

LESSONS ON SMART GRID INTEGRATION WITH FACILITY SECURITY, CONDITION MONITORING, AND CONTROL

Keywords: "Smart Grid", Facility Security, Condition Monitoring, Remote Control, Energy management, Intelligent Energy Consumption

Submitted By:



Thurston Brooks and Benga Erinle

9715 Key West Ave
Suite 500
Rockville, MD 20850
301-670-6779

14 October, 2010

ABSTRACT

Smart Grid concepts have been applied to DoD infrastructure in the implementation of an Enterprise Industrial Controls System (EICS) which provides Navy organizations the ability to monitor and control areas for potential hazards, intrusions, as well as, effective and efficient management of facility energy utilities. Through automation, infrastructure readiness has been increased while reducing costs by eliminating personnel-intensive monitoring and control tasks. This has been accomplished by implementing real-time sensor network connectivity for ashore infrastructures with intelligent energy consumption through the integration of existing multi-vendor Supervisory Control and Data Acquisition / Direct Digital Control (SCADA/DDC) systems into a central monitoring capability. EICS facilitates improved collaboration between an Installation's command center, security forces, emergency responders, and facility managers. The integration of plant security and condition monitoring into a single EICS, incorporating video analytics technology with wireless video for intrusion detection and condition anomaly monitoring; centralized facility utility usage monitoring and control, and data fusion to support improved situational awareness from the Command Center, has resulted in a solution that leverages existing industrial-strength secure wireless and networking solutions. This paper describes the systems engineering perspective and modular design architecture that ensures secure real-time facilities/utilities control and supports collaboration among Command Center, security forces, and emergency responders under emergency conditions. The paper outlines a robust scalable system that is comprehensive and modular for intelligent energy consumption using commercial standards.

INTRODUCTION

Smart Grid concepts are being applied to DoD infrastructure in the implementation of an Enterprise Industrial Controls System (EICS) which provides Navy organizations the ability to monitor and control naval shore-based facilities, as well as, assure effective and efficient management of facility energy utilities. The U.S. Navy is implementing this program in a four part "Smart Grid" implementation effort consisting of 1) smart meters, 2) secure wireless networks for communication, 3) an Enterprise Industrial Controls System (EICS) for managing energy usage and demand response, and 4) recommissioning buildings to gain further savings. Through automation, infrastructure readiness has been increased while reducing costs by eliminating personnel-intensive monitoring and control tasks. The goal is to integrate the existing architecture, technologies and concepts established under previous efforts with new and more advanced technologies and concepts to extend current naval shore-based capabilities to include centralized direct control of sensors at the facility building level for critical infrastructure monitoring and facilities utility usage monitoring and control.

CONCEPT OF OPERATIONS

The EICS program provides Naval Installations and Facilities with a broad set of facility utilities monitoring and control capability, as well as, implements monitoring, communication and surveillance tools to support physical intrusion detection, chemical and radiological agent detection, and other asymmetric threats to base personnel and base infrastructure. The focus is on applying technologies to support the integration of building industrial controls and video monitoring of critical infrastructure elements to support "Green IT", Advanced Metering Infrastructure (AMI), and general energy conservation goals and initiatives of the Commander, Navy Installations Command / Naval Facilities Engineering Command (CNIC/NAVFAC). This is being accomplished through the insertion of new technologies including real-time wireless video image analysis, advanced sensors, wireless asset tracking for security and emergency response personnel, and augmenting those systems with integrated multi-vendor utility systems and Advanced Metering Infrastructure (AMI) within a Virtual Perimeter Monitoring System (VPMS™) architecture and the Navy's Public Safety Network (PSNet). The resulting EICS system is providing base commanders with effective capabilities to not only protect personnel and infrastructure, but monitor and control vital Navy Installation Critical Infrastructure. Many of the capabilities will be physically portable and use wireless data transmission. As a result, the technologies will be capable of monitoring for areas that often have been too difficult or costly to monitor.

The EICS efforts integrate and manage the confluence of the data from the various monitoring and surveillance sensors with all the end users of the information as seen in Figure 1 below. The information can be wirelessly transmitted to a fixed central command center, to a mobile command center, to a temporary command center, or point-to-point response teams (responding individuals in the field).

