Navy and Marine Corps

Smart Grid

CAPABILITY DEVELOPMENT DOCUMENT

DISTRIBUTION STATEMENT A: Approved for public release.

INDUSTRY VERSION

SIGNATURE PAGE

PREFACE

The purpose of the Capability Development Document (CDD) is to establish a set of top-level requirements that both guide and bound the capability provided by the "Smart Grid".

_____ _____

APPROVED BY: RADM KATHERINE L. GREGORY Date
Commander, Naval Facilities Engineering Command

Executive Summary

Two major energy issues facing DoD today are the costs associated with facility energy consumption, representing 20-25%[1] of total DoD energy costs, and cyber vulnerabilities associated with energy infrastructure. Navy and Marine Corps Smart Grid will enable informed energy decisions resulting in significant reduction in energy costs, increase energy security, and provide cost-effective mitigation of cyber threats against Navy and Marine Corps facility infrastructure. Smart Grid capabilities will be applied across Navy and Marine Corps installations only when specific criteria can be achieved, (e.g. ROI, Operational Savings, and/or Security/Safety).

Smart Grid is a concept developed by the electrical industry and has been defined by the Institute of Electrical and Electronics Engineers (IEEE)[2] as *"…the integration of power, communications, and information technologies for an improved electric power infrastructure serving loads while providing for an ongoing evolution of end-use applications"*. SECNAVINST 4101.3 defines the meaning of Smart Grid as prescribed in the Energy Independence and Security Act of 2007 (EISA) that lists ten parallel activities referenced in Appendix G.

The Navy and Marine Corps have partnered to adapt the Smart Grid concept by expanding it to include all utilities production and distribution within Naval installations, and are leveraging this environment to produce enhanced benefits in support of the warfighter. Within the installation fence line the Navy and Marine Corps is both the utility company and the end user, providing increased opportunity for integration of the supply and demand sides of the energy value chain.

This document identifies capabilities of the Navy and Marine Corps Smart Grid (hereafter referred to as Smart Grid) that meet the following goals of the supported commands:

- **Reduce Cost**
- **Reduce Energy Consumption**
- **Support Mission Assurance**

Smart Grid encompasses the interconnected technologies and processes that enable the intelligent monitoring, forecasting, response to, and control of the Navy and Marine Corps' building and utility systems. Smart Grid relies upon a cyber-secure Command and Control (C2) information infrastructure for utility and building systems equipment and is a modernization and integration of utilities and energy Industrial Control Systems (ICS)

[1] *Department of Defense Annual Energy Management Report, Fiscal Year 2011*, Office of the Deputy Under Secretary of Defense (Installations and Environment), September 2012
[2] IEEE Std 2030™-2011 *Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Application, and Loads*

and associated infrastructure. Smart Grid integrates ICS data with a number of external Automated Information Systems (AIS) such as Centralized and Integrated Reporting for the Comprehensive Utilities Information Tracking System (CIRCUITS) (information flow is illustrated in Figure 1).

Smart Grid capabilities, identified in Section 1, and expanded in Section 6, are strategic to achieving improvements in facility and energy management that will:

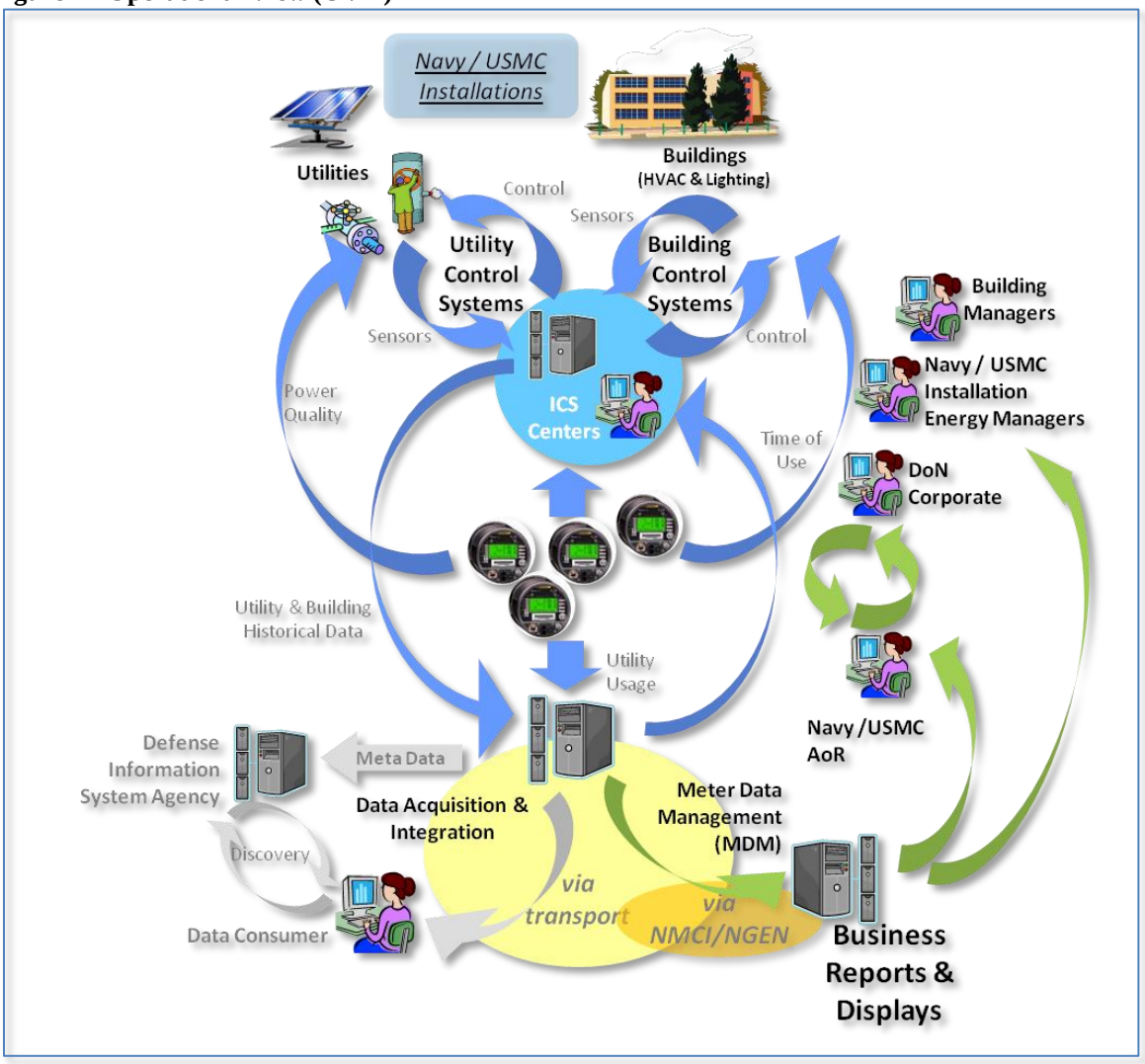
- Enable new business processes to reduce energy consumption, increase Operations and Maintenance (O&M) productivity, and provide an improved return on investment,
- Enable an agile capability to efficiently recognize and realize new energy conservation opportunities in real-time, and readily adopting new technologies and responding effectively to changing energy markets and regulatory environments,
- Provide the means to affordably address increasing cyber security threats.

The set of processes, organizational structures, projects and tools that are collectively used to operate Navy and Marine Corps ICS, rely on the integrated C2, information exchange and information processing provided by Smart Grid. Analysis of data is a key determinant for identifying appropriate actions in support of the Navy and Marine Corps overall energy management and consumption reduction objectives.

Navy and Marine Corps utility and building systems are vulnerable to cyber-attack with the potential for catastrophic consequences. Cyber security of Smart Grid is a critical concern. Ensuring cyber security and accreditation of utility and building control systems is a mandatory program requirement for all ICS assets. (See Section 6, Table 2, Net-Ready Key Performance Parameter (KPP) - IA Compliance). While application of Smart Grid operational capabilities will be driven by a return on investment, cyber security is not considered part of a cost vs. capabilities trade space.

The Capability Development Document (CDD) is a foundational component of an acquisition life cycle. While Smart Grid does not follow a formal DoDD 5000 lifecycle the CDD will be the first of a select set of DoDD 5000 products which will be used to guide the Smart Grid Program. See Appendix E – DoDD 5000 Program Lifecycle Products for a description of additional products that may be utilized.

Figure 1 - Operational View (OV-1)



The Operational View in Figure 1 *shows the core Smart Grid Building Control System (BCS) and Utility Control System (UCS) components, and the integration of information flow between them as blue arrows. Information leaving the Smart Grid is shown on the right, flowing via green arrows, to the business system and business users. The Smart Grid boundary is represented by the blue and green information flow lines and the devices and software that connect them. The grey lines flowing to the left illustrate the mechanism through which Smart Grid will take advantage of Defense Information Services Agency (DISA) defined interfaces with future and upgraded external Automated Information Systems (AIS).*

Revision History

Revision	Date	Name	Reason
0.1	2/15/13	Chester Braun	Initial document formation and input from Smart Grid Summit Team
0.2	2/18/13	Chester Braun	Editing and rearrangement of sections
0.3	2/20/13	Chester Braun	Edits, drawing updates
0.4	2/20/13	Chester Braun	Inputs from early section reviews
0.5	2/21/13	Chester Braun	Early review by DC-J, KW
0.6	2/22/13	Chester Braun	Draft ready for review
0.7	2/27/13	Chester Braun	PM review, Exec Summary rewrite, KPP edits.
0.8	2/27/13	Chester Braun	Reviewer's edits and comments. Exec Summary rewrite
0.8.1	3/1/13	Chester Braun	Formatting and table corrections
0.9	3/4/13	Chester Braun	Reviewer's edits, KW's comments, drawing normalization
0.9.1	3/7/13	Chester Braun	Remaining reviewer comments, drawing updates added text to various sections.
0.9.2	3/8/13	Chester Braun	Adjustments from OPNAV input, KW input
0.9.3	3/11/13	Chester Braun	Comments reviewed and edits added
0.9.4	3/12/13	Chester Braun	Final Draft for distribution
0.10	3/18/13	Chester Braun	Second review inputs, Sections 1 and 6 rework, input from OSD and OPNAV
1.0	9/3/13	Chester Braun	Final for signature with all reviewer input
1.0.1	2/20/14	Chester Braun	Fixed typos and broken references, changed ICS-P to ICS-PE, Updated Common Architecture Framework reference to v1.4

Table of Contents

Figures

Tables

Points of Contact

Name	Email	Phone	Function
Donna Carson-Jelley	donna.carson-jelley1@navy.mil	202-685-9338	Program Team Member
Chester Braun	chester.braun@navy.mil	619-532-1650	Program Team Member
Jeromy Range	Jeromy.range@usmc.mil	571-256-2839	Program Team Member

Purpose

The Capability Development Document (CDD) is the primary means of defining the authoritative, measurable, and testable capabilities that meet the needs of the supported commands. The CDD captures the information necessary to deliver an affordable and logistically supportable capability using mature technology within one or more increments of an acquisition strategy.

The CDD includes a description of the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF), policy impacts, and constraints. The CDD format is contained in CJCSI 3170.01H – Joint Capabilities Integration and Development System (JCIDS) and replaces the Operational Requirements Document (ORD) that was used under the old Requirements Generation System. Normally the CDD supports a Milestone B decision review when the capabilities are approved for production. Though Smart Grid does not follow a formal DoDD 5000 life cycle , many of the formal documents will be used as templates for Smart Grid program management.

Intended Audience

The Navy and Marine Corps Smart Grid CDD capture the goals of the supported commands and the Functional Capabilities that support those goals. It is used as a reference by the supported commands to ensure the Program is meeting their goals.

The CDD normally guides the Program through the Engineering and Manufacturing Development phase of a program's life cycle by defining measurable and testable high level capabilities. For Smart Grid, the CDD will guide organized integration of existing systems, interoperability, and development of ranges of enterprise solutions that will result in procurement and fielding of systems integrated into the Smart Grid.

1. Capability Discussion

The Smart Grid program will integrate existing utility and energy control systems via a common technology ICS Platform (ICS-PE) with robust defenses against cyber-attack. Data generated by these systems will be linked with business information systems to achieve an efficient System of Systems (SoS) [3] that empowers the organization with high quality and timely decision-enabling information. Smart Grid will enable operational capabilities such as Active Facility Management[4], improvements in identification of energy projects, meaningful and timely metrics, demand response, and safer, more reliable utility operation.

The Navy and Marine Corps have ICS, composed of thousands of Building Control Systems (BCS) providing environmental and lighting control, and Utility Control Systems (UCS) managing and monitoring electrical and mechanical utility production and distribution. BCS and UCS are, or will be, integrated by ICS Infrastructure (ICS-I), described in Section 1.3.1. Today many individual BCS or UCS function in a passive and disconnected "on" or "off" mode and do not fully account for internal and external factors such as maintenance issues, usage trends, emergencies, or changes in the cost of energy. Capability gaps, which differ in each Relevant Commander's Area of Authority (RCAoA), exist between current states and Smart Grid Initial Operating Capability (IOC) which is outlined in Section 12.1.

Identifying and closing each gap, across each RCAoA, represents an incremental opportunity toward achieving Smart Grid goals. Additional gains are expected as data availability gaps are successively closed, resulting in an increasingly complete and actionable view of the Navy and Marine Corps energy picture. Each RCAoA will be judged on a case by case basis for ROI and long term reduced operational costs. In some cases these results could influence the decision to avoid the investment and achieve energy reduction/savings without Smart Grid capability.

