



## Mr. Jeffrey Johnson

The objective of my pilot project is to integrate the existing industrial control systems that are in nearly every commercial or military facility that has been built in the last 25 years. These systems include a wide variety of disparate systems and an equally wide variety of cyber protection measures. Our challenge is how

---

---

*A native of Orange County, Virginia, Mr. Jeffrey M. Johnson graduated from the Virginia Military Institute with a B.S. degree in civil engineering in 1980. Commissioned in 1980, Mr. Johnson served 8 years as an Engineer Officer in the U.S. Army Reserve. Mr. Johnson served as head of the Operations and Maintenance Division of several Public Works Departments. During his tenure with Naval Surface Warfare Center Dahlgren Public Works, he also led the Facilities Maintenance Engineering Division and served as Deputy Public Works Officer. He led the effort to deploy and modernize the use of direct digital control systems and enterprise asset management systems to improve the efficiency of facilities management operations at Dahlgren and to reduce energy consumption at the base. Mr. Johnson is currently the Regional Command Information Officer (N6) for the Naval District of Washington. He supports the Anti-Terrorism Force Protection (ATFP) program as an ad hoc member of the Systems Engineering Integrated Product Team and is the Commander Naval Installations Command (CNIC) government representative for Shore Wireless Networking. He has piloted several projects for the ATFP program, including the Virtual Perimeter Monitoring System (VPMS), which is composed of secure wireless networks, video management, and video analytics systems. He also leads for the CNIC SmartGrid Pilot project at Naval Support Activity South Potomac, which leverages the VPMS network components and includes secure middleware panels and software to bring disparate direct digital controls and supervisory control and data acquisition systems into a common, secure, and accredited architecture. He is considered a shore sensor systems expert.*

---

---

can we leverage the existing infrastructure, integrate it onto our cyber secure network that we use for public safety systems, and deploy those systems to enable our facilities commanders to operate and run them from a command and control perspective.

- Metering (AMI and legacy)
  - Centralized & Integrated Reporting for the Comprehensive Utilities Information Tracking System (CIRCUITS) (billing and reporting)
  - Direct Digital Controls (DDC)
  - SCADA
  - Facilities Management Systems
  - Geographic Information Systems
- } Legacy Industrial Control Systems (ICS)

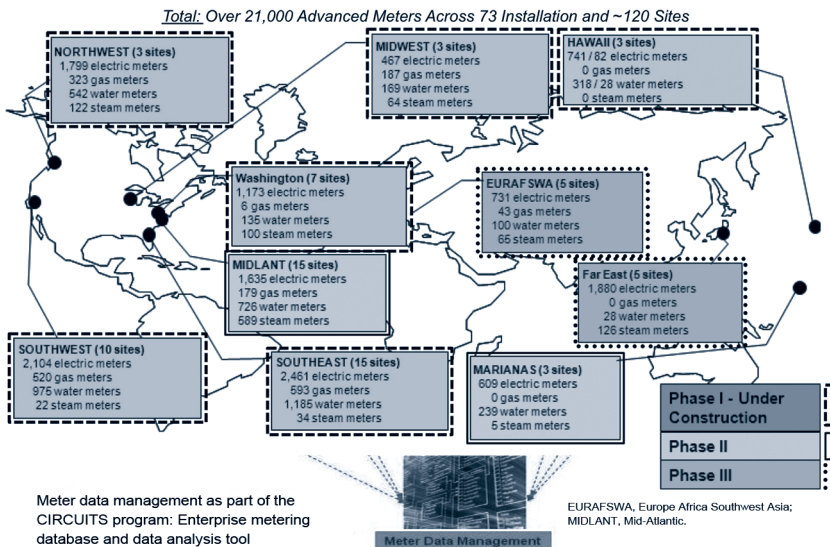
**Secure integration of systems to provide transparency**  
Enabling Command and Control, Emergency and Security Management, Data Management, and Energy Management

**Figure 1. Discover, Certify, Accredite, Connect**

As illustrated in Figure 1, our first challenge is basically a challenge of discovery. The Navy Facilities Command (NAVFAC) has been working to discover the existing systems that are in use in our facilities and infrastructure at the same time that we are deploying the advanced meters that are now legally mandated. By providing precise monitoring, these meters will greatly improve our ability to see how our facilities are using energy. We also want to identify the supervisory control and data acquisition (SCADA) systems that are used to operate such plant systems as water, wastewater, electrical distribution, and natural gas. Once we have integrated those systems into our network, our next challenge will be to integrate them with our facility management systems so we can take advantage of the sensor data for other purposes. Lastly, we intend to then integrate in a graphical environment so that we can display the data geospatially, because a lot of us work better with pictures than we do with words.