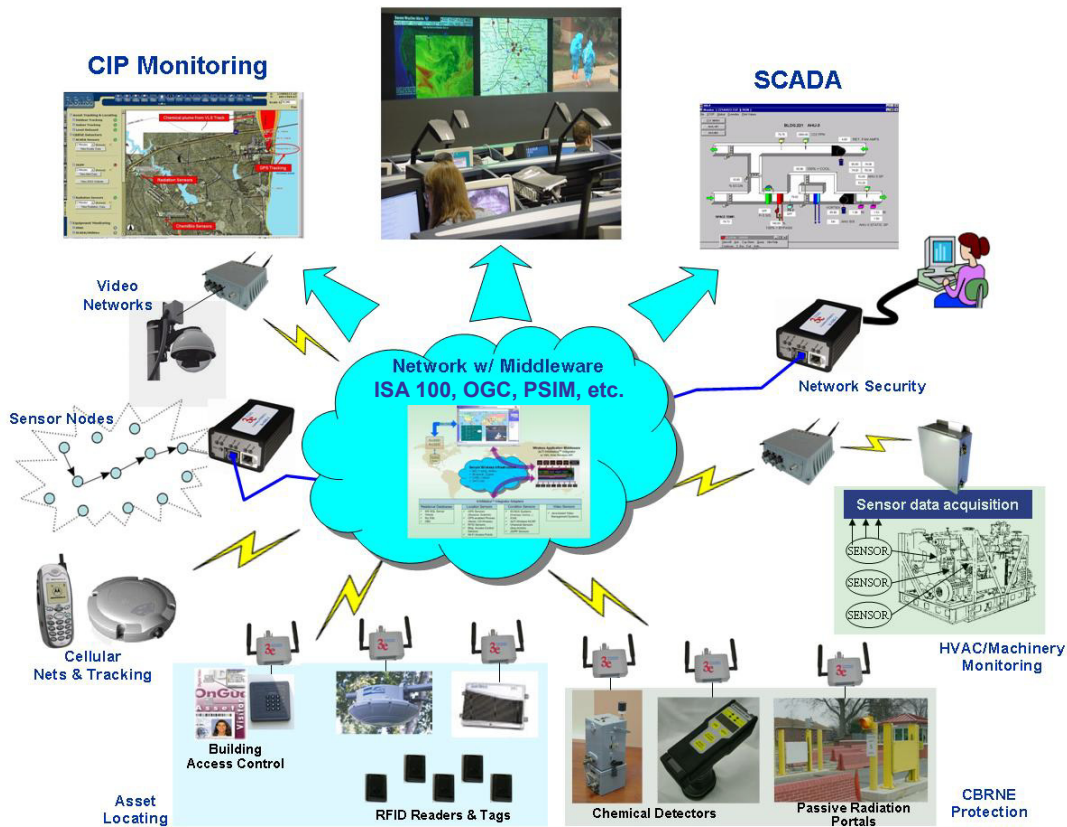


Figure 1: Critical Infrastructure Protection and Monitoring includes Smart Grid Concepts

OBJECTIVES AND BENEFITS OF EICS

The broad over arching objectives of EICS include:

- Improved naval base operations, critical infrastructure monitoring, and control of vital utilities and infrastructure at the building level.
- Expansion of perimeter monitoring capabilities installed at Naval Installations worldwide to enable support of Navy-wide energy consumption awareness and "Green IT" initiatives.
- Utilization of secure wireless meshed networks to support naval base operations, including industrial controls and video monitoring of critical infrastructure.
- Expansion of existing Naval facility utilities monitoring and controls capabilities by integrating disparate multi-vendor systems with an Advanced

Metering Infrastructure (AMI) capability to improve Demand Response operations and support recommissioning activities.

The EICS project will provide the following broad benefits:

- Provide ashore Navy organizations the ability to monitor critical areas.
- Increase infrastructure readiness and reduce costs by eliminating security monitoring tasks and efforts that may be automated.
- Provide a decision support system that will optimize the use of force protection assets.
- Implement real-time sensor network connectivity for ashore infrastructure.
- Facilitate real-time collaboration among Command Center, security forces, and emergency response providers.
- Extend the navy's capability to include use of existing wired and wireless video systems for critical infrastructure monitoring.
- Extend the navy's capability through the integration of existing Supervisory Control and Data Acquisition / Direct Digital Control (SCADA/DDC) systems into a central monitoring capability.
- Provide a single scalable support system that is comprehensive and modular.