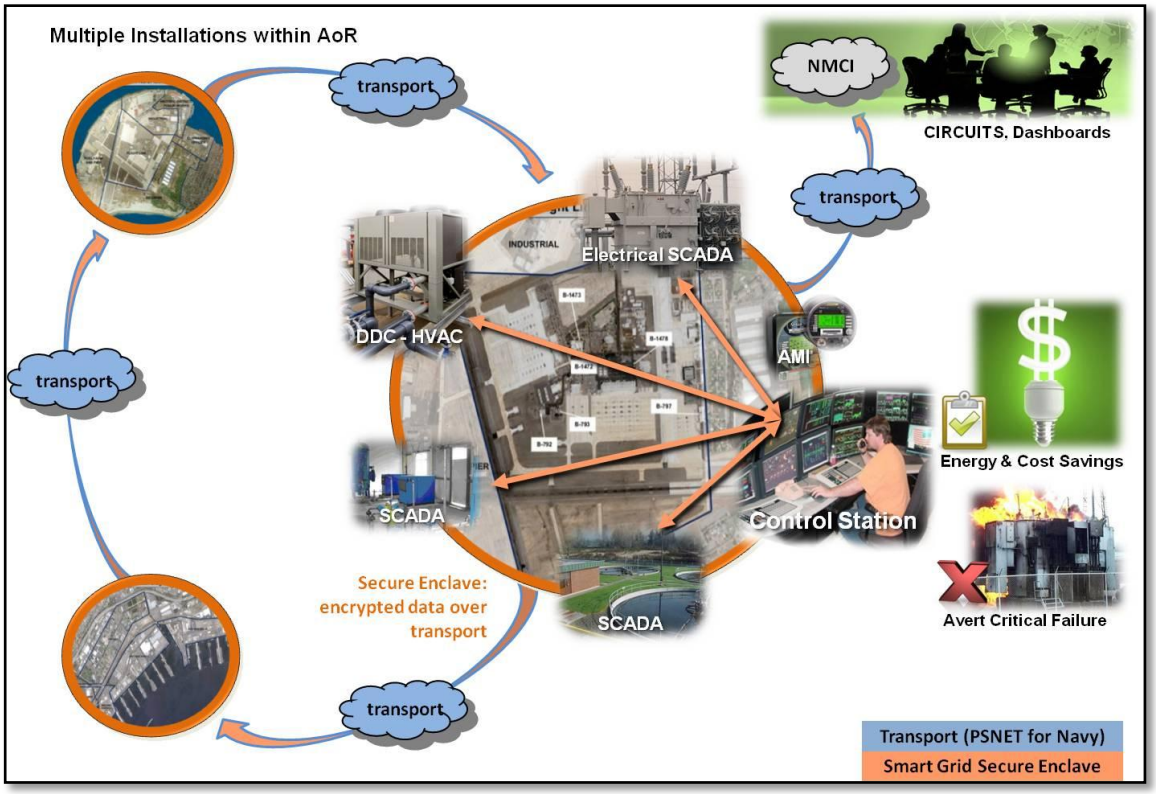
1.1 Functional Capabilities

The Smart Grid Vision is represented in Figure 2. The six functional capabilities are described in Sections 1.1.1 through 1.1.6 of this document. The KPPs and Key System Attributes (KSAs) are identified in Tables 1-3 of Section 6. Together, the functional capabilities, KPPs and KSAs allow Smart Grid to meet the goals of the supported commands, which include: reduce cost, reduce energy consumption and support mission assurance.

[3] The foundational engineering and architectural concepts in this CDD were developed in *A NAVFAC Industrial Controls Systems Common Architecture Framework*, v1.4 [9]. This document is key to a complete understanding of the Smart Grid CDD and concepts such as ICS-P and SoS. See Section 1.4 for discussion of SoS.

[4] Active Facility Management is networked control of Building Control Systems (BCS), including HVAC and lighting systems, to manage day/night setbacks, actively maintain comfort conditions to standards, proactively manage most efficient control schemes, monitor operations to ensure intended performance, identify maintenance needed to ensure functional performance (continuous commissioning), and support condition-based predictive maintenance.

Figure 2 – Smart Grid Vision



Each KPP, in column 1 of Tables 1 through 3, refers to one of the technical capabilities in Sections 1.1.1 through 1.1.6.

1.1.1 Integration of Historical/Near-Real-Time Data

Smart Grid will provide C2 for a portfolio of energy assets to which diversification of energy assets and C2 integration support mission assurance by improving both the reliability and quality of delivered utilities. Both historical and near-real-time (NRT) data will be integrated from an often heterogeneous collection of BCS and UCS across an RCAoA. This integration will provide interoperability for both monitoring and control functions (C2).

This integration is accomplished through an integration layer[5] placed in the bi-directional C2 data stream between UCS and BCS, the Human-Machine Interface (HMI)[6] and historical data servers.

From the IEEE Standard 2030-2011[7]: *"Smart Grid interoperability provides organizations the ability to communicate effectively and transfer meaningful data, even*

[5] The integration layer enables communication and management of data in distributed applications. In Smart Grid it enables communications and provides integration of data from disparate UCS and BCS.
[6] A combination of system operator displays and control input.

though they may be using a variety of different information systems over widely different infrastructures, sometimes across different geographic regions and cultures. Smart Grid interoperability is usually associated with the following:

- *Hardware/software components, systems, and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centered on (communication) protocols and the infrastructure needed for those protocols to operate.*
- *Data formats, where messages transferred by communication protocols need to have a well-defined syntax and encoding.*
- *Interoperability on the content level; a common understanding of the meaning of the content being exchanged."*

Four specific integration requirements address interoperability within the Smart Grid enclave[8], and between Smart Grid and external AIS.

a. Operational data transmission and storage capability within ICS
b. Data transmission to business systems and storage (e.g. NMCI)
c. ICS operational data analytics and display
d. Business data analytics and display

1.1.2 Export of Operational Technology (OT) Data to External AIS

OT data is exported to relevant external AIS in support of business goals. Operational historical data is integrated and staged within the ICS Platform enclave Demilitarized Zone[9] (DMZ) where it can be provided securely to external AIS with low risk to the operational systems.

1.1.3 Consistent and Scalable

Each implementation of Smart Grid shall be consistent and scalable with form, fit, and function to the RCAoA ICS Platform enclave.

A NAVFAC Industrial Controls Systems Common Architecture Framework[10] addresses the architectural boundaries within which each RCAoA must implement. This design space is meant to be wide enough to allow an RCAoA to expand consistent with its existing fielded devices and at the same time retain a commonality with the Enterprise. This design space and all systems fielded within it must still meet all applicable cyber security and Information Assurance (IA) requirements.

---

[7] IEEE Standard 2030-2011, Section 4.4 Smart Grid Interoperability

[8] DoDI 8580.1, E2.1.5.2, defines an 'enclave' as a *"…collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.*" It continues with: "*Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location.*"

[9] A DMZ provides a perimeter network that contains and exposes external-facing services to a larger untrusted network. The purpose is to add an additional layer of security to the private enclave by allowing only limited access between the private enclave and external systems and by buffering data transfers.

[10] Reference [9] in Appendix B. This document is foundational to understand the technical and architectural elements of Smart Grid and the discussions in this CDD.

1.1.4 Facilitate Demand Reduction and Response

This capability enables the C2 function to manage demand reduction and response operations based on variable supply conditions, respond to time-of-use pricing including the ability to pass price signal data on to consumers, and enable continuous commissioning processes where economically feasible.

1.1.5 Cyber Security Accreditation

All new and existing ICS must be resistant to cyber-attack, and as such be integrated into an accredited Platform IT risk approved state, and be maintained in that state. Any new UCS and BCS will be installed in accordance with Navy and Marine Corps IA policies, respectively, to ensure proper integration with an RCAoA's existing accreditation.

All Naval Facility Engineering Commands (FECs) and USMC installations are required to conduct an ICS inventory for Information Assurance accreditation hardware and software artifacts. This will serve as the baseline for determining accreditation gaps within RCAoAs, as well as serve to identify operational gaps.

1.1.6 Foundation for Advanced Capabilities

The Smart Grid will become the foundation for advanced capabilities that will provide additional benefits that support the goals of each supported command.

1.2 Capability Gaps

Existing ICS implementations have technical, operational, regulatory, administrative, and security capability gaps which must be addressed in order to achieve Smart Grid Initial Operating Capability (IOC) and Full Operational Capability (FOC). Solutions to these capability gaps need to account for unintended creation of new operational gaps, and ensure that, where conflicts are unavoidable, any such new gaps are resolved.

Figure 3 illustrates the baseline capability gaps between the majority of currently deployed ICS and Smart Grid IOC. Existing systems are illustrated at the bottom in the green area and the business community at the top in the yellow area. The existing gaps are spread between them in the grey area. White text indicates operational gaps and red text indicates cyber security and gaps in the management of the ICS enclave[11].

Two primary types of capability gaps have been identified that must be filled in order to reach IOC for Smart Grid in each RCAoA;

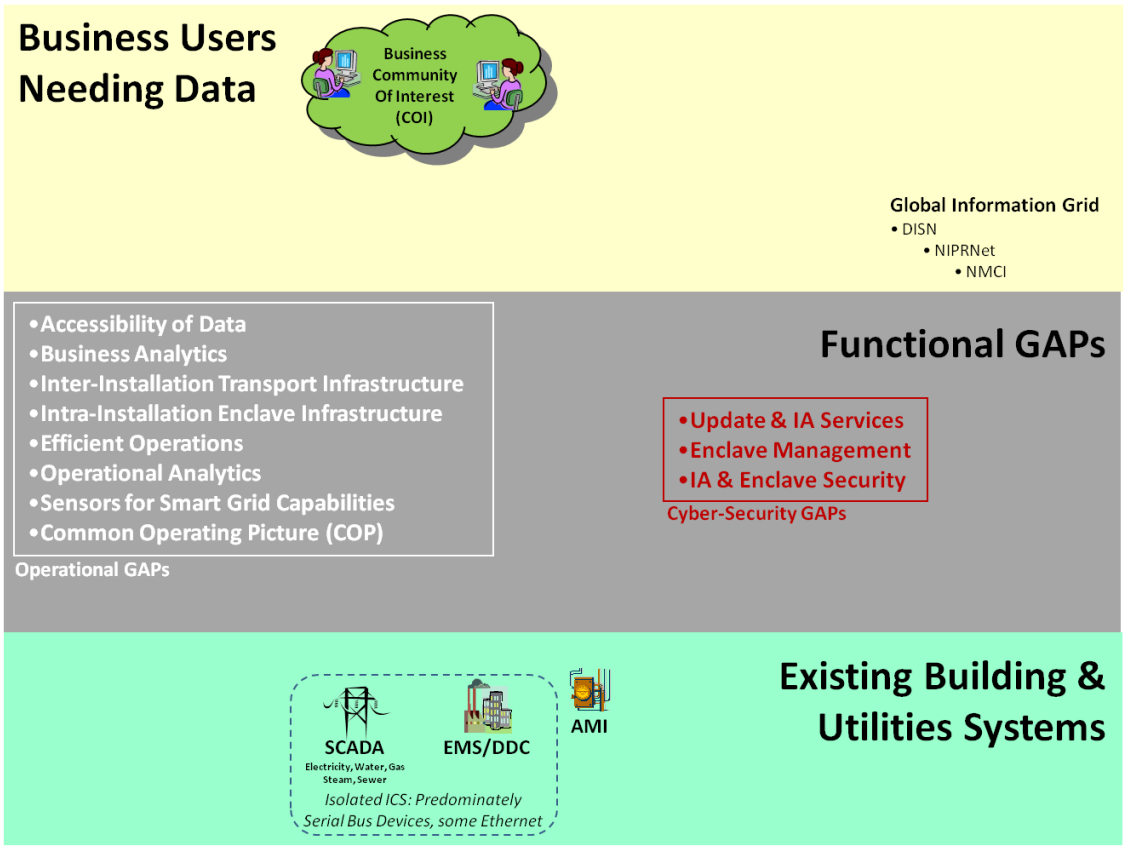
a) Baseline functional capability gap. The functional capability gap between existing system baselines and Smart Grid capabilities identified in Section 1 of this document. There is substantial variance in capability gaps between individual ICS sub-systems within an RCAoA and also between RCAoAs across the enterprise. A separate analysis will identify sensors required for active facility management.

[11] An enclave is defined as a set of information and processing capabilities that are protected as a group.

A gap analysis for each RCAoA will determine costs and help to set priorities for program planning.

b) IA accreditability gap. Though a capability gap, IA can often be a constraint in efficiently filling operational gaps. For example, IA accreditation will require curtailment of external vendor access and vendor laptops connected to a government network.

Figure 3 - Baseline Capability Gap



Existing systems, which will make up Smart Grid, are in a widely different state of capability, functionality, repair, and cyber security from base to base and region to region. The systems are numerous and predominately isolated. Figure 3 represents the 'gaps' that must be filled in order to build historical data bases of building operation that enable the expected benefits from an integrated and consistent ICS build-out. These benefits include; continuous commissioning[12], optimized system performance, and more efficient response to facility condition changes and emergencies by engineers and technicians.

[12] The Microsoft *Energy-Smart Buildings* whitepaper estimates that benefits from a normal five year retro-commissioning cycle can be realized in as little as a one year cycle with continuous commissioning.

