John Mochulski and Rick Silverman

Information Assurance (IA) for Power Conversion Modules (PCMs) for Next Generation Integrated Power Systems

Abstract

The Navy is embarking on the development of the Next Generation Integrated Power System (NGIPS). The NGIPS will continue to meet the power and affordability needs of the fleet and intelligently control electric power. This NGIPS utilizes the Power Conversion Module (PCM) to provide conditioned electric power to the electric loads throughout the ship. In the past, naval power systems operated on closed networks. But now, as open standards such as Ethernet, TCP/IP and web technologies become more standard, the Machinery Control System (MCS) and connected Hull, Machinery and Electrical (HM&E) equipment must address cyber security concerns. This paper will explore the current state of the Information Assurance (IA) controls for the PCMs and will identify the threats and safeguards that will be required to protect future PCMs as the MCS continues to evolve.

MCS Overview

Today's Navy cruisers and destroyers are equipped with an MCS which provides supervisory control and monitoring of machinery systems, including: the propulsion plant, electric power plant, auxiliary systems, and damage control systems.[1] The MCS controls and monitors power for sensors, computers, navigation systems and weapons to operate the ship. Over the past three decades, the MCS has moved from hardware-based logic to software-based logic. Also, with the development of Integrated Fight Through Power (IFTP) PCMs to support DDG-1000 over the last decade, the MCS now has the potential to enable more flexible, more survivable electric plant lineups for next generation ships to meet the increasing demand for power. These new capabilities will be based on distributed software architectures that capitalize on the MCS network and the embedded PCM software. These architectures are similar to what is becoming standard for industrial control systems. Unfortunately, with the increased dependency on software-based controls and network connectivity, comes the increased risk of cyber attacks.

Future naval power systems will continue to leverage current technology developed by the industrial control industry. Being that the MCS and associated PCMs are critical to the ship's operational ability, it becomes more important to implement IA controls in the design.

PCM in the MCS System Architecture

Before discussing the importance of IA controls, it is practical to discuss the design of the MCS. The MCS follows a multi-tiered architecture in its implementation. The three tiers are listed here and shown in Figure 1.

1) Information Layer
2) Network Layer
3) Control Layer

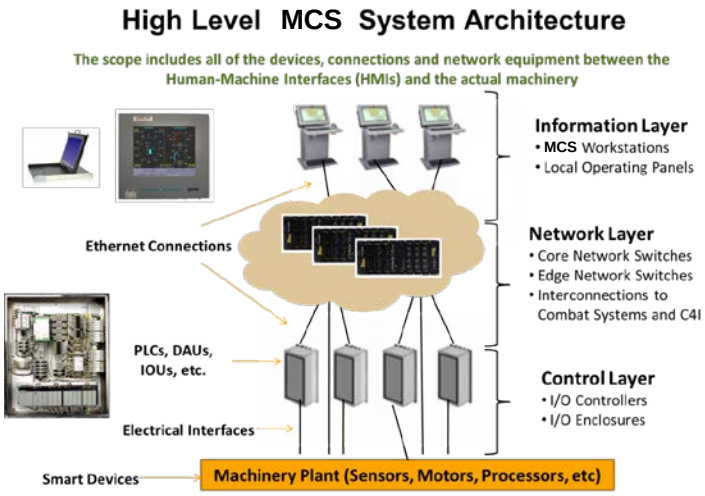

Figure 1: MCS System Architecture[2]

The Information Layer will include local and remote consoles to control and monitor the multiple systems and subsystems within the MCS. Each console will have a Human Machine Interface (HMI) to control and monitor all systems and subsystems. The local operating panels are either part of the equipment themselves or consist of a console nearby. The remote consoles will be located in the Central Control Station (CCS), the engine room or in the bridge. Some of the functions of the MCS will be performing information and alarm processing, formatting, scaling and transfer of control logic.

The Network Layer interconnects the Information and

the Control Layers via a ship-wide control system network. For the DDG-51s, this network is called the AN/USQ-82. This layer consists of a network which routes messages using the best path available. More details will be discussed on this layer in the next section.

The Control Layer consists of processing equipment that provides control, monitoring, and processing of the MCS sub-systems. This layer will be responsible for processing commands from the Information Layer via the Network layer and sending back alarm and status information. The hardware architecture for the Control Layer in the MCS will be PLC (MIL-PRF-32006) or VME (in accordance with IEEE 1014). The Power Conversion Module (PCM) is located at the Control Layer as the MCS provides supervisory control. Though PLCs are often used in industrial control systems, the MCS primarily uses VME and other embedded controllers.