SYSTEM CONCEPT

EICS will extend and integrate existing building utility monitoring and management systems, including legacy devices in multiple locations and from a wide range of manufacturers, to securely operate over a single network. EICS will use a wide variety of advanced sensors to detect conditions. Sensor data transmission will be done wirelessly to provide rapidly reconfigurable monitoring of permanent installations and mobile monitoring for portable applications and temporary bases. Computerized discrete image analysis of video, thermal and IR images will be used to detect intrusions, as well as, other anomalies such as fires. Advanced data fusion techniques will be combined with innovative Human Machine Interface (HMI) displays to promote situational awareness to command and surveillance personnel.

HMI displays will be tailored for use with a wide range of computers and consoles used for command centers or large command and control facilities. Additionally, through the wireless mesh networks, laptops or tablet PC's can be employed by mobile applications and Smartphones or PDA's can be used for individual observers or roving guards/lookouts/watch

standers. Wireless asset tracking using advanced Global Position Systems (GPS) and GIS technologies will help keep a fix on essential personnel and mobile assets wherever they may be allowing command center personnel and roving personnel to locate key assets such as emergency response vehicles, rapid response counter intrusion teams, key command personnel, or roving guard/lookout/watch stander personnel at any time.

As shown in Figure 2, networked monitoring allows real-time alarm and activity monitoring and real-time demand response and usage. Facility graphical layouts identify / locate points of entry, exit and alarms, provide unique alarm point instructions and provide comprehensive reporting with searchable historical data and exportable results.

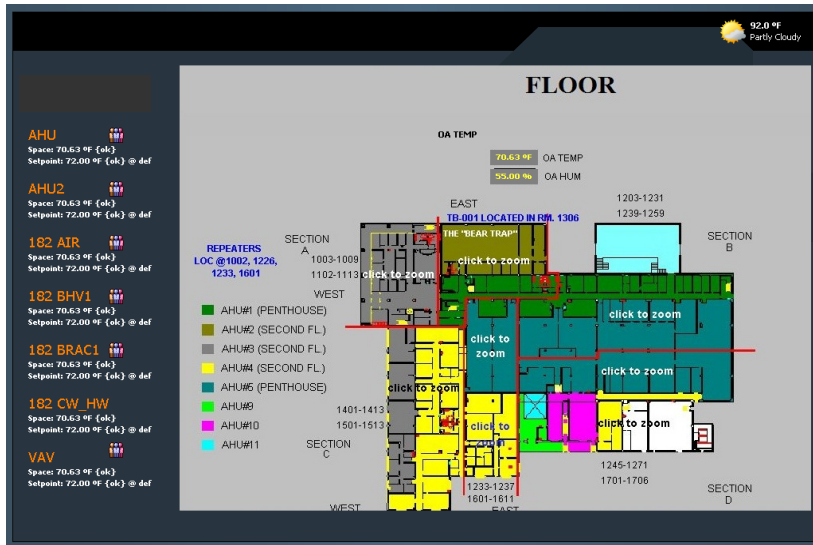


Figure 2: Sample of EICS GUI Interface for Facility Management

EICS not only provides for increased security and safety of base personnel and assets, but it facilitates optimal manning concepts by supporting monitoring control automation,

maintenance automation and industrial control and monitoring of utilities, power consumption, HVAC systems, etc, facility-wide at the building level.

For permanent facilities, sensor data can be used to provide awareness of network and facility conditions. For example, detection of a Chemical or Radiological threats could lead to of shutdown facility ventilation systems to prevent spread of contamination or detected problems with the electrical power distribution system could result in automatic reconfiguration of the base power supplies, including startup of emergency generators as necessary.

