset valuation.

http://energy.gov/eere/buildings/downloads/buildings-grid-technical-opportunities-introduction-and-vision

Mission

- Work with the market to develop and deploy cost effective solutions to building owners/operators, service providers, and manufacturers to manage energy consuming assets more easily and efficiently (38 quads of primary energy).

- Utilizing these solutions, enable optimum building energy efficiency and performance, renewable generation with reduced utility investments, and standardized financial transactions for across the meter opportunities

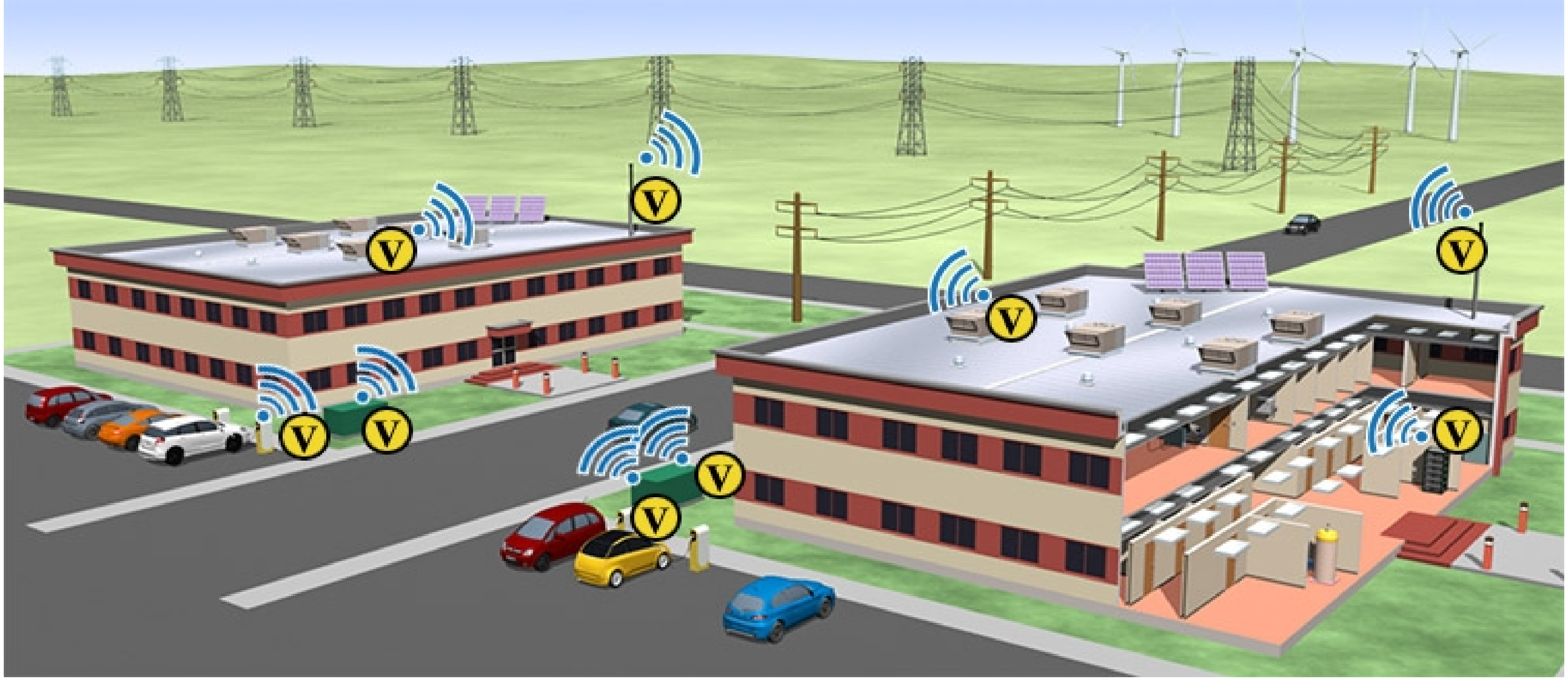
Research, Development and Deployment

Develop and commercialize advanced diagnostics and controls to create self-aware buildings that optimize performance.