1.2.1 Current Increment - Smart Grid IOC

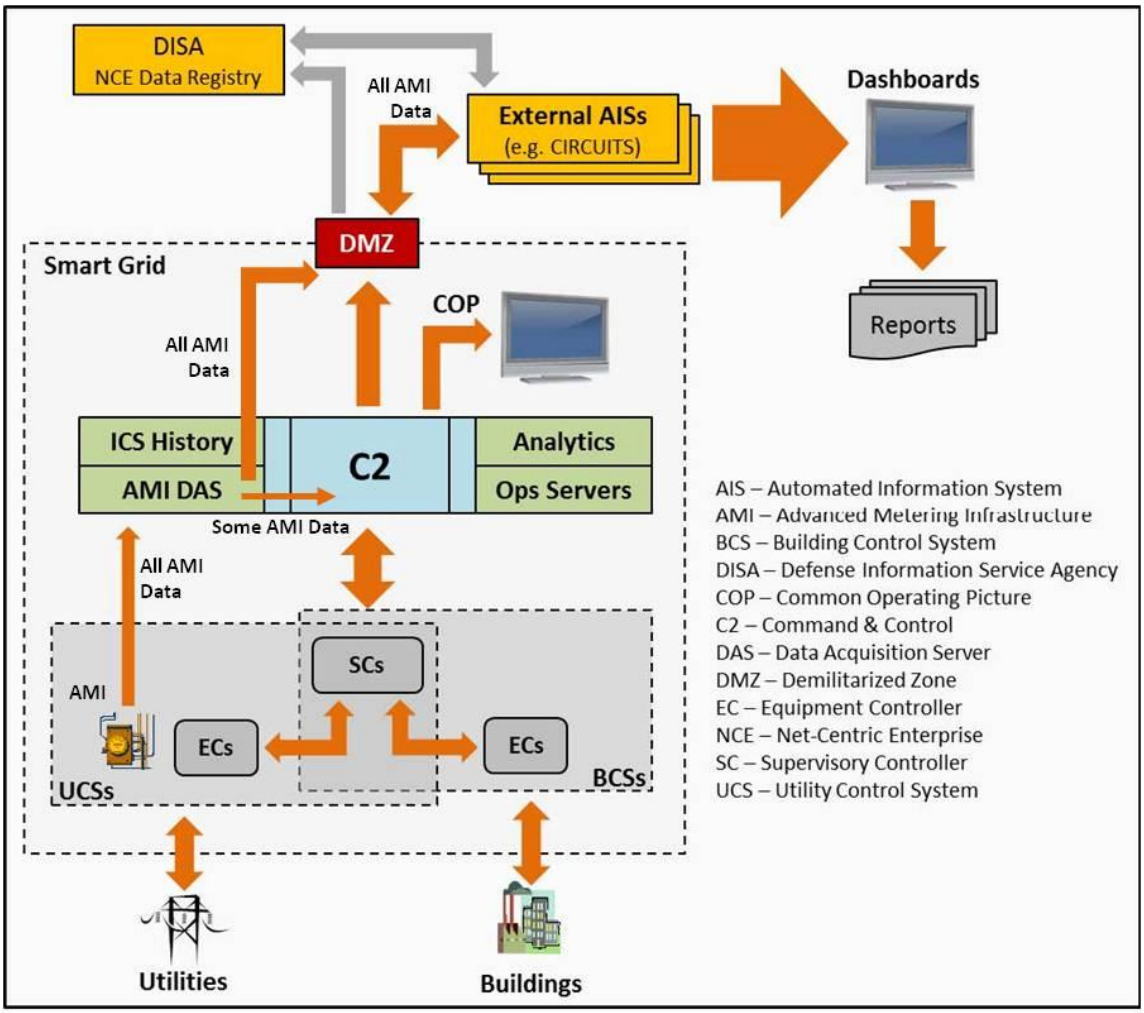
Tailored efforts to reach Smart Grid IOC will exist for each RCAoA to account for respective maturity levels, existing networked systems, and ongoing ICS-related projects.

The capability gaps between maturity level and IOC will be analyzed and prioritized accordingly and criteria (see KPP-1 Threshold in Table 1, Section 6) that include; ROI (e.g. energy savings and operations efficiencies), Security (physical and cyber), and tenant mission requirements.

1.2.2 Data Availability

A pervasive data availability gap exists both within existing ICS and between ICS and external AIS that consume or exchange data with the Smart Grid. This gap is addressed by multiple KPPs and KSAs located in Section 6. The expected data flow is depicted in Figure 4.

Figure 4 - Data Flow



Data and control signals connect building equipment such as Heating, Ventilation and Air Conditioning (HVAC) and utility equipment such as metering and electrical switch gear to Utility and Building Control Systems (UCS and BCS) and Equipment Controllers (ECs). ECs typically provide real-time process control. Supervisory Controllers (SCs) aggregate data, coordinate between ECs, provide data to and accept high level commands from C2 servers and Human-Machine Interfaces (HMI).

Integrated data is made available within a secure Demilitarized Zone (DMZ) to external AIS where it can be aggregated with other business information and presented as dashboards or integrated reports.

1.2.3 IA Accreditation and Cyber Security

Currently most Navy and Marine Corps ICS have very little in the way of IA controls and cyber security measures in place. Recent audits[13] of major utility providers are representative of the state of Navy and Marine Corps systems of similar types. A secure and accredited platform and common architecture[14] is required as the basis for all operational capabilities.

A number of DoD Directives and Instructions govern AIS, cyber security and IA.

NUMBER	DATE	TITLE
DoD M-5200.01 v1-4	4/22/2008	DoD Information Security Program
DoD 8523.01		Communications Security (COMSEC)
DoDD 8100.2	4/23/2007	Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)
DoDD 8500.1E	4/23/2007	Information Assurance (IA) updated for DIARMF
DoDI 8500.2	2/6/2003	IA Implementation updated for DIARMF
DoDI 5200.08	12/10/2005	Security of DoD Installations and Resources
DoDI 5215.2	9/2/1986	Computer Security Technical Vulnerability Reporting Program, (CSTVRP)
DoDD 5200.2	4/9/1999	Personnel Security Program

Cyber Security must be built into new acquisitions, and both new and existing ICS must be assessed for risk with respect to control systems providing C2 to Navy and Marine Corps facility infrastructure as well as the Global Information Grid (GIG). All building

[13] For example: GAO-04-354, GAO-08-526 and Victorian Auditor-General Report 2010-11:15

[14] Smart Grid has two accreditation packages for each AoR. The ICS Platform enclave (ICS-P) supports the information infrastructure for Smart Grid in that AoR, and the ICS Common Architecture (ICS-CA) is the set of operational components.

and utility control systems will be accredited under the DoD Risk Management Framework whenever and wherever they include components or architecture for which DoDD 8500.1 applies.

1.3 Operating Environment

The operating environments of ICS differ slightly and tend to be widely dispersed throughout building and utility systems serving Navy and Marine Corps locations. Control systems currently exist in utility facilities such as electrical sub-stations and waste water treatment plants as well as shipyards, dry-docks and other waterfront facilities. Environmental controls and sensors are often spread throughout weapons magazines including special weapons facilities. Smart Grid capability will be targeted toward facilities with high energy use and those that will achieve operational cost savings. Mission Assurance is a key factor in judging projects that provide Smart Grid capabilities.

1.3.1 Industrial Control System Infrastructure (ICS-I)

ICS-I is defined in UFC 2-000-05N per 89050-1, ICS-I, "*manages and moves data that provides real-time operational capability...*" and "*…includes all hardware and software automation equipment located in a central control center/room(s) and/or distributed throughout an installation, fiber, copper and/or electromagnetic communication pathways that carry only Industrial Control System (ICS) traffic, associated electronic construction, the Facility Point of Connection (FPOC), and all electronic components and software necessary for interface with the FPOC*".

A single instance of ICS-I exists at each installation supporting UCS and BCS at that installation. ICS-I may be connected between installations forming a larger Smart Grid. DoD uses facilities Category Codes to define and track facilities.

1.3.1.1 Server Rooms

Server rooms and the ICS Platform enclave (ICS-PE) administration centers are secured facilities with limited access. Physical access to equipment in these areas is secured at the room or building level. Rack-mounted equipment is secured within a secure rack.

Local uninterrupted power supply (UPS) and backup generation is provided for time durations necessary to satisfy IA requirements, operational requirements and will be coordinated with backup generation inherited from the installation's electrical distribution system.

1.3.1.2 Operations Centers, Control Rooms

Primary monitoring and control of sub-systems shall take place inside of controlled-access areas. Network equipment and supervisory controllers should be further secured in locked cabinets with restricted access. Distributed workstations are secured in access-controlled locations.

1.3.2 Utility Control System (UCS)

As defined in UFC 2-000-05N per 89050-3.2, UCS, "*also called Supervisory Control and Data Acquisition (SCADA) systems (and other terms), are used for monitoring,*

controlling and/or regulating utility systems in real time, and measuring, collecting and analyzing energy usage. These systems are integrated into individual utility plants and are in most cases a component of individual utility facilities. Advanced Metering Infrastructure (AMI) meters are part of the UCS."

Metering devices, many of which are IP-addressable, are located on transformers along roadsides, at utility distribution points, in or on buildings and in utility plants. Where these devices are IP-addressable, physical security and logical security, through network traffic control, must be in place to protect the network.

Devices that are used to control and monitor the production and distribution of utilities are normally located in specialized industrial facilities such as electrical substations, steam plants and waste water treatment plants. Physical security of these areas is critical to the security of the systems being controlled.

1.3.3 Building Control System (BCS)

As defined in UFC 2-000-05N per 89050-3.2, BCS, "*also called Direct Digital Control (DDC) systems (and other terms), are used for monitoring, controlling and/or regulating building systems in real time. These components are integrated into building systems such as HVAC, irrigation and lighting, and are in most cases components of individual facility buildings."*

These types of devices are located inside facilities of all types, and are often networked between multiple facilities.

1.4 System of Systems Approach

DoD Directive 4630.5 states that a System of Systems (SoS) is "A set or arrangement of independent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole."

Smart Grid is an advanced capability-enabling information infrastructure for facility and utility systems within the Navy and Marine Corps. It is a *"…complex system made up of interrelated sub-systems* [and, as each sub-system] *is upgraded, it will enable integration and interoperability of a greater diversity of technologies and applications."*[15]

From the same IEEE reference: "*This interoperation will include a preponderance of monitoring and control activities, enabling two-way flow of electricity and information for the production, transportation, and consumption of electric energy. In its most encompassing form, implementation of a Smart Grid adds intelligence to all areas of the power system infrastructure that will interoperate with end-use applications and loads."* And: "*The Smart Grid will generate data in vast quantities. To manage, store, and effectively use this data, the power system, communications, and information*

[15] IEEE Std 2030™-2011, Section 4.2 The Smart Grid – A Complex System of Systems

technologies should be coordinated using a system of systems approach; that is, achieve interoperable communications across smart grid technologies."

While the IEEE refers to an electrical Smart Grid, the Navy and Marine Corps Smart Grid encompass all utilities and these fundamental principles still apply.

Smart Grid integration consists of a set of components, hardware and software, that can be both centralized as servers and dispersed geographically as a distributed system of Supervisory Controllers (SC) as defined in UFC 2-000-05N 89050-3.3.

Placing the integration components (hardware and/or software) as high up in the data flow hierarchy as possible allows the greatest use of existing systems, and maximizes competition within the UCS and BCS where the majority of incremental acquisition takes place. Selection of an integration framework that extends down to the supervisory controller at the facility maximizes interoperability and standardization within the as integration components are acquired or replaced, which lowers sustainment costs, increases efficiencies of operation and enables SoS-wide analytics.

ICS-I operational software, including middleware, supports the integration BCS and UCS. The data collected may often be useful if integrated into displays used for C2. Integration opportunities exist between the supporting operational software, the Graphical User Interface (GUI), historical data, dashboards and hardware platforms.

ICS-I, BCS and UCS, together, serve a common purpose of providing command and control for critical infrastructure and are interrelated. Providing a common platform enclave across these interrelated systems both increases efficiencies and provides a consistent IA and network security posture across all ICS.

The intent of a System of Systems (SoS) architecture is to enable the Smart Grid capabilities stated in Section 1. IEEE Standard 2030-2011 also identifies several noteworthy burdens. "*For instance, correct design of one particular system, including data, command, and control, without complete consideration of other systems, may not result in the best operation of the whole system. Information that is produced and consumed in a closed system*[16] *may need to be exchanged with other systems in the future. In complex systems, some coordination is required because the potential interactions may not be obvious at the beginning, but potential inadvertently 'designed in' problems can be corrected by an overall supervisory system"* and "*To manage, store, and effectively use* [the] *data* [Smart Grid] *should be coordinated using a system of systems approach; that is, achieve interoperable communications across smart grid technologies."*

[16] A "closed system" in this context refers to a system whose communications pathways are isolated to the system, not to be confused with an "open system architecture" which refers to a vendor-independent, non-proprietary architecture based on official and/or popular standards.

2. Analysis Summary

A number of analyses at Navy and Marine Corps installations have been completed, or are underway, that investigate the relevant considerations of Smart Grid development. There are several distinct types of analyses that are predominant in the program at this stage, including those that determine technical and economic system attributes such as those that were used to develop the Smart Grid KPPs. Analysis details can be found in Appendix C.

Determination

Smart Grid technical analyses have evolved from the various Smart Grid pilot applications that currently exist across the Navy and Marine Corps, and economic analyses have been executed via a series of studies performed both at the installation level and the enterprise level.

Identification

Smart Grid KPPs were identified and developed through partnering sessions between OPNAV, CNIC, and Marine Corps resource sponsors, NAVFAC Leadership, and Smart Grid and IA subject matter experts.

Alternatives

Multiple factors from multiple sites were considered in the determination of system attributes. Input was solicited from Supported Commands, NAVFAC and industry SMEs, and other stakeholders to incorporate all relevant factors. In the case of the economic analyses, cost vs. benefit has been a major driver of the resultant project scope.