MCS Family of Networks

The first ship of the class, the DDG-51 Arleigh Burke, was designed with a Data Multiplex System (DMS). The DMS network interconnected the distributed controls across the ship.[2] DMS was a fast-circuit-switched network. The time that it took to send or receive a DMS data packet was very short – typically only a few microseconds (μS), and at most, 68.4 milliseconds. For short sessions, typical of control system traffic, the DMS design supports low latency data transfer and good bandwidth utilization. The speed of the DMS network was at 24 Mbps and utilized circuit switching.[3]

The DMS backbone network was updated to a redundant fiber optic ring system called the Fiber Optic Data Multiplex System (FODMS). One of the important features of the FODMS was the ability to perform packet switching. The speed of the network increased to 100Mbps. FODMS also introduced fiber optic cabling to Aegis ships. When FODMS was introduced to DDG-51, 2400 circuits were supported. By the time of the ship's commissioning, that number had doubled. As the DMS system matured, the design of ships began to take advantage of the network's capabilities. FODMS provides connectivity for the MCS, Steering systems, sensors, actuators and other electrical components throughout the ship.

In 2002, talks began on upgrading the Aegis network to the Gigabit Ethernet Data Multiplex System (GEDMS). The Navy was looking for ways to further increase the system performance of the network. The speed of GEDMS was increased to 1 Gbps, and introduced to commercial off-the-shelf (COTS) interfaces and protocols such as Ethernet and the Internet Protocol (IP). By including these protocols the MCS became compatible with many commercially available power systems.

It is anticipated that a PCM for the future DDG-51 FLT III design will be connected to the Gigabit Ethernet Data Multiplex System (GEDMS). The primary purpose is to address increased power requirements for new sensors. As shown in Figure 2, the GEDMS interface allows many standard interface specifications that it is compatible with. These are:

1) MIL-STD-1397
2) NATO STANAG 4156
3) Ethernet
4) TCP/IP
5) UDP/IP
6) RS-422 with TCP/IP or UDP/IP
7) RS-485
8) Analog Voltage
9) Synchro 60Hz or 400Hz
10) Voltage Level Discrete

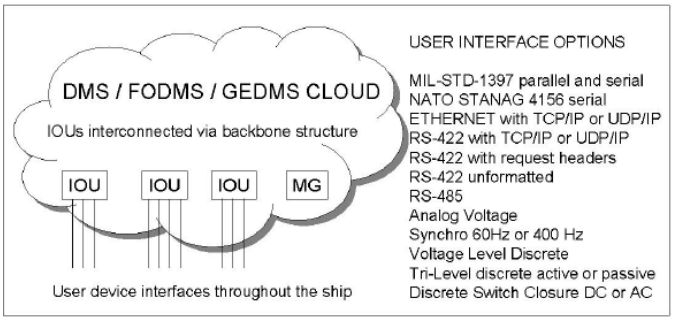

Figure 2: GEDMS Ship Interfaces

Current MCS IA Control Guidance

In this paper, the discussion will focus on IA controls for the PCM. All of the sub-systems shown in Figure 3, like the PCM, are part of the HM&E System. Each of them is considered sensitive for security concerns because they are all critical to the Ship's Mission. Information Assurance controls are applied to all of these systems to mitigate any security concerns.

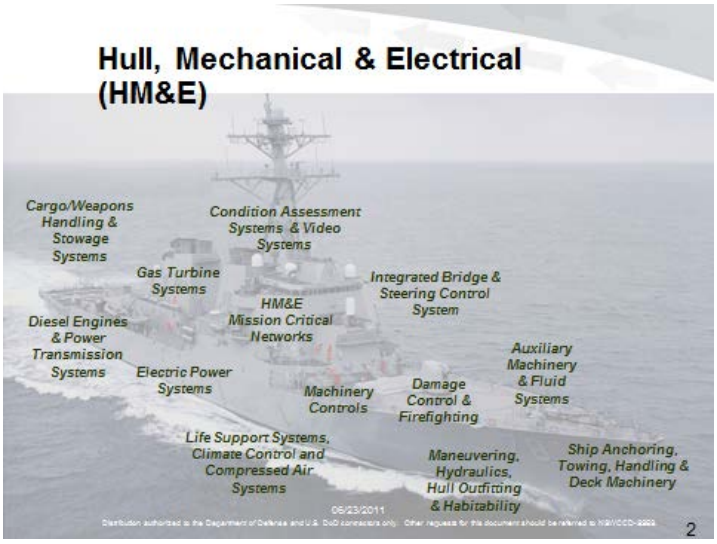

Figure 3: HM&E Systems requiring IA Controls[2]

As the MCS network evolves, Information Assurance controls will become of major importance, especially if MCS ever gets connected to classified networks. This will further the HM&E capability for the ship's mission.