Define, test, quantify and validate the value proposition, response and related services provided by Building Technologies

Enable buildings to interact (e.g. with the grid) to support transactive energy opportunities and deliver the value proposition

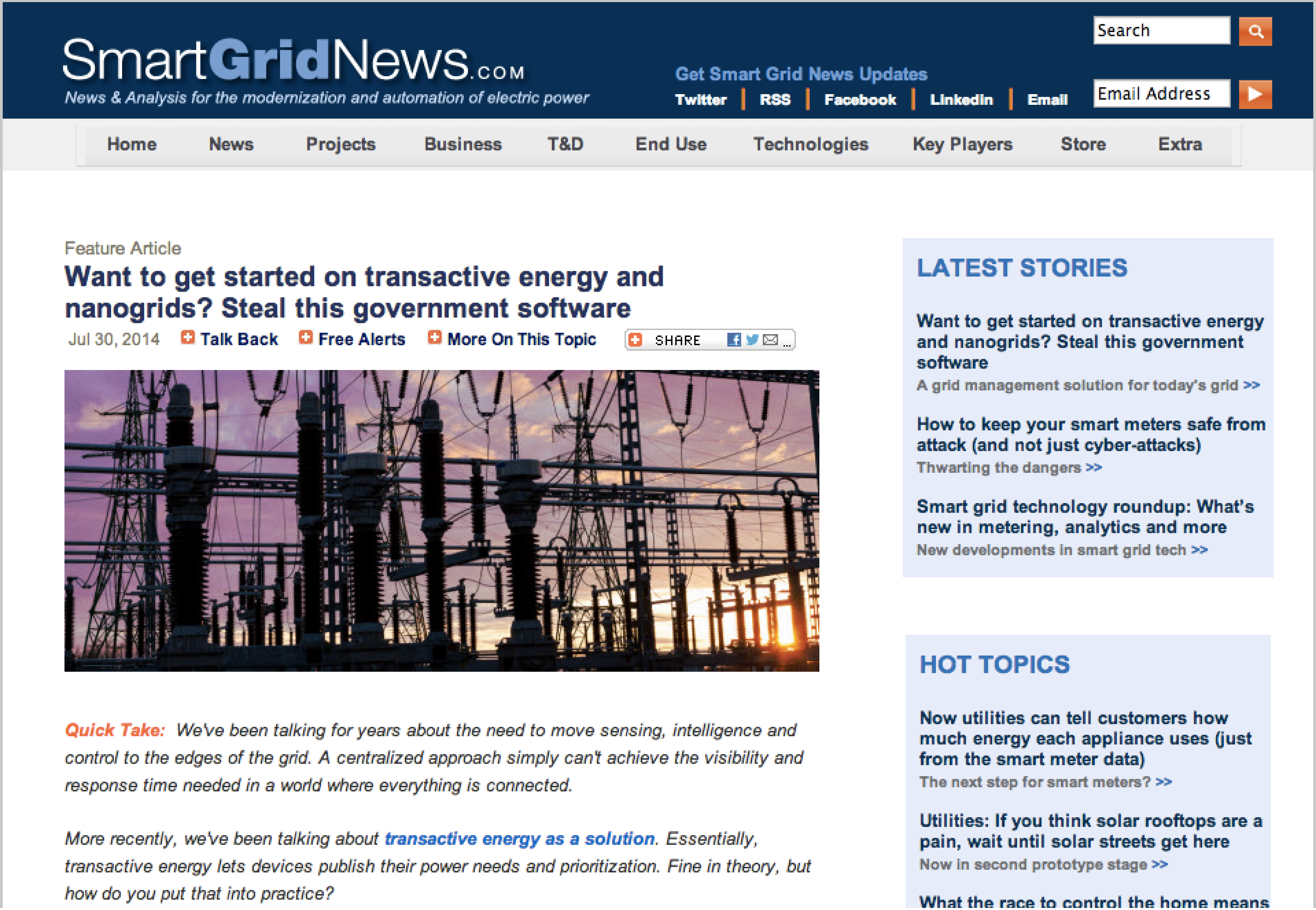
EERE Supporting Development Of Controls Platform



VOLTTRON is **an application platform** (e.g., Android, iOS) for distributed sensing/control applications. Attributes include:

- Open-source, flexible, modular and scalable
- **Built in features to streamline app developmen**t
- **Secure communication** (e.g., security libraries/cryptography)
- Platform services

For More Information:
http://transactionalnetwork.pnnl.gov/volttron.stm and volttron@pnnl.gov



SmartGridNews.com
News & Analysis for the modernization and automation of electric power

Get Smart Grid News Updates
Twitter | RSS | Facebook | LinkedIn | Email

Search
Email Address

Home News Projects Business T&D End Use Technologies Key Players Store Extra

Feature Article

Want to get started on transactive energy and nanogrids? Steal this government software

Jul 30, 2014 Talk Back Free Alerts More On This Topic SHARE

Quick Take: We've been talking for years about the need to move sensing, intelligence and control to the edges of the grid. A centralized approach simply can't achieve the visibility and response time needed in a world where everything is connected.