Objectives

Existing Smart Grid capability will weigh in to planning scope of work for projects. DD1391s will address filling existing gaps to fulfill supporting commands goals in accordance with CDD requirements.

Assumptions

Smart Grid studies have shown that Smart Grid technologies can, under most circumstances, provide enough economic benefit to justify the required investment. Justification assumes that the technology is used to improve facility management processes in order to reduce energy consumption and costs.

Cost Estimation Model

Site study results were, and are continually, used to develop and refine a parametric model and applied to the Navy enterprise. The results of the model indicate that Smart Grid may provide an economical return on investment, reduce energy consumption, improve energy security, or enable key energy program capabilities.

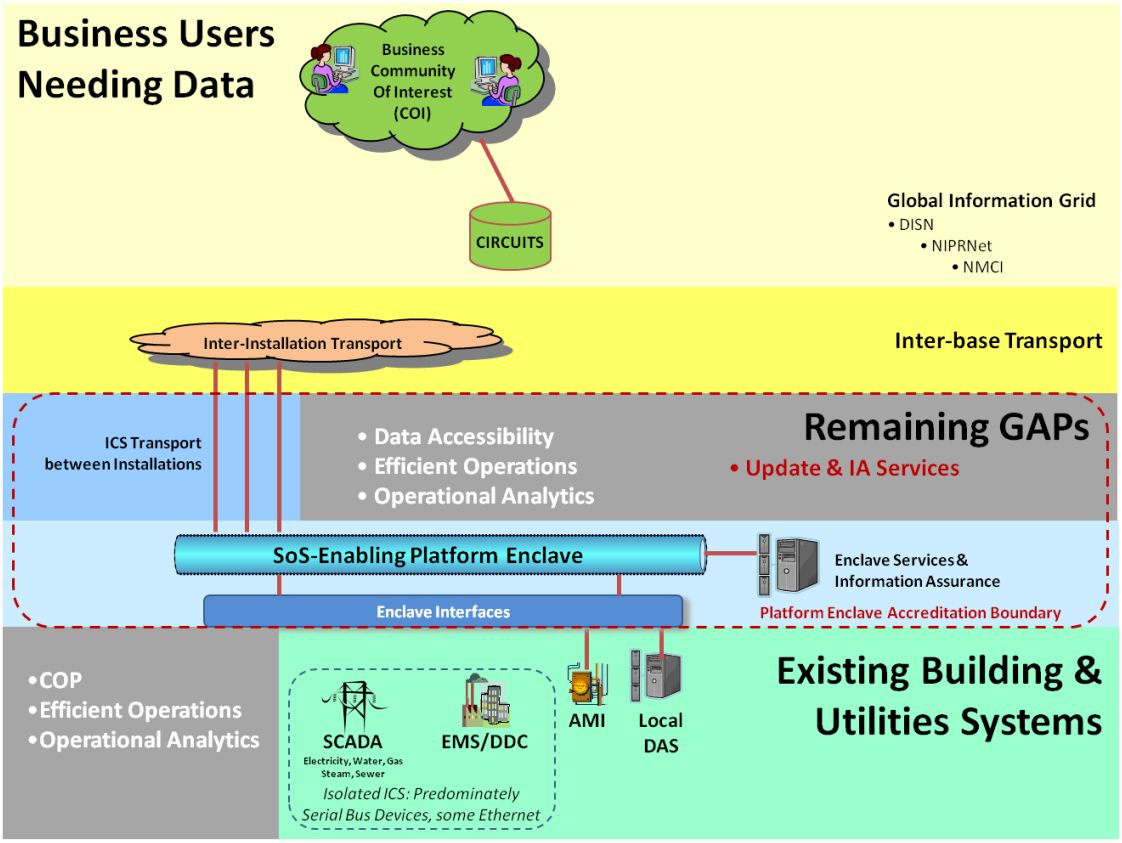
3. Concept of Operations Summary

Smart Grid will enable an enterprise Smart Energy Concept of Operations (CONOPS). A formal enterprise Smart Energy CONOPS, once fully developed, will be used in delineating specific Standard Operational Procedures (SOPs). The full development of the Smart Energy CONOPS and its related SOP's will address the operation of Smart Grid for utilities and buildings. This operational construct will introduce new, more efficient, procedures for operations and maintenance of utilities and buildings, facilities engineering, energy analytics, awareness, and Smart Grid sustainment activities.

3.1 System of System (SoS) Integration

Systems management and administration will be integrated through a common platform enclave that enables SoS as shown in Figure 5 where it initially links AMI between bases and provides the capability to link existing and future ICS as shown in subsequent figures. This SoS enclave will enable cross system sharing of data as well as common operations capabilities and common enclave administration and information assurance services. This will enable a full Net-Centric Environment (NCE), further explained in Sections 3.2 and 3.3, with fully integrated sets of data for utilities and buildings that cross functional boundaries.

Figure 5 - SoS Enablement



The Smart Grid enclave architecture and management processes will help to mitigate risks associated with increased integration (Section 4 – Threat Summary). It will provide a platform upon which all DoN ICS are accredited in two packages, ICS-PE and ICS Common Architecture (ICS-CA)[17], for each RCAoA. The Smart Grid program's accreditation requirement applies across all ICS independent of prioritization build-out of Smart Grid operational capabilities.

Capabilities derived from advancing existing isolated ICS to a SoS architecture include:

- Centralized C2
- Accurate system information for identification and response to real issues
- Centralized administration
- Data integration

In order to provide a manageable path to the interoperability and integration required, while maintaining the integrity of existing systems and creating as wide a competitive field for future acquisition as possible, an Open Systems Architecture[18] (OSA) approach is taken that utilizes a middleware concept at intermediate and top layers in the data path.

3.2 Initial Net-Centric Environment (NCE) Capability

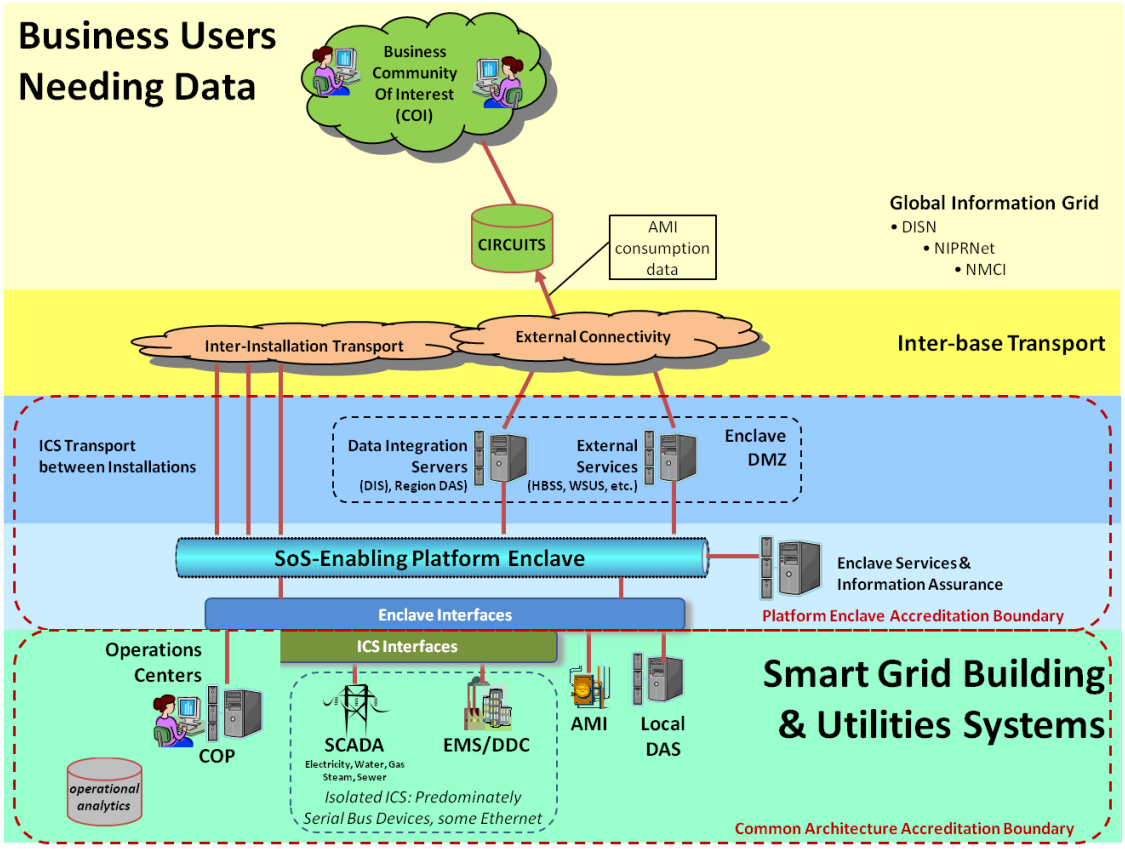
The *Net-Centric Environment – Joint Functional Concept* v1.0 from April 2005 states that a net-centric environment is *"A framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it."*

Business Systems are those that are accessible directly from the Navy Marine Corps Intranet (NMCI) and require frequent and automatic access to various UCS and BCS data. Figure 6 shows that the first implementation of this enabling capability will provide utility metering data to the relevant external business AIS (e.g. CIRCUITS) and the first step toward a full NCE system by providing data availability to business systems.

[17] Explained in detail in *A NAVFAC Industrial Controls Systems Common Architecture Framework*, referenced [9] of Appendix B.

[18] Open System Architecture is a system design approach that establishes key interface boundaries between the functional elements and the modular components within them.

Figure 6 - NCE-Enablement, Data Availability



3.3 Full Net-Centric Data Strategy (NCDS)

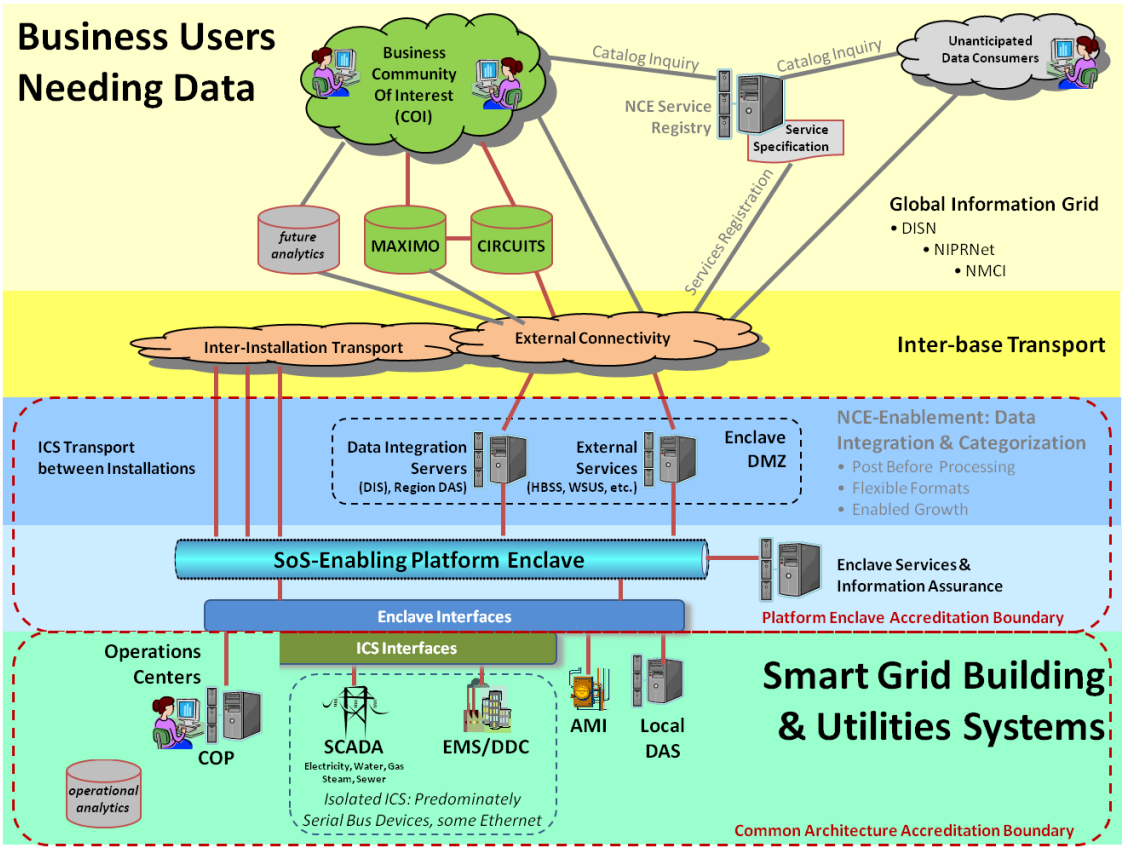
In the final data availability stage a fully Net-centric data environment in accordance with DoDD 8320.02 is formed as depicted in Figure 7. The full net-centric goal is to have data collected from all sub-systems and integrated in a way that makes the data understandable to all users without reference to the technical nature of its source.

DoD Architecture Framework states that data management should *"focus on making data available, understandable and trusted in a Net-Centric Operating Environment (NCOE)"*. The NCDS identifies key aspects of an NCOE as;

a. Make data visible, available and usable,
b. "Tag" data with metadata to enable discovery
c. Post data to shared spaces, and
d. Move away from point-to-point interfaces to "many-to-many" exchanges within a net-centric data environment.