Being in the digital age, we are constantly reminded of the cyber threats that can infect our digital systems. As the MCS matures, designers need to be cognizant of this cyber threat. The MIL-STD-X628 draft specification was written to help architect future MCS systems.[4] There are several requirements in this standard that address information assurance. This standard will provide guidance to those system engineers that will be developing requirements for the specifications within the MCS. As a note, these requirements are listed as "the MCS shall consider", meaning care in selection of each one should be scrutinized given all factors. Here is a list of requirements taken from MIL-STD-X628 which address Information Assurance.

1. Physical security shall consider, but not be limited to:
    a. Proper signage of equipment
    b. Locked enclosures for primary control elements
    c. Enclosures with intrusion detection
    d. Obstructed or removed external ports
2. Network security shall consider, but not be limited to:
    a. Disabling unused ports
    b. Port-based security
    c. Media Access Control (MAC) based security
    d. Disabling unused services and protocols
    e. Default security parameters
    f. Secure network protocols
    g. Intrusion detection
3. Controller (PLC) security shall consider, but not be limited to:
    a. Password authentication
    b. Login failure lockout
    c. Password failure lockout
    d. Code protection
    e. Control firmware validation
    f. Digital signatures
4. Console/computing security shall consider, but not be limited to:
    a. User access
    b. Application white-listing
    c. Operating system patching
5. Application security shall consider, but not be limited to:
    a. Virus scanning
    b. Secure coding standards
    c. Application authentication
6. System security shall consider, but not be limited to:
    a. Virus scanning
    b. Change logs
    c. User authorization
    d. Password standards
    e. Vendor default modifications
    f. Disabling or removal of unused ports
    g. Protocols
    h. Software features
    i. Information Awareness (IA) training
7. External interface security shall consider, but not be limited to, firewalls.
8. Supply chain security shall consider, but not be limited to, U.S. parts only.
9. The MCS design shall be implemented in consideration of the above security measures and in accordance with the NAVSEA 9400.2-M and DOD (Department of Defense) Instruction 8500.2.[9]

The DOD Instruction 8500.2 encompasses all components that are "DOD-owned or controlled information systems that receive, process, store, display or transmit DOD information". This statement is taken from the Applicability section of 8500.2.

Current DDG-51 IA Requirements

DDG-MOD (DDG-51 Modernization) is the modernization effort which is being performed on backfit DDG-51 ships. The backfit destroyers are the original design, with retrofits for new technology insertion. The first ship to complete the DDG-MOD

midlife hull, mechanical, and electrical upgrade, was the USS JOHN PAUL JONES, DDG53.

The DDG-MOD upgrade consisted of extensive changes throughout every compartment of the ship. Beginning in the spring of 2010, the local maintenance community and numerous contractors worked together with the ship's crew to install more than 70 ship alterations, 35 of which had never been done before. [5]

The engineering plant was remodeled around a new MCS, an interoperable computer design that expands the resources available to any given watchstander, reduces manning requirements, improves reliability, and cuts costs. The MCS software is accessible to the engineering watch team at any of the four universal control consoles, each of which are capable of monitoring and controlling every facet of plant operation. With MCS, the engineering officer of the watch has an unparalleled ability to run the plant.

DDG-MOD added virus checking software to each workstation. Virus definition updates are made regularly. This makes it seamless for the sailor to have the latest protection against cyber threats.

Information Assurance Guidance

As defined by Department of Defense Instruction (DODI) 8500.01E,[8] Information Assurance "provides measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation." Successful protection of DOD assets requires policy compliance and an understanding of the vulnerabilities humans face when interacting with information systems. [6]

There are 3 core principles of information security in the CIA Triad:

1. Confidentiality - Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
2. Integrity - Protection against unauthorized modification or destruction of information.
3. Availability - Timely, reliable access to data and information services for authorized users.[2]

To develop IA controls for the PCM, system engineers will apply guidance from the 8500.2 DIACAP (DOD Information Assurance Certification and Accreditation Process). DIACAP is the result of a National Security Agency (NSA) directed shift in underlying security paradigm. The DIACAP succeeds its predecessor: DITSCAP[7] on July 6, 2006. An overview of the DIACAP activities is shown in Figure 4. One major change in DIACAP from DITSCAP is the embracing of the idea of information assurance controls (defined in DODD 8500.1 and DODI 8500.2) as the primary set of security requirements for all automated information systems (AISs).