*More recently, we've been talking about **transactive energy as a solution**. Essentially, transactive energy lets devices publish their power needs and prioritization. Fine in theory, but how do you put that into practice?*

LATEST STORIES

Want to get started on transactive energy and nanogrids? Steal this government software
A grid management solution for today's grid >>

How to keep your smart meters safe from attack (and not just cyber-attacks)
Thwarting the dangers >>

Smart grid technology roundup: What's new in metering, analytics and more
New developments in smart grid tech >>

HOT TOPICS

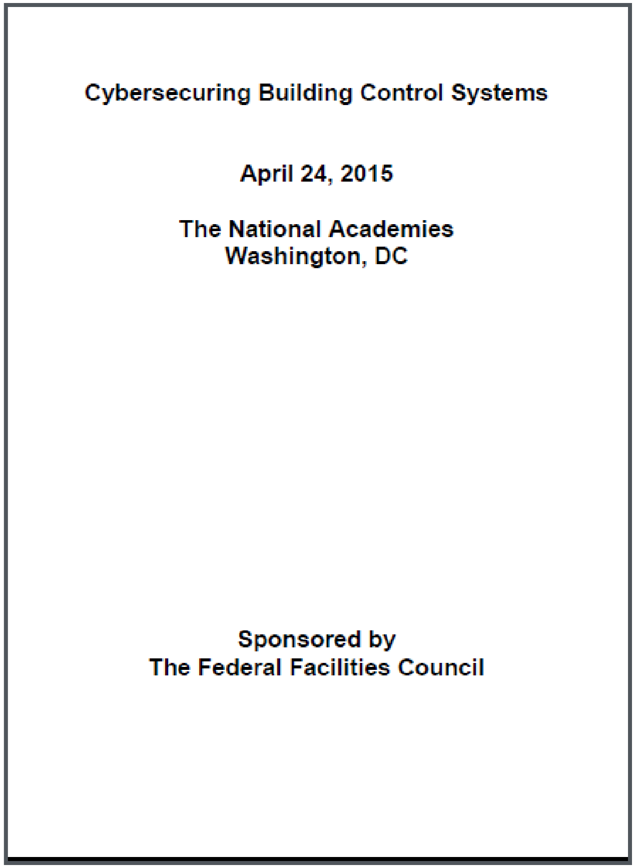
Now utilities can tell customers how much energy each appliance uses (just from the smart meter data)
The next step for smart meters? >>

Utilities: If you think solar rooftops are a pain, wait until solar streets get here
Now in second prototype stage >>

What the race to control the home means

http://www.smartgridnews.com/story/want-get-started-transactive-energy-and-nanogrids-steal-government-software/2014-07-29

National Academies Identifies “Connected = Vulnerable”



Cybersecuring Building Control Systems

April 24, 2015

The National Academies
Washington, DC

Sponsored by
The Federal Facilities Council

“**The nation's buildings are increasingly relying on building control systems with embedded communications technology and many enabled via the Internet**. These systems provide critical services that allow a building to meet the functional and operational needs of building occupants, but they can also be easy targets for hackers and people with malicious intent. These facilities contain building and access control systems such as heating, ventilation, and air conditioning; electronic card readers…that are increasingly being automated and connected to other information systems or networks and the Internet. **As these systems are becoming more connected, so is their vulnerability to potential cyber-attacks.”**

EERE approach:

1. **convene industry** and Federal agencies to define problem in complex space of connected devices and buildings
2. **develop simple tool** for variety of building types to measure potential cybersecurity awareness and readiness

DOE-EERE Project Goals

- **Assess relevancy of the Energy Sector Cybersecurity Capability Maturity Model (ES-C2M2)** developed for utilities to building owners/operators and the vendor supply chain
  - ES-C2M2 refined and launched by DOE Office of Electricity.
  - Today, ES-C2M2 is de-facto benchmarking tool used by utility sector
- **Develop white paper** on cyber-physical threats to buildings and facilities.
- **Adapt ES-C2M2** through defining steps with industry to create a Buildings-C2M2.
- **Vet the Buildings-C2M2** approach through pilot tests, partners, outreach

B-C2M2 is a first of its kind cybersecurity tool developed in corporation with diverse buildings stakeholders to measure buildings maturity in response to emerging cyber and physical threats.