Additionally a key concept of the net-centric environment is to accommodate the unanticipated user by emphasizing that *"…the NCO (Net-centric Operations) intends for users to look to the NCE, rather than being constrained to a predefined source, to find the information and capabilities they need to execute their missions."*

Figure 7 - Full NCE



DoD will adopt[19] the National Information Exchange Model (NIEM) as the best suited option for standards-based data exchanges. Key data attributes are: Visible, Accessible, Understandable, Trusted, and Interoperable. Among NIEM's value propositions[20] are:

- *Enhancing the quality of governmental decision making by enabling accurate, timely, complete and relevant information to decision makers;*
- *Achieving greater efficiency, effectiveness and return on investment (ROI) in operations by accelerating information exchange design and development;*
- *Reducing risk in development efforts for practitioners and industry by having common exchange standards, tools, processes, and methodologies; and*
- *Improving public safety and homeland security by breaking down stovepipes, enabling real-time, secure, enterprise-wide information sharing.*

The NIEM will provide the architecture for future interfaces between Smart Grid and external AIS and provide a cost effective method of meeting KPP-3 and KPP-4.

[19] DoD CIO Memorandum, 28 March 2013, *Adoption of the National Information Exchange Model within the Department of Defense*
[20] Introduction to the National Information Exchange Model (NIEM), Feb 12, 2007, Version 0.3, page 17

4. Threat Summary

As utility and building control systems evolved from isolated simple controllers to intelligent electronic devices linked by special purpose computer systems, the management of Information Technology (IT) aspects of these systems did not keep pace, as they were rarely thought of as being related to IT; Manufacturers of ICS components and software routinely have lagged behind modern IA practices by five to ten years. Today's ICS management practices do not typically incorporate the Department of Defense (DoD) Information Assurance (IA) requirements or best industry practices and a gap has developed between today's network threats and the resilience of ICS components. Individual BCS and UCS are being interconnected by computer networks that provide C2 and aggregate management and monitoring information from remote locations. This integration provides efficiency through centralized management and maintenance.

"Business drivers are resulting in automated decision intelligence replacing manual operations, and as a result reliability of the power system is increasingly affected by the [ICS] *infrastructure."*[21]

And: "*A broader new smart grid feature set is making the power system critically reliant on the overlaid* [ICS] *infrastructure by requiring integration of diverse, connected, interdependent, and adaptive functions and applications."*

In the past when BCS and UCS were stove-piped, the damage an adversary could cause would be isolated to the physical location where access was granted. However, the natural evolutionary automation of these systems exposes operations and business processes to vulnerabilities that could be exploited by deliberate attacks, operational mistakes, equipment failures, and natural disasters. An intruder now has the potential to disrupt or damage mechanical and electrical equipment, and supported commands, beyond the original penetration point.

Today a remote user can exploit vulnerabilities across the entire ICS simultaneously. His reach is only limited by the extent of the ICS to which he gained access, and the level of damage is only limited by his expertise, research and malicious intent.

Page 1 of the Executive Summary of NIST Special Publication 800-82 explains:
"Originally, ICS implementations were susceptible primarily to local threats because many of their components were in physically secured areas and the components were not connected to IT networks or systems. However, the trend toward integrating ICS systems with IT networks provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats. Also, the increasing use of wireless networking places ICS implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. Threats to control systems can come from numerous sources, including hostile governments, terrorist

[21] IEEE Standard 2030-2011, Section 4.5.3 - Security

groups, disgruntled employees, malicious intruders, complexities, accidents, natural disasters as well as malicious or accidental actions by insiders. Protecting the integrity and availability of ICS systems and data is typically of utmost importance, but confidentiality is also an important concern."

Smart Grid may rely upon an inter-installation communications transport that carries more than just Smart Grid traffic. Smart Grid traffic is encrypted as it crosses a transport Point of Presence (PoP). The transport provider is responsible for safeguarding its infrastructure from intrusion originating within or outside the Smart Grid, and for the cyber-security posture of the Smart Grid ICS-PE to support that requirement. It is also the responsibility of the Smart Grid ICS-PE to ensure the cyber security of Smart Grid systems from intrusion both within and from external sources. To this end, the ICS-PE must be able to isolate from a potentially breached transport and continue to operate at isolated bases within an RCAoA. Smart Grid needs to have pervasive resilient postures against safety and security incidents so that they are prevented, detected, and recovered from in a timely fashion.

Refer to Appendix F for a summary of cyber risks associated with a highly integrated and networked Smart Grid.

4.1 Damage

If hackers gain access to the computers and servers they could corrupt and damage the software, crash the systems or alter the behavior to cause physical damage. This could be coordinated to occur simultaneously across multiple systems.

Figure 8 depicts the division of the system into three broad security bands: Operations and Network Administration, and two bands composed of end devices such as controllers and meters. The diagram shows relative system sensitivity vs. extent of deployment, the most numerous deployments being metering in relatively unsecured locations.

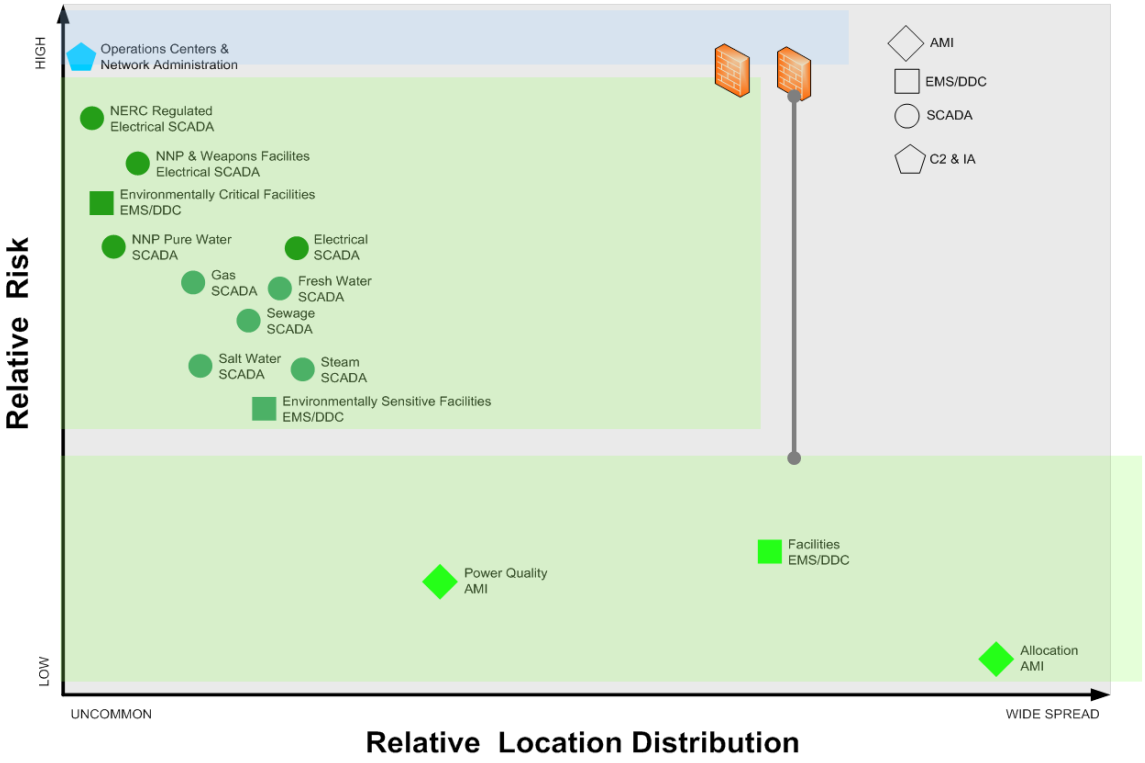
Many physical systems and devices are set to automatically shut off at preprogrammed points to protect the systems from overheating or overstressing. It is possible for an attacker to reset the stress points and drive the hardware to failure. Examples include: a) rhythmically turning on and off a 480-volt motor can destroy it, b) commanding a valve to operate beyond its rating or range can destroy it, and c) the Aurora Attack[22].
The risk to ICS is increasing as their obscurity diminishes. Security by obscurity is not sufficient to protect our critical infrastructure. Today it is quite easy to obtain manufacturer information on most ICS.

[22] The Aurora Attack creates an out-of-synchronization re-close that can translate high electrical torque to stress on the mechanical shaft of rotating equipment such as primary generators, causing them to catastrophically fail.

Four factors contribute to the escalation of risk to ICS:

1. Control systems are adopting standardized technologies with known vulnerabilities, such as Microsoft operating systems, common and not well secured controls protocols, and the Internet.
2. Control systems are connected to other networks that are not secure.
3. Insecure connections exacerbate vulnerabilities.
4. Manuals on how to use ICS are publicly available to the terrorists as well as to legitimate users.

Figure 8 - Risk vs. Distribution



Protecting the Smart Grid from vulnerabilities and attacks preserves mission and security which are of utmost importance to the Navy and Marine Corps.

Infrequently mentioned are threats to performance grouped under the term *Power Quality*[23]. The threat affects both Smart Grid C2 equipment as well as equipment operated by supported commands that rely on power monitored by Smart Grid. Smart Grid C2 of power systems, to which supported commands rely, directly supports mission assurance.

[23] Power Quality is defined by IEEE Standard 1519 as: *The concept of powering and grounding sensitive equipment in a manner that is suitable to the operation of that equipment.*

4.2 Scope of Threat

The cyber threat is real, proven, and in evidence in a wide variety of examples[24].

Computer systems are exposed to a wide spectrum of attackers with various degrees of malicious intent. Hackers, organized crime, cyber terrorists, and nation states are examples of different classes of adversaries. Motives can range from a hacker testing his skills, to organized crime planning on extortion to extreme radicals trying to undermine national security or cause loss of life.

Security in ICS is often an afterthought with networks cropping up out of necessity. Tools to audit the security configuration of the ICS networks and to monitor and alert for system intrusions in many cases do not exist at all. As Smart Grid components become more complex, zero-day[25] vulnerability attacks will become more prevalent. Networked components of Smart Grid and its supporting information infrastructure are not exempt from experiencing this escalation in discovered vulnerabilities.

The ICS may be vulnerable by different routes, including wireless transmission, direct access to control system computers, exploitation of dial-up modems used for maintenance, or through the internet.

> *"Security for SCADA is typically five to ten years behind typical information technology (IT) systems because of its historically isolated stovepipe organization."*[26]

4.3 Risk Mitigation and Management

Typical risk mitigation for cyber threats begin with a passive defensive perimeter followed by detection, isolation and recovery. However it is widely held today that one cannot prevent offensive cyber dominance by any passive tactic. Risk is managed by balancing information assurance (IA) with operational system and process requirements.

Prevention

Preventive measures will meet all Navy, or Marine Corps respectively, and DoD requirements leading to Platform IT Risk Assessment (PRA) acceptance. Risk is managed by balancing IA with operational system and process requirements and is managed by a combination of prevention detection, isolation, and recovery processes.

Detection

Intrusion detection is provided by a number of mandatory tools such as Host Based Security System (HBSS) with Host Intrusion Prevention System (HIPS) and rogue sensors, virus scan, port security, and Intrusion Detection and Wireless Intrusion Detection Systems (IDS, WIDS). Additionally ICS systems would benefit from ICS-specific rule sets for firewalls.

[24] Examples of cyber attacks in Appendix B, References [1] through [6]
[25] A zero-day attack is a cyber-attack that exploits a vulnerability on 'day zero' of awareness of the vulnerability, meaning developers have had zero days to address and patch the vulnerability.
[26] Appendix B, Reference [8]

Detection, however, requires the workforce to respond in a timely manner. Smart Grid availability for critical infrastructure directly affects mission and processes and personnel must be in place for a timely response. This is the nature of detection.

Isolation and Recovery

If an intrusion is successful, the first response involves isolating the affected systems and subsequently restoring services. To this end, an Incident Response Plan, a Continuity of Operations Plan (COOP), and a Disaster Recovery Plan must be developed with sufficient RCAoA-level details, training, and drills in place – and they must be exercised on a periodic basis. Documenting and logging events both during and after an attack are critical to future prevention and detection efforts.

5. Program Summary

Smart Grid performs as an interoperable and cyber-secure information collection and controls technology that supports near real-time command and control of utility and building control systems and delivers Smart Grid data to external AIS via the GIG. Together, these capabilities improve energy and information security and utility system reliability, and drive cost savings through improved energy efficiency and more effective participation in demand response programs.

A key criteria for assessing, validating, and prioritizing Smart Grid investments will be the Energy Return on Investment (eROI).

5.1 Overall Strategy

The ICS systems that will make up an RCAoA's Smart Grid already exist in one form or another. Often they have been connected in an ad-hoc manner or, in a few instances, much more sophisticated Smart Grids have been fielded. The overall strategy is to gather these disparate networks together under common RCAoA-wide System of Systems Platforms use existing DoD transport network infrastructures wherever possible. Not every site, building, or system will be connected to the grid. Connection will be based on specific criteria (Navy only criteria in Appendix I) in the areas of cost effectiveness, building operations, cyber security, and mission criticality.

The overall strategy philosophy is to secure first, connect second. This is accomplished via an incremental approach as illustrated in Figure 9 showing the Platform Enclave deployed first for AMI and then for ICS. Step 1 of this approach establishes a secure enclave first that allows both meter and Industrial Control System information to safely be transported and protected along the grid. The enclave requirements are additive and expand incrementally until all devices can safely connect. Step 2 is connection of devices. For any given device, connection is dependent on security "readiness". Because security "readiness" varies across installations, the incremental approach allows device connection to the extent allowable by the maturity of the secure enclave. Enclave requirements for each increment will be prioritized. For example, some installations have devices like meters and SCADA systems already in place, therefore enclave requirements for in-place systems will be addressed early on in the incremental approach.

Successful integration to the enclave and compatibility of disparate devices are addressed via a "common architecture", which will be designed to connect both fully functional legacy devices and devices with more advanced technologies. The common architecture stays common throughout the incremental approach, which controls cost and helps maintain cyber accreditation consistency and compliance.