The Advanced Meter Initiative (AMI) is a Navy-wide initiative to deploy advanced electrical meters on Navy facilities around

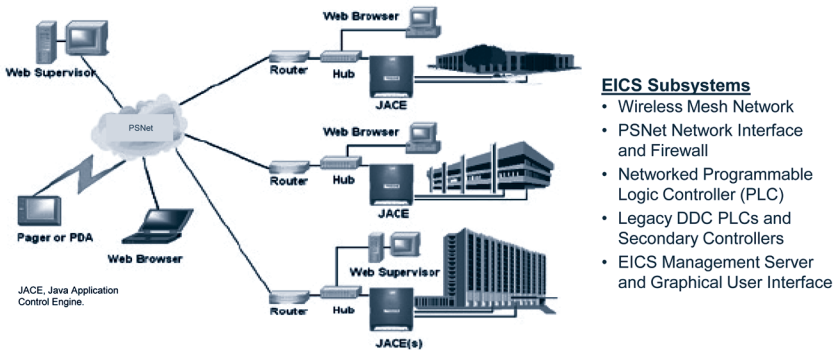
the world. The dashed boxes in Figure 2 indicate the regions that have already been awarded and have meter installations currently underway. The solid boxes identify locations where we hope to deploy meters this fiscal year subject to funding, while the dotted boxes show locations where we hope to deploy next year. All of these meter systems are being deployed on our foundational cyber secure network that we call the PSNet. The meters connect to a server infrastructure that we call the Meter Data Management System. That system allows us to collect the meter data and then interface with our billing systems in NAVFAC and with the systems that our customers use to monitor their own energy use.



**Figure 2. Advanced Metering Initiative Programs**

The pilot project that we have is related to integration of these various control systems (Figure 3). The issue of cyber security for industrial control systems has been in the news a lot recently; a great many people are concerned about it. So we have a big challenge in how to take all these different systems, integrate them on a network, and make them secure enough that we can take advantage of the systems without having to replace them. Our approach is to use a middleware architecture that involves installing a new

industrial control system middleware panel. That panel then is firewalled to add an extra layer of network security. We are also deploying new servers to then read that panel. The architecture that we are using will communicate with the legacy protocols for the multitude of different control systems that exist across the Navy and pull them into a common framework. In addition, it will be able to communicate in modern protocols. As NAVFAC deploys new facilities, they are using new construction specifications that require the system to communicate with modern protocols. Accordingly, the system we are deploying is a foundational system that integrates older technology that is noncompliant and cannot communicate in a modern language with that newer technology.



**Mission**

- Develop a centralized energy monitoring capability that integrates DDC and SCADA systems in support of Region Energy Reduction Initiatives
- Develop an EICS model scalable for Navy enterprise-wide deployment

**Capabilities**

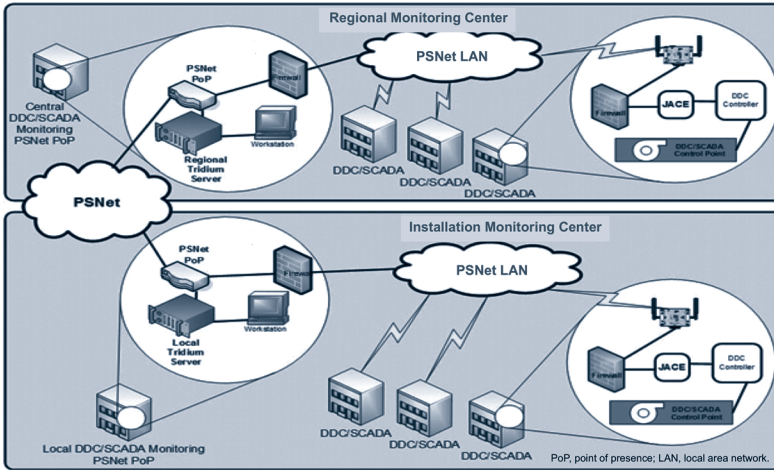
- Integrated EICS solutions
- Critical Infrastructure Monitoring using the Virtual Perimeter Monitoring System (VPMS)

**Figure 3. Enterprise Industrial Controls Systems (EICS)**

Given the meter locations and the state of our networks, particularly on the industrial controls and utility systems side, we are leveraging wireless networking to reduce the cost of our deployment and to provide connectivity for our mobile workforce. We are also focusing on meeting cyber-security requirements and satisfying DoD and Navy mandates for wireless networking (Figure 4).

From a command and control perspective, we fully intend to respect the chain of command. Accordingly, at the installation

level, we are establishing command centers, and we are establishing the ability for the installations to operate their facilities and their infrastructure. At the same time, we are taking advantage of the Navy's strong regional approach. Thus, we have command and control at the installation level and we have visibility at the regional level (Figure 4). This tiered approach relies on a web-based architecture to accomplish that mission.



**Figure 4. Secure ICS Architecture**

Given the wide variety of control systems that we are interfacing with, we have developed a regional screen template so that the command centers at all the bases will have the same look and feel. They will use the same monitoring screens to display the data in a graphical format. We will have standardization and centralization of data so that we can interface with our business systems while retaining decentralized command and control.

As part of the industrial control systems that we are deploying, we will also be able to collect alarm and event data that can be used to trigger our work management activities. This alarm data basically is deployed at the installation level; however, a regional alarm server rolls all that data up into one regional framework.