SYSTEM ARCHITECTURE

EICS will employ a distributed infrastructure complete with real-time sensor systems and open architecture displayed in Figure 3. The open architecture will support a “plug and play” mode where application modules (e.g. Threat Assessment, Intrusion Detection, Camera Surveillance, Maintenance Forecasting, Etc.) are inserted into the common operating environment. Open systems offer the greatest scalability and expandability to adjust to changing requirements. Open systems also facilitate the integration of OEM developed applications. A Graphical User Interface (GUI) provides a “windows” style user interaction using “wizards” for ease in entering/accessing information and “point and click” functionality to minimize keystroke entry. The EICS network includes distributed client/server systems that are fault tolerant and readily accessible via Web technology.

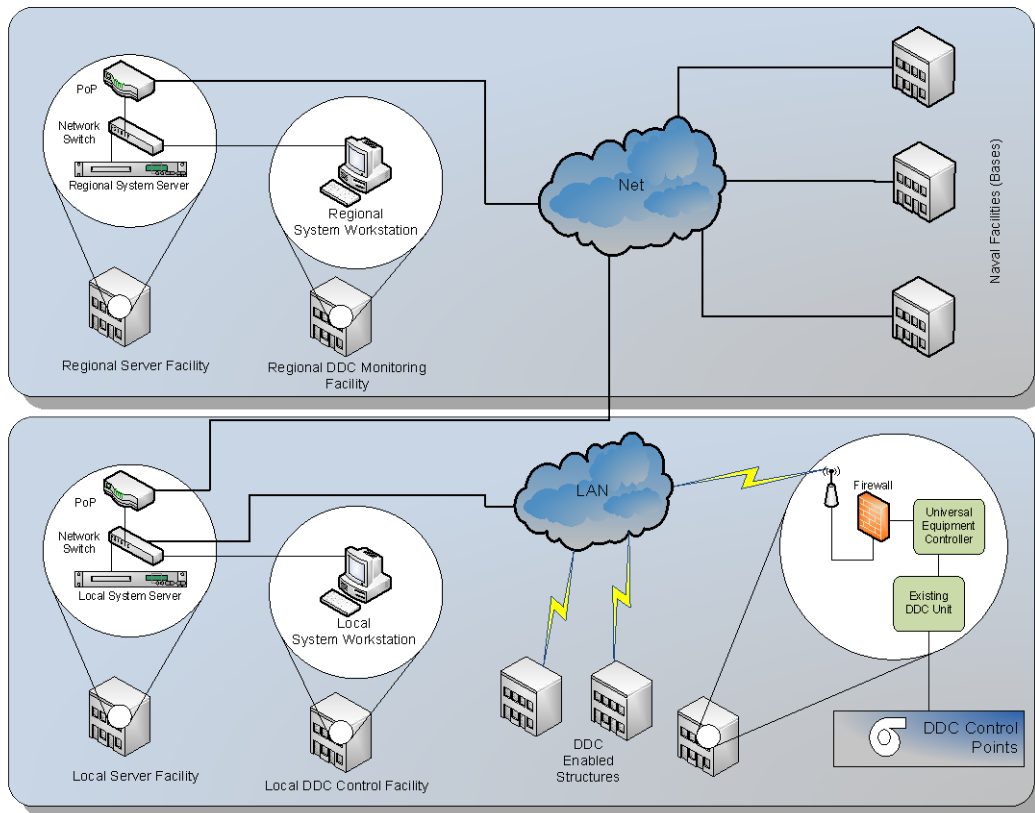


Figure 3: EICS Conceptual Architecture

Web-based Graphical User Interfaces will provide improved interactive access to distributed systems and enable access to:

- Environmental sensors such as temperature, HVAC status, etc
- Equipment and infrastructure condition monitoring sensors
- SCADA/DDC data
- Perimeter protection sensors, as well as, surveillance cameras
- Remote secure communication devices
- System performance data

EICS employs web-based technologies integrated into embedded environments. As equipment controllers gain more intelligence, embedded web technology provides a common interface to operators and maintainers. Figure 4 shows a high-level physical configuration of a typical EICS installation.