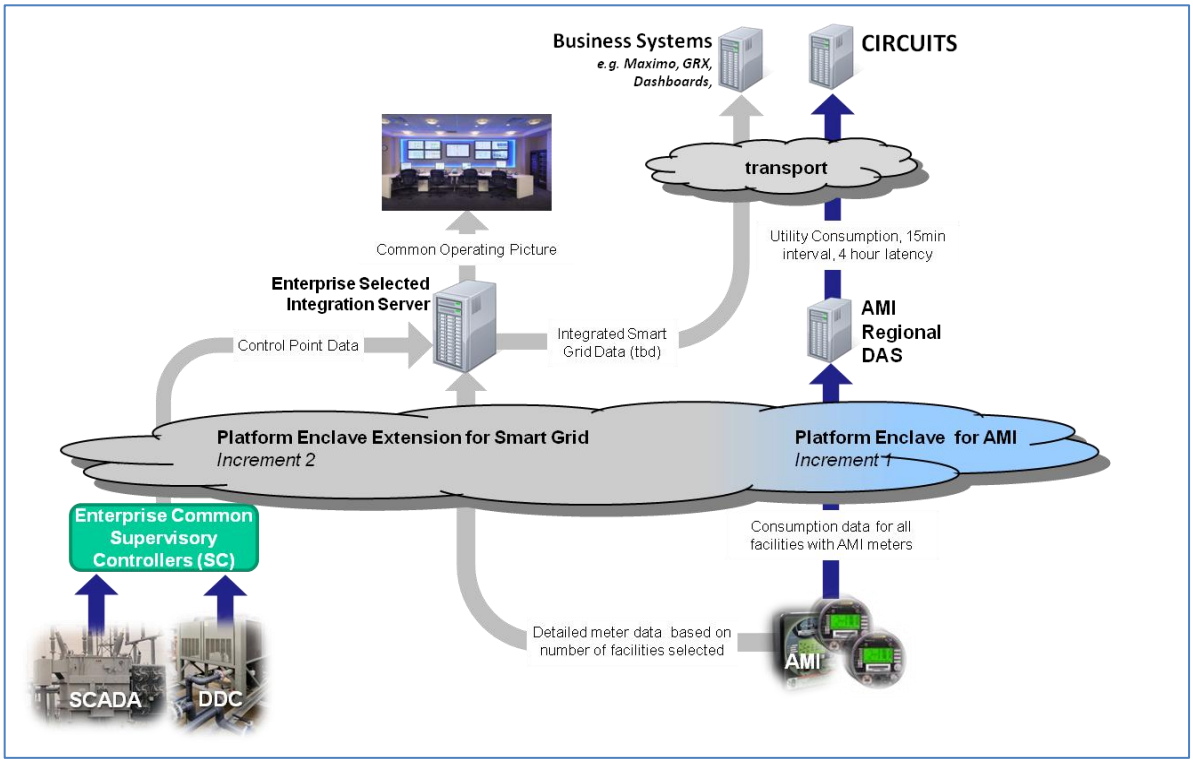
Smart Grid will leverage existing systems for cost efficiency. In support of reusability Smart Grid Program will execute Plans of Action and Milestones (POA&Ms) to accredit existing unaccredited systems. This effort will include the repurposing existing non-related local capabilities such as identifying and utilizing existing dark fiber. To the maximum extent possible, Smart Grid ICS Centers will be planned within existing infrastructure/footprint. Options for distributed ICS Center functions will be addressed in

the Systems Engineering Plan. New infrastructure/footprint will require adequate justification for approval.

At its core the Smart Grid is an integrated sensor system comprising OT. Therefore, it is envisioned that all Smart Grid components will be approved to operate in the Platform Information Technology (PIT) environment with a PIT Risk Assessment (PRA).

NIST Special Publication 800-82 *Guide to Industrial Control Systems (ICS) Security* and DHS External Report # INL/EXT-06-11478 *Control Systems Cyber Security: Defense in Depth Strategies* shall be used to guide architecture of ICS enclaves and supporting transport requirements. Smart Grid will be accredited within the DoD Risk Management Framework (RMF). ICS systems that need to furnish data to the corporate business network should be configured per the NIST and DHS recommendations and within the context of a DISA DoD Network model.

Figure 9 - Incremental Secure First Approach

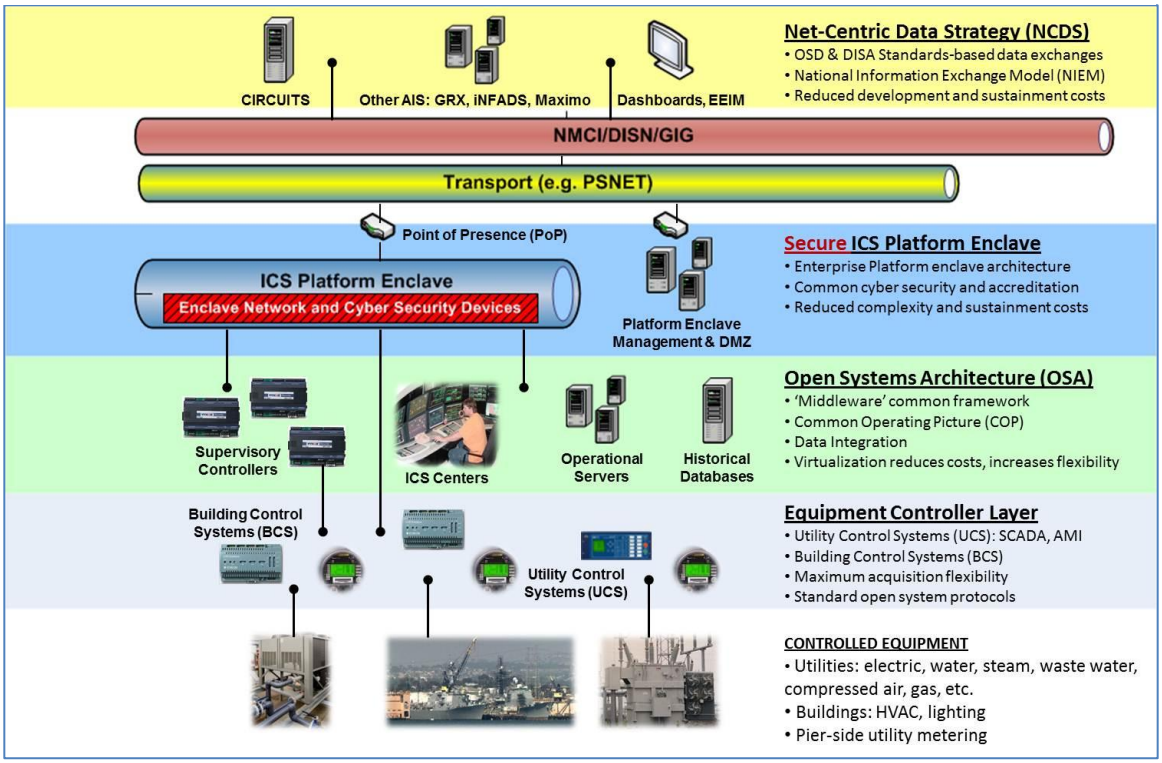


5.2 Integrated Common Architecture

The *NAVFAC Industrial Controls Systems Common Architecture Framework* will be an essential element that directs the Smart Grid program through its development and deployment. This will be combined with those maintenance strategies and concepts that will enable efficient and affordable sustainment. The common architecture framework will employ OSA principles.

Figure 10 illustrates the Smart Grid common architectural layers. Each layer will employ common elements and OSA principles that support the operational functions within that layer. The Navy's application of Smart Grid shall use a single platform transport coupled with an added layer of security via the ICS enclave depicted in this figure.

Figure 10 - Common Architectural Layers



Smart Grid Pilots and other projects have played a significant role in informing the best way ahead for a common architecture framework solution for the enterprise and future implementation of Smart Grid.

5.3 Increment Relationships

Each incremental addition (to be defined in the Smart Grid Program Plan documents[27]) of advanced capability is dependent upon the successful completion of the previous increment (the first being IOC) and provides a structure for IA, network security and

[27] See Appendix E for relevant Program Plan documents such as the Integrated Master Plan (IMP) or the Integrated Master Schedule (IMS).

consolidation of data without adversely affecting baseline functionality of existing systems.

It is important to understand that for nearly all RCAoAs there are existing operational systems that are constantly in a state of flux as various projects with Smart Grid content are executed. Timing of each increment needs to take into account the requirements of projects that use, modify or expand the existing Smart Grid without affecting the execution of contracts that could impact cost and schedule.

5.4 Considerations

Considerations driving the incremental delivery plan:

- Fleet Concentration Areas
- Return on Investment (ROI)
- Mission Critical Loads
- Critical Infrastructure Determinations
- Information Assurance – including Accreditation and Risk Acceptance
- Gap Analysis
    - Existing sub-system functionality
    - Infrastructure availability
    - SoS integration maturity
    - Technologies to be developed
    - Operational needs of existing ICS
    - Cost

5.5 External Dependencies & Risks

External dependencies and risks will be addressed as part of the Program Plan and, those that have IA impact, in IA documentation.

5.6 Previous Methods of Acquisition

In the past acquisition for sub-systems and necessary network infrastructure was made on a per project basis. Much of the OT acquisition was made by contractors or subcontractors with little input from government. If a specific project required network components they were sized specifically for that project and not for the overall SoS requirements and anticipated expansion. Additionally, platform enclave administration was not viewed from an RCAoA-centralized perspective so there was little consistency in IA procedures, operating system patches, virus scan patches or hardware refresh processes.

Practices of allowing vendors to install communications channels for remote access has resulted in a poorly understood existing cyber risk. These practices must be curtailed and remaining links discovered and removed. Future acquisition will not allow this legacy practice.

6. Performance Parameters

Performance parameters are used to determine how well a system or capability will meet the supported command's requirements or goals. Performance parameters must be concise and measurable; preferably via a quantitative measurement. These parameters typically have a threshold value associated to indicate minimum acceptable performance. Objective values may be useful in determining a Trade Space to accommodate budget or other restrictions. All performance parameter values were based upon supporting rational such as: subject matter expert (SME) experience, lessons learned, trade studies, or pilot project results. In each of the following tables column 1 references the functional capabilities in sections 1.1.1 through 1.1.6.

6.1 Key Performance Parameters (KPPs)

KPPs are a special subset of the performance parameters used by a program sponsor or Milestone Decision Authority (MDA) to determine if a program should continue. The KPP rigidly defines the most important performance aspect(s) of a program.

Table 1 - Key Performance Parameters (KPPs)

Functional Capability	ID	Key Performance Parameter	Development Threshold	Development Objective
1.1.1,1.1.3 ,1.1.6	KPP-1	Integration of all Smart Grid ICS by RCAOA	Integrate AMI, new ICS, and some[28] existing ICS that are connected to a network.	Integrate AMI, new ICS and 100% of existing ICS that are connected to a network
1.1.1,1.1.6	KPP-2	Collection and utilization of operational data for facility management through integration with all energy related ICS components	Data storage capacity to account for 5 years by RCAOA	Data storage capacity to account for 10 years by RCAOA
1.1.2,1.1.6	KPP-3	Transfer of operational data to external business AIS(s) with metrics of; comprehensiveness, consistency, timeliness and storage capacity.[29]	All AMI data, at 15 minute intervals, with 4 hour latency and stored for 5 years	All relevant[30] ICS data, at 15 minute intervals, with 4 hour latency and stored for 10 years
1.1.2	KPP-4	Data accessible by external AIS is accurate	Quality Score[31] of >50%	Quality Score of >80%

[28] Criteria for choosing threshold ICS are based upon; ROI (e.g. energy savings and operations efficiencies), Security (physical and cyber), and Mission Assurance.
[29] Data transfer metrics based upon the standard set for AMI transfer to CIRCUITS.
[30] Relevant data will be defined in the Program Plan documents described in Appendix E.
[31] The CNIC HQ N441 Data Quality Score assesses the accuracy of facility data in Navy authoritative databases currently by correlating data between iNFADS, CIRCUITS and DUERS. The scale is 0-100% with zero indicating no valid reporting.

1.1.1	KPP-5	Information displayed[32] on system operator displays allows for effective action-based decisions	Operator[33] satisfaction is 75% or greater	Operator satisfaction is 95% or greater
1.1.4	KPP-6	Demand reduction and response Command and Control (C2)	Predicted load reduction achieved within 25%	Predicted load reduction achieved within 10%
1.1.4	KPP-7	Establishing/re-establishing facility operational baseline (commissioning)	Initial commissioning complete across all facilities	Design performance maintained within 10%

There are a number of required KPPs associated with Major Automated Information System (MAIS) programs or Acquisition Category (ACAT) programs with identified AIS components. The NetReady KPPs address cyber security accreditation and information interoperability, both of which are essential to the Smart Grid program.