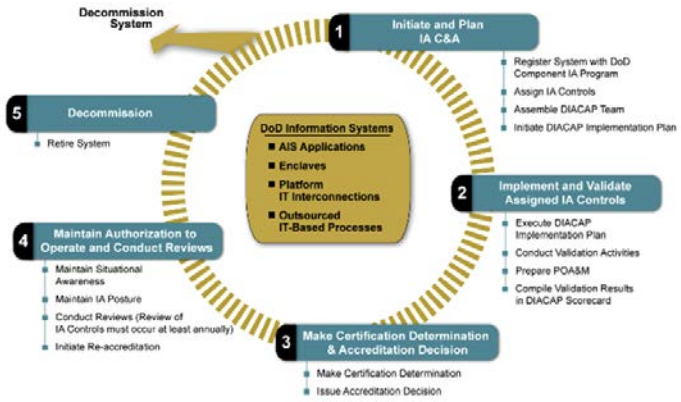

Figure 4: DIACAP Activities

DIACAP is a 3 part process. As show in Figure 5, the 3 parts are:

1) DODi 8510.01 Instruction
2) DIACAP Knowledge Service
3) Automated C&A Process

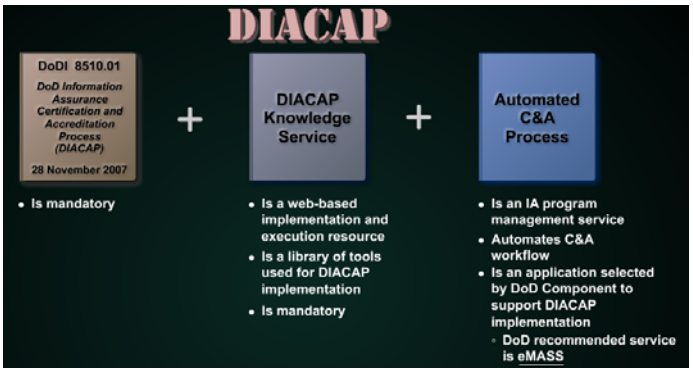

Figure 5: DIACAP – 3 Part Process

DIACAP Certification and Accreditation

The Certification and Accreditation (C&A) IA 8500.02 Controls directive established standards for certification of Navy mission systems. The process discloses what residual risk is acceptable to the mission. If the process determines that the IA controls chosen meet the C&A guidelines, then the system is accredited and approved.

As shown in Figure 6, Certification involves a comprehensive evaluation of both technical and non-technical security features.

The IA Controls are determined based on the system's mission assurance category (MAC) and confidentiality level (CL).[8]

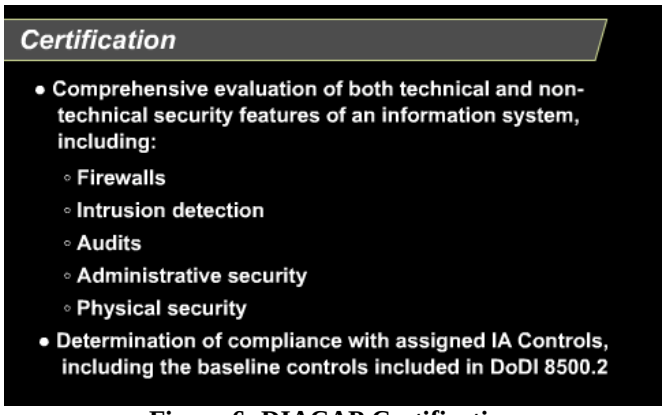

Figure 6: DIACAP Certification

The Mission Assurance Category is applicable to DOD information systems. The mission assurance category reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories: [9]

1) Mission Assurance Category I (MAC I). Systems handling - information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.
2) Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.
3) Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities

Confidentiality Level is used by the DOD to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has three defined confidentiality levels:

1) Classified
2) Sensitive and
3) Public.[9]