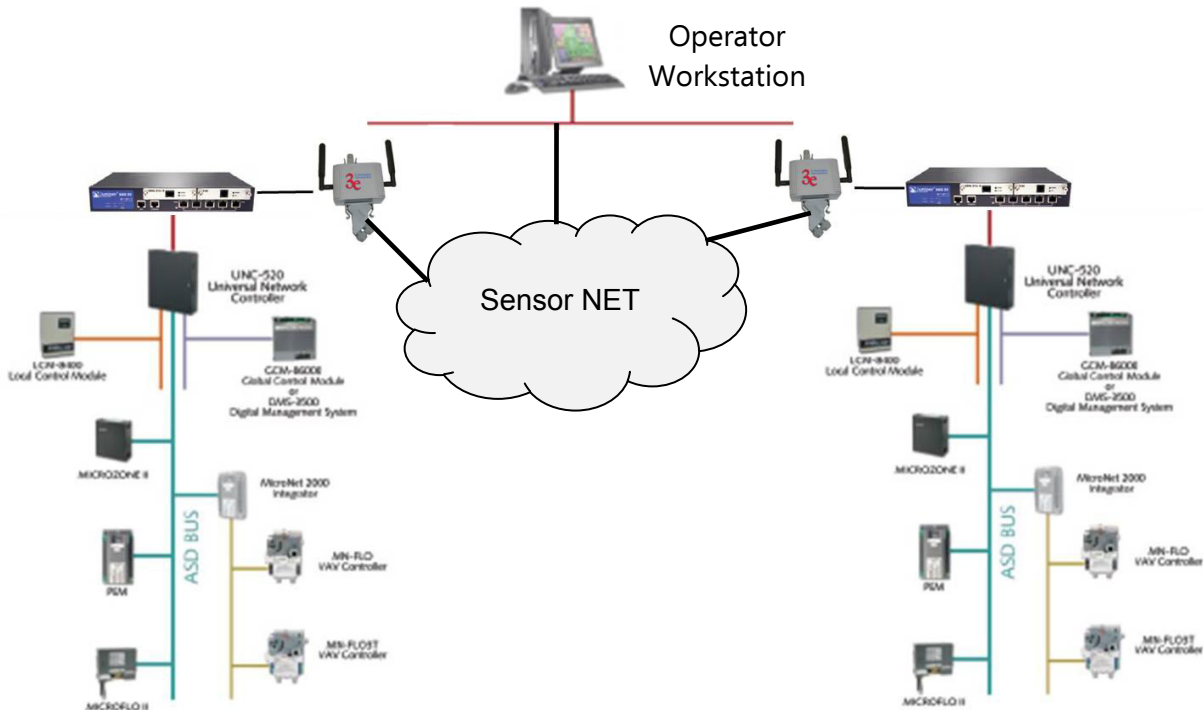


Figure 4: Example EICS Physical Configuration

The EICS will ultimately include many components/capabilities.

ADVANCED VIDEO ANALYTICS TECHNOLOGY

Video analytics technology applied to wireless video for intrusion detection, condition anomaly detection, and utility system monitoring. Computer software watches video streams to determine activities, events or behaviors that might be considered suspicious and provide an appropriate response when such actions occur. This is done by teaching machines to understand what they “see” through a camera. Traditionally, computer vision has had limited success in real-world commercial applications, but recent advances in technology and computational power have allowed video analytics to come out of the lab and into commercial video surveillance products. This technology analyses video imagery and determines motion relative to pre-defined rules overlaid on the scene. The theory being that motion in the direction or of the type specified in pre-defined rules are of interest to operators.

ADVANCED WIRELESS MESHED SENSORS

To assist the Navy in realizing significant improvements, EICS employs advanced wireless sensors as part of the EICS for use in system monitoring, environmental monitoring, damage assessment, and virtual instrumentation. Secure Wireless Networks with mesh networking that

complies with the requirements of DoDD 8100.1 Information Assurance (IA) and DODD 8100.2E "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)". EICS will sensorize infrastructure systems for system and equipment monitoring and will use a wide variety of sensors to create a network for intrusion surveillance and monitoring.

The sensors will be networked using topologies such as point to point, star, mesh, and star/mesh combination to optimize detection probability and sensor fault tolerance. The goal is to provide a redundant and fault tolerant sensor network.

In many cases, sensors will be used to trigger alarms and will turn on additional surveillance devices, such as cameras. A variety of trigger management techniques will be used such as individual triggers, sequential triggers, sectored triggers, sleep period/wake period triggers, and auto logging type triggers. Triggered alarms will result in a wide variety of notifications from simple alarms on a command center console, alarms on watch stander's portable client device, or other local actions such as audible alarms, visual alarms, spot/flood lights, or IR/Strobe lights.