Table 2 - Required KPPs

Functional Capability	Required KPP	Development Threshold	Development Objective
1.1.5	NetReady - IA Compliance per DoDD 8500.1	100% compliant[34]	100% compliant
1.1.1,1.1.2, 1.1.6	NetReady - Net Centric Data Strategy (NCDS) Compliance per DoDD 8320.02	NCDS Statement	100% compliant and integrated in a net-centric operating environment
1.1.1, 1.1.2	NetReady – Global Information Grid (GIG) Tech Guidance per DoDD 8320.02	Key Interface Profile Declaration	Meta-data[35] registration with DISA
	Sustainment - Availability	To be developed as part of the Program Plan	To be developed as part of the Program Plan
	Energy Efficiency[36] *(selectively applied)*	To be developed as part of the Program Plan	To be developed as part of the Program Plan
	System Training *(selectively applied)*	To be developed as part of the Program Plan	To be developed as part of the Program Plan

[32] System operator displays are user interfaces that allow C2 as well as detailed near-real-time monitoring.
[33] Operators are cross-trained personnel that actively perform C2 and analytic functions directly connected to UCS and BCS.
[34] There is no Threshold-Objective trade space for IA Compliance, The Threshold equals the Objective.
[35] Meta-data is data about data. It allows another entity such as business AISs to discover the format and access rules of the data produced by Smart Grid. This in turn provides a common method of access such that multiple custom interfaces between AISs no longer have to be designed, built and supported.
[36] This refers to designing energy efficiency in to the equipment that supports Smart Grid, i.e. server virtualization and Direct Current (DC) for IT/OT equipment.

6.2 Key System Attributes (KSAs)

KSAs are a subset of the performance parameters of a system or capability. KSAs are a prioritized list of the most important attributes that characterize the desired system or capability.

Table 3 - Key System Attributes (KSAs)

Functional Capability	ID	Key System Attribute (KSA)	Development Objective
1.1.2	KSA-1	Common data elements accessed by external AIS	Standards-based and common data language
1.1.1, 1.1.3,1.1.4 ,1.1.6	KSA-2	Integration of new systems into the Common Operating Picture[37] (COP)	Develop an enterprise COP standard
1.1.2,1.1.4	KSA-3	Information displayed on business dashboards[38] allow for effective business-based decisions	Supports comprehensive report generation[39]
1.1.3	KSA-4	Open System Architecture framework compliance	Complete framework document [9]
1.1.3	KSA-5	Unified Facilities Criteria (UFC) Standards compliance and Unified Facility Guide Specifications (UFGS)	Guidance Established
1.1.5	KSA-6	Reciprocal accreditation approval for DoD	
	KSA-7	Sustainment - Reliability	
	KSA-8	Sustainment – Total Ownership Cost[40]	

[37] COP is defined as single identical display of relevant [operational] information shared by more than one command. A COP facilitates collaborative planning and assists all echelons to achieve situational awareness.

[38] Business dashboards present fusion of data from multiple AIS. Data fusion is the process of integration of multiple data and knowledge representing the same real-world object into a consistent, accurate, and useful representation.

[39] Measured and monitored according to the Test and Evaluation Master Plan (TEMP) as defined in Appendix E.

[40] See Section 15 – Program Affordability for a discussion of evaluating Total Ownership Cost

7. Family of System and System of System Synchronization

With the Task Force Energy focus on fleet energy systems, and the effects shipboard systems have on shore energy systems when in port, a synchronization between Smart Grid and fleet systems must be considered; fleet energy dependencies on the shore energy Smart Grid as well as Smart Grid dependencies on the fleet energy systems.

8. Information Technology and National Security Systems Supportability

This capability's data will be made accessible on the GIG through the DISA Net-Centric Enterprise Services (NCES) by complying with the Net Ready KPPs.

The goal is to provide ICS historical data, with as little delay as possible from the sub-systems collecting the data, to the GIG in keeping with the NCDS post-before-process strategy. Smart Grid data will be accessible on the GIG through the DISA Net-Centric Enterprise Services by complying with the Net-Ready KPPs.

9. Intelligence Supportability

A number of cyber intelligence, reporting and critical infrastructure mechanisms are available to help protect Smart Grid from a growing number of threats. Among these are:

- Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) shares control systems-related security incidents and mitigation measures.
- U.S. Cyber Command (CYBERCOM) Information Assurance Vulnerability Management (IAVA) which, among other duties, provides access to vulnerability notifications.

10. Electromagnetic Environmental Effects (E3) and Spectrum Supportability

10.1 Radio Frequency (RF) Authorization

All Radio Frequency (RF) transceiver installations shall be coordinated through the FECTL and Frequency Coordinator for the RCAoA in accordance with OPNAVINST 2400.20F Electromagnetic Environmental Effects (E^3) and Spectrum Supportability Policy and Procedures. An approved DD Form 1494 for the system is required prior to operation within CONUS and US Territories. Additional coordination is required for all non-US installations.

10.2 Electromagnetic Interference (EMI)

The ICS-PE shall conform to MIL-STD-461E for electromagnetic interference. The component performance shall not be degraded by ambient or intentional EMI from other RF emitters. In addition, ICS-PE components shall not produce adverse effects in other RF devices. Any RF transmitter in the design shall meet all requirements for and be certified for Hazards of Electromagnetic Radiation to Ordnance (HERO), Hazards of Electromagnetic Radiation to Fuel (HERF), and Hazards of Electromagnetic Radiation to Personnel (HERP).

11. Assets Required to Achieve Initial Operational Capability (IOC)

The performance of Smart Grid in meeting the goals is dependent upon the state of repair of the controlled equipment and the degree to which sensors and controls are applied to that equipment. This may often require the reevaluation of the utility grids themselves; components and subcomponents.

Required assets for achieving IOC will be provided in the Program Plan.

12. Schedule and IOC and Full Operational Capability (FOC) Definitions

12.1 KPP Objective & Threshold Relationship to IOC

The overarching purpose of the objectives and thresholds is to allow a "range" of systems that can be connected to the Smart Grid. The minimum or "threshold" is the baseline requirement that mandates 100% of AMI consumption data and some AMI and ICS data, chosen by building criteria & funding decisions. The objectives allow for additional ICS & building connections to the Smart Grid beyond what is chosen for threshold, but also bounds connections to just ICS. The incremental acquisition strategy provides flexibility for scheduling and funding of work scope over shorter or longer periods of time.

12.2 IOC Definition

Two increments of the ICS Platform Enclave (ICS-PE) will support the KPP Thresholds for IOC:

- Increment 1 provides a secure enclave for the safe transport of AMI data to Circuits via the PSNET transport.
- Increment 2 adds security capability to the enclave to accommodate the integration of the Industrial Control Systems and SCADA. (again, this involves only a subset of ICS depending on funding decisions)

Installations will be prioritized and scheduled to align with the AMI installation schedule and IAW budget decisions via the POM Budget process.

In order to 'claim' achievement of IOC, each installation must:

1. Demonstrate all KPP thresholds via successful execution of a test plan.
2. Achieve ICS-PE and ICS Common Architecture (ICS-CA) accreditation
3. Training in place for ICS Platform support and sustainment.
4. Training in place to maintain and operate AMI systems and to analyze AMI data.
5. All necessary maintenance and warranty contracts in place to sustain and support all connected UCS (AMI and SCADA), BCS, and ICS Platform Enclave.

The following summarize the capabilities reached at IOC:

1. The real-time ability to efficiently collect, transport, and integrate installation-level energy consumption and load demand information.
2. The real-time ability to analyze, determine and deploy the most appropriate actions that will reduce Installation-level energy consumption.

3. The near-real-time ability to identify energy system losses, faults, and business opportunities to execute Installation-level actions to reduce energy costs, reduce utility system(s) energy loss and/or consumption, and/or improve reliability, initial demand side management, and targeted commissioning activities.

12.3 FOC Definition

FOC will be achieved when projected cost savings are achieved.

13. Other DOTMLPF and Policy Considerations

The Join Capabilities Integration Development System (JCIDS) process defines a mnemonic that enables planners to consider issues of involving combinations of; doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF).

13.1 Policy Considerations

The following policies support or drive the supported command's goals and the capabilities described in this document;

- OPNAVINST 4100. 5E (Shore Energy Management)
  Navy Shall "Develop and utilize an integrated system which links infrastructure maintenance and recapitalization systems with energy management and distribution systems to realize even greater efficiency through improved requirements identification, demand management and condition-based maintenance."
- Public Law 110-140, Energy Independence and Security Act of 2007, compliance to a 30% energy efficiency increase by 2015
- National Defense Authorization Act of 2010 with a goal of 25% renewable energy production by 2025
- National Defense Authorization Act of 2011
- National Defense Authorization Act of 2012
- NDAA Excerpts
  - 335 - Energy security on Department of Defense installations
  - 2841 - Adoption of unified energy monitoring and utility control system specification
  - 2843 - Department of Defense participation in programs for management of energy demand or reduction of energy usage during peak periods, for military construction and military family housing activities.
  - 2845 - Study on development of nuclear power plants on military installations.
  - 2846 - Comptroller General report on Department of Defense renewable energy initiatives, including solar initiatives, on military installations
  - 2867 – Energy monitoring and utility control system specification for military construction and military family housing activities
  - 3105 – Energy Security and Assurance
- SECNAVINST 4101.3 of 3 FEB 2012, DoN Energy Program for Security and Independence Roles and Responsibilities
- EPACT 2005 requiring advanced metering and annual energy audits by 2012
- Executive Order 13423 of January 24, 2007 – Strengthening Federal Environmental, Energy, and Transportation Management
- UFC 3-400-10N Mechanical Engineering – Direct Digital Controls
- DoD Instruction 4170.11 Installation Energy Management
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards CIP-001 through CIP-009

- Executive Order 13327 Real Property Asset Management that promotes efficient spending to support agency operations.
- CNO, SECNAV, and ASN guidance on energy conservation and workforce efficiency

13.2 Operational Availability (A_o)
In general, Operational Availability can be described by the equation

A_o = System Up Time / Total Time

Because Smart Grid systems have dramatically different operational profiles, the measurement and interpretation of A_o varies from system to system. For purposes of A_o measurement and analysis, Smart Grid systems are divided into two classes (defined in terms of the way system is used):

- Continuous-use systems: Systems that are (nearly) always in use on a daily basis.
- Intermittent-use (non-continuous or on-demand) systems: Systems that have relatively long periods of standby or inactivity between uses.

Smart Grid is considered a continuous use system. For continuous-use systems, mean calendar time between failure is identical to mean operating time between failure, and use of Meat Time Between Failures (MTBF) in the A_o equation is consistent with the notion of measuring uptime in terms of calendar time. This notion is critical since all downtime is measured in calendar time. Therefore, the following equation provides an acceptable approximation of A_o in terms of reliability, maintainability and supportability.

$$A_o = \frac{MTBF}{MTBF + MTTR + MLDT}$$

13.2.1 Mean Time Between Failures (MTBF)
For a particular interval, the total functional life of a population of an item divided by the total number of failures within the population. The definition holds for time, rounds, miles, events, or other measures of life unit.

13.2.2 Mean Time To Repair (MTTR)
MTTR is a basic technical measure of maintainability - the average elapsed time (clock hours) for corrective maintenance (including testing times for fault detection, isolation and verification of correction).

13.2.3 Mean Logistics Delay Time (MLDT)
The average time a system is unavailable due to logistics system delays associated with the maintenance action.

13.3 Centralization – Optimal Theatre of Operations Concept
Since an industrial controls network is unlike a business network in that it is a many-to-few connectivity with few users and localized raw data usage, it makes more sense to locally (region) manage the network. Additionally the support requirements for ICS sub-

systems are very dependent on the specific sub-system. Optimal ICS network management becomes more difficult and poses an increasing risk of interruption of service as it encompasses a larger theatre of operations.

13.3.1 Smart Grid Enclave Management

Roles and Responsibilities for the Navy's current transport supporting Smart Grid and for Smart Grid enclave management are detailed in the *Enterprise Interconnection Security Agreement Between CNIC PSNet and NAVFAC for the Platform Network and Industrial Control Systems*, v2.5, dated 1 DEC 2011. This document serves as an example of an Interconnect Agreement (ICA) between Smart Grid and a transport provider.

Smart Grid is 'transport-agnostic', meaning that the Smart Grid enclave can utilize any approved transport between installations within an RCAoA and functions within the enclave are independent of the transport. This allows maximum flexibility for Navy and Marine Corps RCAoAs to take advantage of available transport services.

13.3.2 Automated Network Auditing

Host Based Security Systems (HBSS) were initially thought to be largely incompatible with ICS sub-systems. An effort to meet CTO 10-02 and FRAGORD 13 CHANGE 3 initiated a wide-spread implementation of HBSS with HIPS in protect mode and a POA&M to bring it from 90% compliance to 100% compliance within six months.

The HBSS implementation is hierarchical and in keeping with the HBSS CONOPS: having agents report from within the privately IP-addressed ICS Enclave to the HBSS ePolicy Orchestrator (ePO) server within the ICS Enclave DMZ, which in turn reports upward to an IA/CND Suite ePO server outside of the ICS Enclave.

13.3.3 System Update Services

System update services shall be managed within the Optimal Theatre of Operations Concept outlined above. ICS sub-systems are exceptionally prone to failure when the OT environment changes. All updates to Operating Systems (OS) and operation software must go through RCAoA-local test and validation before being pushed to sub-systems within the RCAoA ICS Enclave. It is a high risk process to automatically push updates to operational sub-systems. The sub-system operations OT manager should pull the update from the enclave patch repository server that has retrieved it from the external source once test and validation is complete.

13.4 NERC Standards

Certain select NERC standards may be applicable to Smart Grid. The North American Electricity Reliability Corporation (NERC) is responsible for developing and enforcing standards for bulk power industry participants. One of the criteria for falling under these standards is transmission-level voltage control. For sites that fall under NERC Critical Infrastructure Protection (CIP) requirements, an evaluation shall be made to identify corrective actions and costs associated with meeting these requirements. Transport characteristics shall not prohibit meeting NERC CIP requirements.

Additionally NERC provides a framework for system operator training and for timely sharing of information related to cyber security through its Electricity Sector Information Sharing and Analysis Center (ES-ISAC) designed to increase the flow of cyber and threat information between government and private industry.

13.5 Mobile Utility Support Equipment (MUSE)

MUSE is transported and used internationally for support of a variety of operations. Integration of MUSE as components of Smart Grid may require consideration.