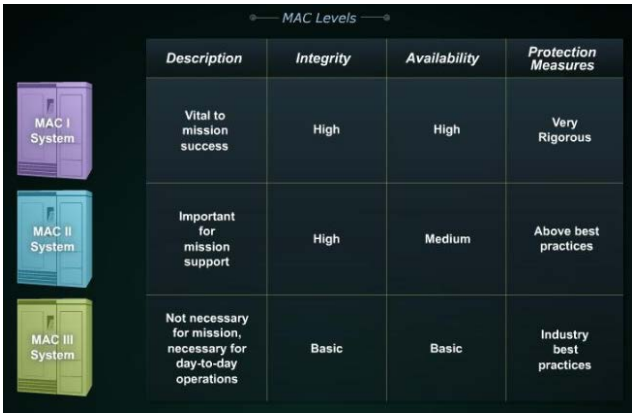

Figure 7: MAC – Mission Assurance Category

For the PCM in the MCS, the decision was that the information being transmitted on the Gigabit Ethernet Data Multiplex System (GEDMS) network would be vital to the operational readiness and mission effectiveness for the ship. This would give the PCM a Mission Assurance Category (MAC) of Level 1, or vital to mission success.

Since the information involved on the MCS is not Classified, the Confidentiality Level would be set to Sensitive. By following the 8500.02 spreadsheet, there are several considerations to implement IA for the PCM. These controls are listed in the following Table.

The column "PCM Included" states those IA controls that would be recommended for inclusion for the PCM.

Table 1- List of 8500.02 Information Assurance Controls

Control Number	PCM Included	Control Name	Control Number	PCM Included	Control Name
COAS-2	x	Alternate Site Designation	ECID-1		Host Based IDS
COBR-1	x	Protection of Backup and Restoration Assets	ECIM-1		Instant Messaging
CODB-3	x	Data Backup Procedures	ECLO-1	x	Logon
CODP-3	x	Disaster and Recovery Planning	ECLP-1	x	Least Privilege
COEB-2		Enclave Boundary Defense	ECML-1		Marking and Labeling
COED-2		Scheduled Exercises and Drills	ECMT-1		Conformance Monitoring and Testing
COEF-2	x	Identification of Essential Functions	ECND-2		Network Device Controls
COMS-2	x	Maintenance Support	ECNK-1		Encryption for Need-To-Know
COPS-3	x	Power Supply	ECPA-1	x	Privileged Account Control
COSP-2	x	Spares and Parts	ECPC-2	x	Production Code Change Controls
COSW-1	x	Backup Copies of Critical SW	ECRC-1	x	Resource Control
COTR-1		Trusted Recovery	ECRG-1	x	Audit Reduction and Report Generation
DCAR-1		Procedural Review	ECRR-1	x	Audit Record Retention
DCAS-1	x	Acquisition Standards	ECSC-1	x	Security Configuration Compliance
DCBP-1	x	Best Security Practices	ECSD-2	x	Software Development Change Controls
DCCB-2	x	Control Board	ECTB-1	x	Audit Trail Backup
DCCS-2		Configuration Specifications	ECTC-1		Tempest Controls
DCCT-1		Compliance Testing	ECTM-2	x	Transmission Integrity Controls
DCDS-1		Dedicated IA Services	ECTP-1	x	Audit Trail Protection
DCFA-1	x	Functional Architecture for AIS Applications	ECVI-1		Voice-over-IP (VoIP) Protection
DCHW-1	x	HW Baseline	ECVP-1	x	Virus Protection
DCID-1	x	Interconnection Documentation	ECWM-1	x	Warning Message
DCII-1		IA Impact Assessment	ECWN-1		Wireless Computing and Network
DCIT-1		IA for IT Services	IAAC-1	x	Account Control
DCMC-1		Mobile Code	IAGA-1	x	Group Authentication
DCNR-1		Non-repudiation	IAIA-1	x	Individual Identification and Authentication
DCPA-1		Partitioning the Application	IAKM-2		Key Management
DCPB-1	x	IA Program and Budget	IATS-2		Token and Certificate Standards
DCPD-1	x	Public Domain Software Controls	PECF-1	x	Access to Computing Facilities
DCPP-1	x	Ports, Protocols, and Services	PECS-1		Clearing and Sanitizing
DCPR-1	x	CM Process	PEDI-1		Data Interception
DCSD-1	x	IA Documentation	PEEL-2		Emergency Lighting
DCSL-1		System Library Management Controls	PEFD-2		Fire Detection
DCSP-1		Security Support Structure Partitioning	PEFI-1		Fire Inspection
DCSQ-1	x	Software Quality	PEFS-2		Fire Suppression
DCSR-2		Specified Robustness - Medium	PEHC-2	x	Humidity Controls
DCSS-2	x	System State Changes	PEMS-1	x	Master Power Switch
DCSW-1	x	SW Baseline	PEPF-1	x	Physical Protection of Facilities
EBBD-2		Boundary Defense	PEPS-1	x	Physical Security Testing
EBCR-1	x	Connection Rules	PESL-1		Screen Lock
EBPW-1		Public WAN Connection	PESP-1		Workplace Security Procedures
EBRP-1	x	Remote Access for Privileged Functions	PESS-1		Storage
EBRU-1	x	Remote Access for User Functions	PETC-2	x	Temperature Controls
EBVC-1	x	VPN Controls	PETN-1	x	Environmental Control Training
ECAD-1		Affiliation Display	PEVC-1	x	Visitor Control to Computing Facilities
ECAN-1	x	Access for Need-to-Know	PEVR-1	x	Voltage Regulators
ECAR-2	x	Audit Record Content – Sensitive Systems	PRAS-1	x	Access to Information
ECAT-2	x	Audit Trail, Monitoring, Analysis and Reporting	PRMP-1	x	Maintenance Personnel
ECCD-2	x	Changes to Data	PRNK-1	x	Access to Need-to-Know Information
ECCR-1	x	Encryption for Confidentiality (Data at Rest)	PRRB-1	x	Security Rules of Behavior or Acceptable Use Policy
ECCT-1	x	Encryption for Confidentiality (Data at Transmit)	PRTN-1	x	Information Assurance Training
ECDC-1	x	Data Change Controls	VIIR-2	x	Incident Response Planning
ECIC-1	x	Interconnections among DOD Systems and Enclaves	VIVM-1	x	Vulnerability Management