For a fixed base-wide application, there will be many assets collecting data to monitor infrastructure conditions in addition to the intrusion and threat detection sensors. All data collected via the sensor network will be fed through to a desired location to be analyzed by the command center and installed middleware. This software will manage the data collection and be responsible for providing the appropriate alarm or notification.

DATA FUSION FOR SITUATIONAL AWARENESS

One of the keys to successful infrastructure control and protection is to have effective presentation of sensor data to key personnel. Having roving maintenance data takers and/or security patrols stationed around a perimeter is manpower intensive. What is needed is an effective way to determine and graphically present information in a "situational awareness" context where the operator can ascertain the existing situation in real time. Some concepts include:

- Alarms or triggers for that alert the operator to a specific out-of-band condition or camera view.
- Graphic high level screen displays of areas, systems, or components color keyed to status.
- Detail graphic screen pages that drill down from the high level overviews to display sensor values, camera images, etc.

- Pop up windows to describe emerging warning or danger events, for example, an intrusion or threat detection.
- Hot buttons on the warning or danger event message windows to lead the operator to appropriate displays or detail graphic screens.

Simply bombarding the operator with raw sensor data is no more effective in promoting situational awareness than having the operator stare at a huge bank of video monitors. The technological innovation involved in this effort is taking the raw data readings from the variety of advanced wireless sensors and fusing that raw data into information that the operator can effectively absorb. This effort is followed by the development of Graphical User Interface (GUI) screens that communicate the information easily and concisely to the operator.

WIRELESS ASSET TRACKING

The remote camera monitoring, advanced sensors, and data fusion activities are all aimed towards providing a command center or dedicated dispatch center operators and response personnel (emergency response teams, security response teams, threat neutralization teams, Etc.) with accurate situational awareness as they respond to an incident. Sensor data and camera images are two legs in the tripod with the actual location of force/infrastructure protection assets as the third leg. Advanced concepts using GPS, wireless RFID sensors and other wireless asset tracking mechanism will be explored and implemented.

LESSONS LEARNED

Lesson 1: Intelligent energy consumption has measureable benefits through real-time sensor and control network connectivity.

The illustration below highlights savings associated with application of Smart Grid concepts (Figure 5). As shown, early results already indicate that increased application of DDC and SCADA control of facility lights, HVAC and equipment results in a decline in energy cost per square foot.