14. Other System Attributes

14.1 Risk Management through Sub-system Partitioning

Compartmentalization within the ICS-P, while retaining both optimal operational efficiency and visibility for intrusion detection, is necessary for isolating the effects of technical failures, human error and malicious intrusion or disruption. NAVFAC Command Information Office (CIO) has developed an Enterprise ICS-P that includes extensive VLAN partitioning intended to meet IA and cyber security requirements and industry best practices.

14.2 Contingency Planning

Per DON Contingency Plan Message 291600ZFEB, a Contingency Plan shall be developed and reviewed for compliance with NIST Computer Security Special Publication 800-34: Contingency Planning Guide for Information Technology Systems, the DOD 8500.2, and corresponding IA controls designated by the system's Mission Assurance Category (MAC) and Confidentiality Level (CL).

The contingency plan for the network administration for the ICS is broken into two sections; Equipment Failure and Disaster Recovery.

The contingency plan elements:

- Will describe the interim measures used to recover and restore the ICS Enclave following an emergency or system disruption.
- Will provide specific guidance to the site Information Assurance Manager (IAM) on the system requirements for recovery from a disruptive event or emergency that can be incorporated into the site's contingency and COOP plans.
- Will be exercised (tested) at least every 12 months for MAC II and MAC III systems.

The most critical components are those that are required to maintain operation of sub-systems, specifically ICS-I, UCS and certain critical BCS.

Smart Grid survivability from natural disasters and extensive attacks such as Electromagnetic Pulse (EMP)[41], for which the electrical grid and control systems are

[41] U.S. Naval Institute Blog March 2010: The Return of EMP Threat Analysis

particularly susceptible to major disruption or destruction, should be analyzed. The risks from each should be evaluated based upon the site-specific architecture and identify mitigation plans, procedures and associated costs. Geomagnetic disturbances (GMD) can produce ground-induced currents that have effects similar in nature to the E3 component of EMP. Disruptions caused by geomagnetic storms have occurred many times in the past and resulted in the collapse of the Quebec Hydro grid in 1989.[42]

From the EMP Commission's Executive Report, page 35, vulnerabilities "*…are produced by the responses of the electronic control systems that provide and utilize the near-real-time data flows needed to operate the fuel/energy infrastructure efficiently, as well as to identify and quickly react to equipment malfunctions or untoward incidents. EMP could also cause control or data-sensor malfunctions that are not easily discernible, leading to counterproductive operational decisions.*"[43] And from page 27; "*The wireless system [telecommunications] is technologically fragile in relation to EMP, certainly in comparison to the wired one. In general, it may be so seriously degraded in the EMP region as to be unavailable."*

14.3 Training

Smart Grid requires a level of interoperability and integration for which our present workforce does not have sufficient training. The core component of efficient and effective Smart Grid is operations staff that performs the C2. The success of Smart Grid is highly dependent on these operators and their knowledge of both the theory behind the systems that they operate and the real world physical configuration of the systems for which they are responsible. Training of operational personnel must be defined such that the benefits of Smart Grid can be optimally realized while meeting all RCAoA-specific requirements.

Smart Grid maintenance personnel, who create and modify programming sequences in Smart Grid ECs, will require training in standardized sequences which utilize a plug-and-play approach, allowing easy incorporation of new code sequences into a well-defined Smart Grid.

All users and administrators of both ICS-I equipment and operational equipment must be properly trained and aware of all security and IA requirements promulgated by the command security manual and all other applicable security requirements/procedures. All administrators on the servers have been identified as having at least Operating System (OS) certification on these servers or equivalent work experience. Those who have access to operational ECs related to life-safety, such as protective relaying equipment, will need to have graduated from a training program prior to adjusting associated settings. Full compliance with DoD 8570.1, Information Assurance Training, Certification, and

[42] North American Electric Reliability Corporation report on the March 13, 1989 Geomagnetic Disturbance
[43] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, established pursuant to title XIV of the FY2001 NDAA and reestablished via FY2006 NDAA, Volume1: Executive Report, 2004

Workforce Management is required. Training of site safety procedures for personnel operating the equipment will conform to site rules and regulations.

Operational training must be defined such that the benefits of Smart Grid can be optimally realized while preserving the RCAoA-specific requirements and workforce limitations.

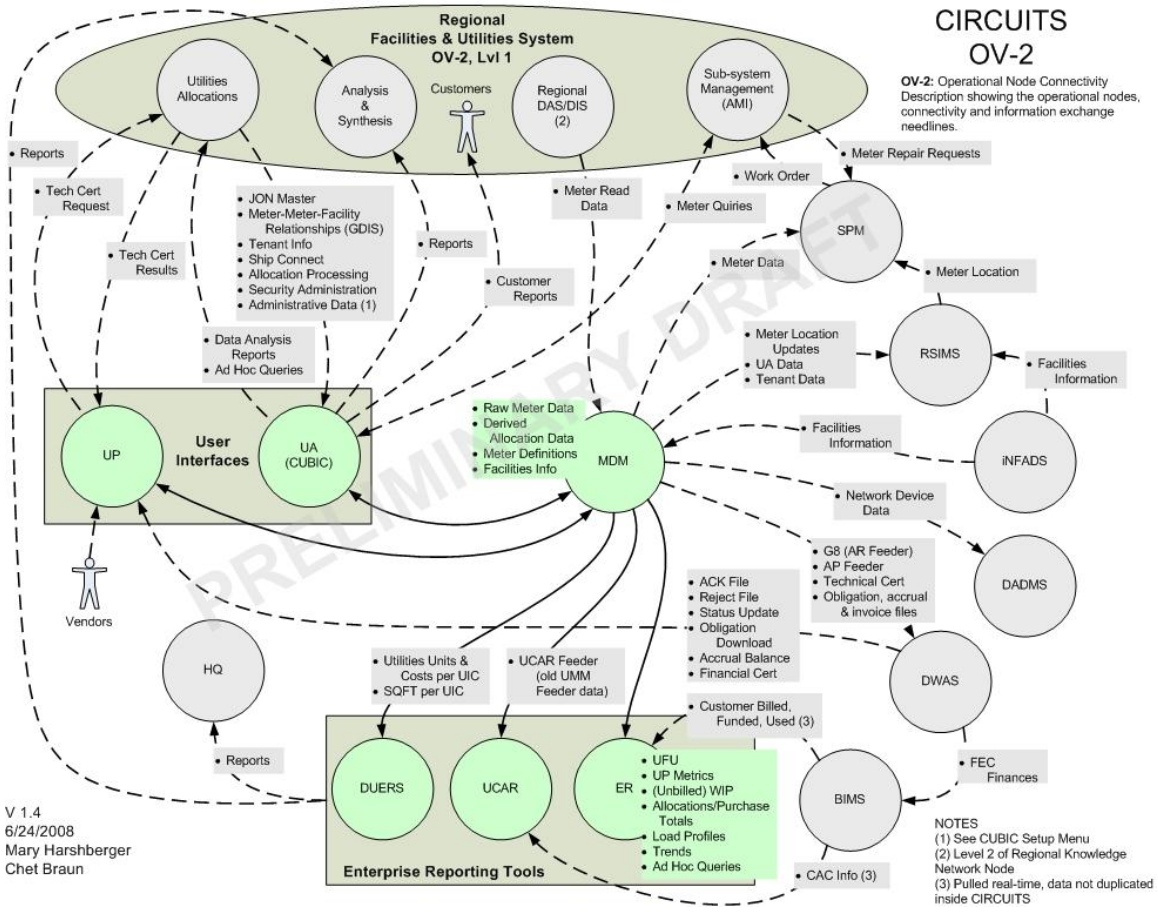
15. Program Affordability

This section is government program office specific and has been removed for public release.

Appendix A – Architecture Products

This section is government program office specific and has been removed for public release.

Figure 11 - CIRCUITS OV-2



Appendix B – References

[1] "Hacker jailed for revenge sewage attacks" http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

[2] "Slammer worm crashed Ohio nuke plant network" http://www.securityfocus.com/news/6767

[3] "California hack points to possible IT surveillance threat" http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html

[5] SCADA Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems" http://www.fas.org/irp/congress/2005_hr/scada.pdf

[6] "Terrorist Interest in Water Supply and SCADA Systems," National Infrastructure Protection Center, Information Bulletin 02-001, January 30, 2002.

[7] "Cyber-Attacks by Al Qaeda Feared" http://washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26

[8] Federal Technical Support Working Group (TSWG)'s "Sustainable Security for Infrastructure SCADA" http://www.tswg.gov/tswg/ip/SustainableSecurity.pdf

[9] *A NAVFAC Industrial Controls Systems Common Architecture Framework*, v1.4, 2013, Chet Braun.

Appendix C – Methodology and Results of the Analysis

This section is government program office specific and has been removed for public release.

Appendix D – Acronym List

AIS	Automated Information System
AMI	Advanced Metering Infrastructure
ATO	Authority to Operate
BCS	Building Control System
CA	Common Architecture
C&A	Certification & Accreditation
CIRCUITS	Centralized and Integrated Reporting for the Comprehensive Utilities Information Tracking System
CNIC	Commander Navy Installations Command
DAA	Designated Approval Authority
DADMS	Defense Application and Database Management System
DAS	Data Acquisition System (part of the Enterprise Metering Program)
DDC	Direct Digital Control
DISA	Defense Information Security Agency
DMZ	De-Militarized Zone
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities
EC	Equipment Controller
EMCS	Energy Management & Control System
EMS	Energy Management System
ENE	Enterprise Network Exception
EPAct05	Energy Policy Act of 2005
FPOC	Facility Point of Connection
GIG	Global Information Grid
GOGO	Government Owned, Government Operated
GUI	Graphical User Interface
HVAC	Heating, Ventilation and Air Conditioning
IA	Information Assurance
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Alert
IOC	Input/Output Controller
IT	Information Technology
KPP	Key Performance Parameter
KSA	Key System Attribute
MAN	Metropolitan Area Network
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NMCI	Navy Marine Corps Intranet
ODAA	Operational DAA
OSA	Open Systems Architecture
OT	Operational Technology
PIT	Platform IT
PITI	Platform IT Interconnect
PoP	Point of Presence
PRA	Platform IT Risk Assessment
PSNet	Public Safety Network (communications transport for NAVFAC AMI/ICS)
SC	Supervisory Controller
SCADA	Supervisory Control and Data Acquisition
SIP	System Information Plan
SIPRNet	Secret Internet Protocol Router Network
SoS	System of Systems
STIG	Security Technical Implementation Guide
UCS	Utility Control System

Appendix E – DoDD 5000 Program Lifecycle Products

This section is government program office specific and has been removed for public release.

Appendix F – Smart Grid IA Security Risks Summary

Security Risks	Amplification of Risks
Physical Security	Given the operational nature of ICS and the networks that connect them, unauthorized physical access provides an entry point for malicious attacks and is deemed high risk
1. Network	Physical access to network ports enabling unauthorized network access and possible contamination of networked resources
2. ICS Controllers	• Malicious injection of commands onto base-wide ICS • Malicious code execution on ICS Controllers • Manipulation/overwrite of ICS Controller Firmware
3. Controlled Equipment	Physical access to certain critical infrastructure equipment could result in significant damage and Public Safety issues
Network Security	Ineffectively implemented network environments may result in an ICS environment that does not meet IA requirements
1. Eavesdropping on communications between ICS Controller and Server	Monitoring of ICS operational parameters for future exploits such as replay attacks and simulated commands
2. Man-in-the-Middle Attack	Malicious code injected onto the network from Operator Workstations, field controllers, AMI meters, or ICS Server may launch attacks on base-wide ICS
3. Denial of Service on ICS Component	Compromised Operator Workstations may serve as launch points for DoS attacks on key ICS components
4. Inter-base Transport Boundary Security	Unauthorized and malicious access to the transport from compromised ICS environment and to ICS from a compromised transport
5. Security enclave boundaries within ICS	Unauthorized and malicious access / control of other ICS controllers from compromised Operator Workstations, Laptops or ICS controllers
6. Mitigations to exceptions required for older ICS components.	Easy compromise of insecure Ethernet capable ICS devices may result in unauthorized and malicious access/control of other ICS controllers from the compromised ICS controllers
7. Malicious software and virulent infestation of ICS Operator Workstations and Servers	Ineffective IA controls and management of ICS computing environment could result in non-compliant IA environment
8. Continuous availability of ICS platform for Base Operations	Ineffective network management environment could result in critical ICS network components becoming unavailable thereby degrading ICS mission
ICS Operations	A reasonable balance of ICS operational and Information Assurance risks must be achieved to ensure the most effective ICS operational capability
1. Effective ICS C2 Situational Awareness	Use of multiple ICS Command & Control platforms may result in malicious activity going undetected and mitigated
2. Continuous availability of ICS Command & Control environment	Wide-area (site-to-site) network outage may degrade portions of the ICS Command & Control environment and result in temporary loss of C2 capability

Appendix G – EISA 2007

EISA 2007 Section 1301 ten parallel activities:

1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. Dynamic optimization of grid operations and resources, with full cyber-security.
3. Deployment and integration of distributed resources and generation, including renewable resources.
4. Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.
5. Deployment of ‘‘smart’’ technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.
6. Integration of ‘‘smart’’ appliances and consumer devices.
7. Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.
8. Provision to consumers of timely information and control options.
9. Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.
10. Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services.

Appendix H – Reference Drawing

Figure 12 is a sample of a customer dashboard that provides management information content external to the C2 functions of Smart Grid.

Figure 12 - Sample Customer-level Dashboard

Appendix I – Navy Criteria for Connection to Smart Grid

This section is government program office specific and has been removed for public release.