B-C2M2 provides a high level view of cybersecurity situational awareness and risk focusing on ten critical cyber domains, whereas CSET and GrassMarlin focus more on specific threats and vulnerabilities.

Together, these suite of tools can provide a more holistic cyber security posture for our nation’s most critical cyber-physical buildings assets.

Buildings-C2M2 is not an end solution – using it does not make you secure. It is a measuring tool for executives, operators, and industry professionals

101: Introduction to Maturity Models

What is a “maturity model” and why do we need them?

- Many “clients” have trouble explaining what is exactly wrong and what they want done – **discussing symptoms not root causes.**
  - As a result, much of the burden of scoping a solution falls on others – unspecified by “client.”
  - There are number of diagnostic tools that consulting firms have created over the years to help identify problem areas (think… SWOT analysis, benchmarks, waterfalls, workshops and even simple check lists).
  - These tools are like the x-rays, thermometers, or blood tests used in a physical exam. It is not treatment, just diagnostics to find sickness.

- A common tool is the **maturity model** which gauges the client’s maturity in a number of areas and points out the areas of improvement.
  - Different functions / capabilities are shown on one axis and the different maturity levels are on the other axis.

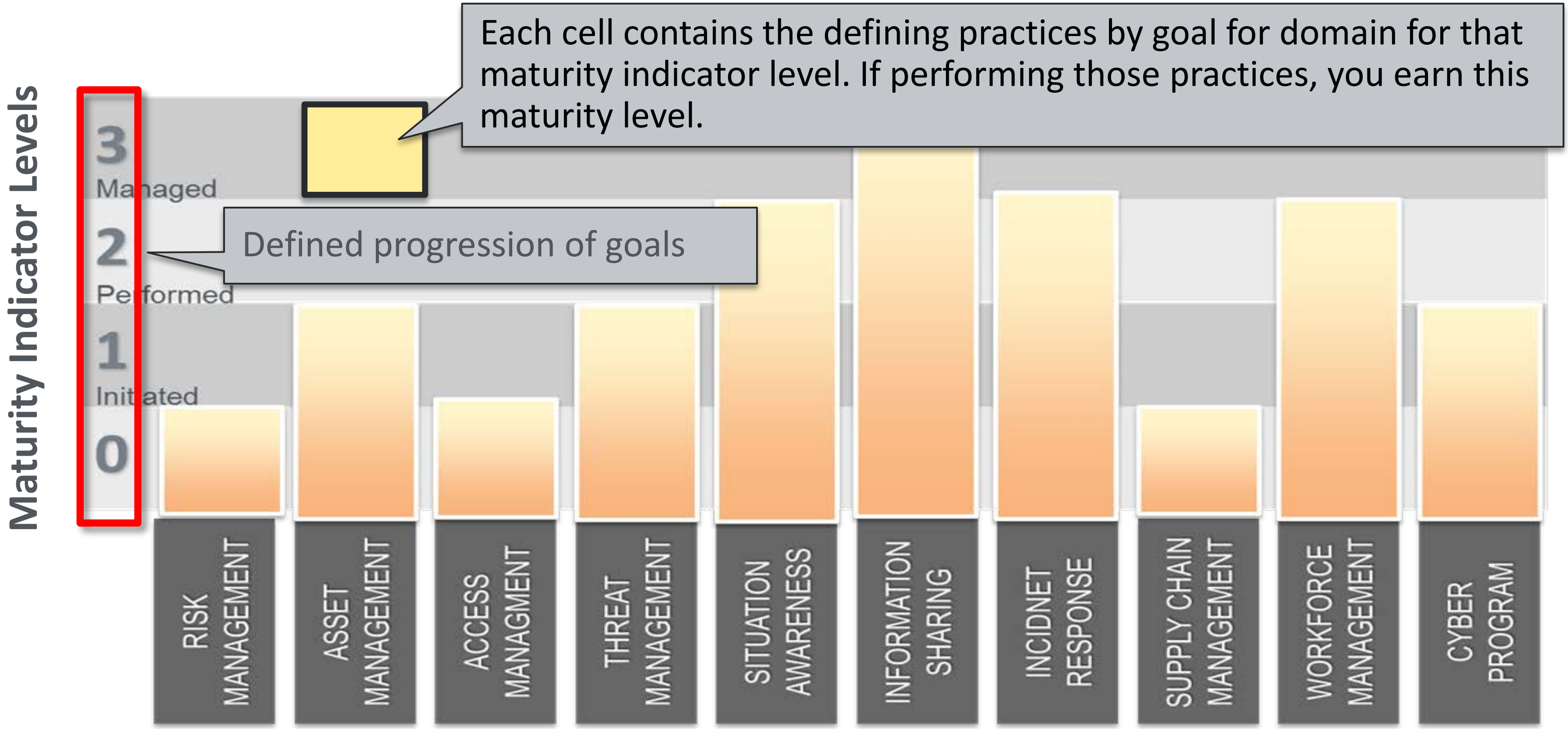
Case Study – Utility Sector:

Utility Challenge: Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid.

Approach: Develop self-evaluation survey and a maturity model to develop, measure, and track cybersecurity capabilities.

Results: A scalable, sector-specific model that provides an industry structure based on root causes and goals.

Evaluating Cybersecurity Maturity with Maturity Model



Each cell contains the defining practices by goal for domain for that maturity indicator level. If performing those practices, you earn this maturity level.

Defined progression of goals

- Example shows cybersecurity maturity levels plotted for each of C2M2's 10 security domains.
- High maturity level shown for "Information Sharing" while "Supply Chain Management" and other security domains have low maturity level.
- This may indicate that more attention should be placed on domains with low maturity.
- Alternatively, if cybersecurity risk is small, low maturity level may be perfectly acceptable from a cost-benefit perspective.

What is the C2M2?

C2M2…

- ✓ Measures the maturity of an organization’s cybersecurity capabilities
- ✓ Focuses on the programmatic structure
- ✓ Provides descriptive and flexible guidance
- ✓ Publicly available

C2M2 IS NOT…

- ✖ Guidance for implementing specific security controls
- ✖ An audit, controls assessment, or a penetration test.
- ✖ Intended to replace other cybersecurity-related activities, programs, processes, or approaches.

Lesson Learned from First Pilot

- 312 questions in **B-C2M2** (and all versions of C2M2) more than needed for a satisfactory building system assessment.
- May need **B-C2M2 "Lite"** that is streamlined and yet provides coverage of all security domains and major properties. This should require an hour for an assessment rather than the 6-10 hours for the full **B-C2M2**.
- **B-C2M2** assessment, though lengthy, provided useful information on cybersecurity program maturity for pilot building.

*Need to determine when **B-C2M2** answers need to focus on an organization's cybersecurity program for its network resources and when they need to focus only on their program for building control systems.*

DOE Project Status

- ✓ **Assessed relevancy** of the C2M2 to building system owners/operators and their supply chain.
- ✓ **Developed draft white paper** on cyber-physical threats to buildings
  - o **If you are interested in reviewing, please let us know.**
- ✓ **Adapted the C2M2 into a building system version,**“B-C2M2”.
- ✓ **Conducted an initial pilot test** of the B-C2M2 in PNNL building
- □ **Conduct additional pilot testing** of other Federal agency buildings.
  - o **If you are interested in pilot testing, please let us know.**
- □ **Fine-tune the B-C2M2 tools** based on the entire set of pilot testing.
  - o **If you are interested in helping us fine-tune, please let us know.**
- □ **Prepare to roll out the B-C2M2 tools** for operational use.

DOE-EERE highly values stakeholder input in tool development.
Your participation would be very helpful to us!

How to Contact Us

DOE

- Joe Hagerman, Project Manager
  joseph.hagerman@ee.doe.gov

PNNL Project Team

- Andrew Nicholls, Project Manager ak.nicholls@pnnl.gov
  703/789-3964
- Cliff Glantz, B-C2M2 cliff.glantz@pnnl.gov
  509/375-2166
- Michael Mylrea, Cybersecurity michael.mylrea@pnnl.gov
  509/375-2496

Thank You.

U.S. DEPARTMENT OF ENERGY | Energy Efficiency & Renewable Energy