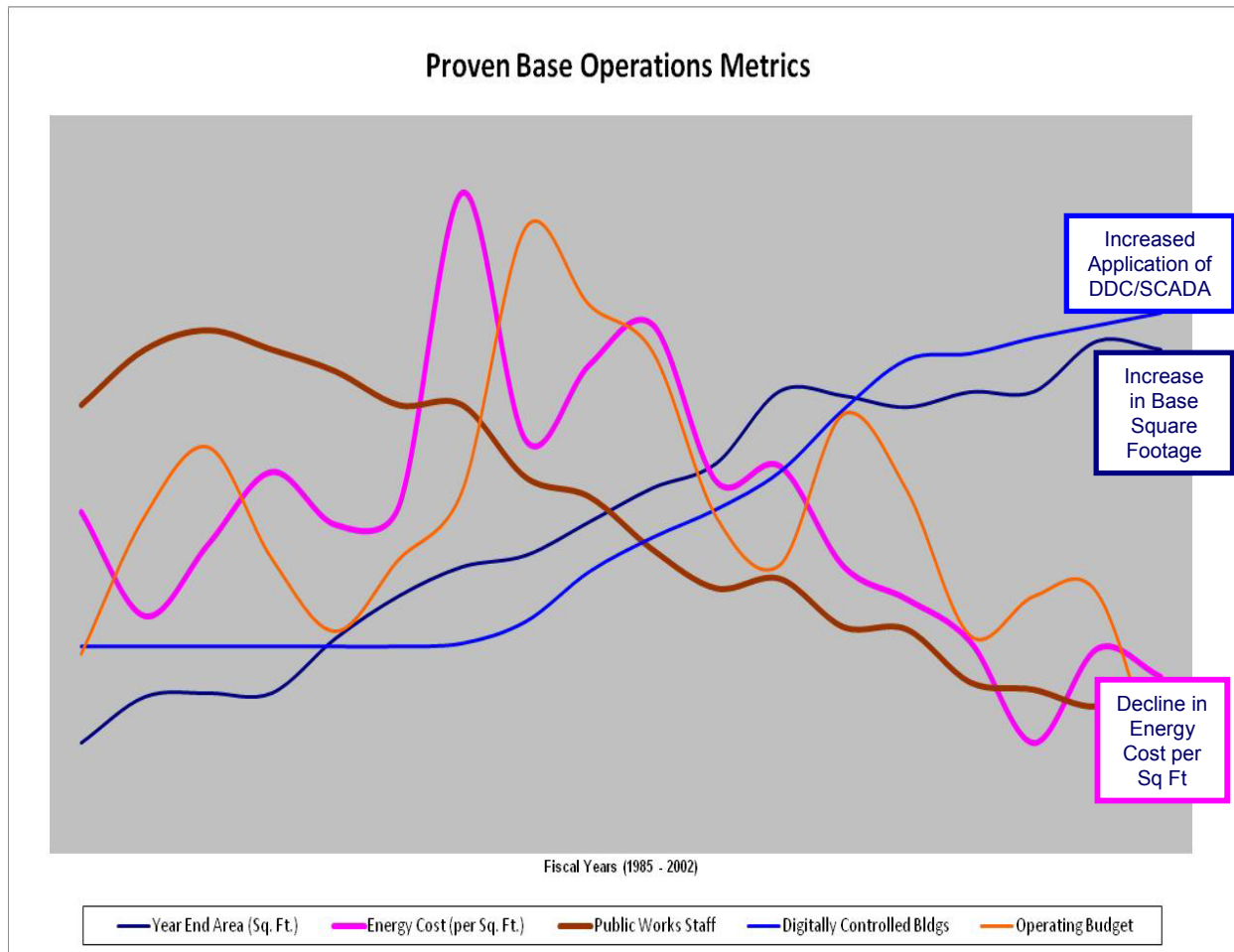


Figure 5: Results from Single Base over 15 Years

Lesson 2: Security must be built into the system architecture from the ground up.

The U.S. Navy has significant expertise in engineering, deploying, sustaining and securing its business systems. The subject matter expertise to support these activities is readily available. In addition, the expertise in assembling and supporting business systems for the U.S. Navy must follow the Information Assurance (IA) guidance the DOD and federal government have instituted. IP based systems must meet this guidance prior to being allowed to operate on a government network. Federal and DOD business systems typically operate on secured networks with equipment and processes in place to prevent external access and compromises. However, legacy commercial Industrial Control Systems (ICS) frequently do not include requisite Internet Protocol (IP) security enhancements. Many of the existing ICS devices utilize vendor proprietary communication protocols and typically only include limited IP capabilities. In addition, federal and DOD IA guidance are not applied to these systems in as rigorous a fashion as IP business systems. The Federal Government and DOD require IP business systems and networks to

comply with recurring system security scans, but such requirements are most often not extended to ICS systems. Most organizations are taking to implementing ICS and IP based systems in two separate domains with different maintenance and support practices since the skill sets supporting these systems are uniquely different.

Lesson 3: Through plug-n-play modularity a scalable smart system can be created with commercial-off-the-shelf components.

Integrating Navy ICS systems to Navy secured IP network is not an easy endeavor especially when there are literally thousands of ICS systems currently in operation in the U.S. Navy. To be effective and efficient in this activity, integrators will need to understand the customer's ICS, current business practices and develop unique implantation/engineering methodologies. A methodology alone does not guarantee effective and efficient implementation. Performing discovery and surveying of existing ICS within a facility can be a major effort. Whenever possible, friendly plug-n-play capability goes a long way toward reducing integration headaches and problems.

CONCLUSIONS

Expected payoffs from implementing EICS will include:

- Reduce utility usage and cost
- Improved information flow to mobile assets
- Increased situational awareness for Naval Command Center Personnel.
- Optimized manning for Naval Security Forces.
- Increased readiness
- Reduced Total Ownership Cost relative to Emergency Response capabilities.
- Increased safety of Naval Installations.