DIACAP Knowledge Service

The DIACAP Knowledge Service is a website portal managed by the Navy to provide up to date information for Information Assurance certification and accreditation. This portal is a central repository for all DIACAP related information. [10]

Of most importance, the DIACAP portal provides the definition of each IA control, along with the validation procedure for each control. These validation procedures are required to certify the system under DIACAP. As shown in Figure 8, there are 8 categories of a total of 157 IA Controls.

Abbreviation	Subject Area Name	Number of IA Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

Figure 8: DIACAP IA Controls

Each description and validation procedure is described on the portal and is kept current. The use of the DIACAP Knowledge Service is required for the DIACAP certification process.

Automated C&A Process

The DIACAP Knowledge service lists eMASS as the automation service to satisfy Certification and Accreditation. The Enterprise Mission Assurance Support Service (eMASS) is a government owned web based application, which provides visibility and automation of IA Program Management processes. eMASS enables IA managers and senior decision makers at all enterprise levels to comprehend the scope and state of IA activities within the enterprise, which can assist in identifying IA requirements, developing policy, and making decision concerning acquisition and IA resources and programming.

Need for Information Assurance Controls

One of the most important reasons to implement IA controls is to prevent malware from infecting the MCS system. Malware stands for "MAL-icious soft-WARE", and will disrupt the normal operations of a control system. A particular malware, called Stuxnet, infected several industrial plants, worldwide, in 2008. Its name was derived from keywords buried in the code.[11] While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that subverted industrial systems. Stuxnet was discovered and analyzed by the Symantec Corporation, one of the world's largest anti-virus software companies. The initial attack occurred on Nov 20, 2008 and to date has infected over 60,000 host computers worldwide.

Stuxnet Malware – How it worked

The Siemens industrial control system that was infected by Stuxnet was similar to others SCADA (supervisory control and data acquisition software) systems that consist of several PLC controller boards. The PLCs communicate with a supervisory host. The host computer in this case was a PC using a Windows operating system. The PLCs are programmed from the Windows computer. These computers are usually not connected to the Internet or even the internal network. In addition, the industrial control systems themselves are also unlikely to be connected to the Internet. An example of the PLCs that were exploited by Stuxnet is shown in Figure 9.

Figure 9: PLC Controllers exploited by Stuxnet

The Stuxnet malware utilized a piece of Siemens software, called WinCC. Though not known, it is probable that Stuxnet was spread via an infected memory stick by plugging it into a computer's USB port. Once the virus is copied to the computer, it checks to see if WinCC is running. If it is, it tries to log in and install a clandestine "back door" to the internet. It then contacts a server in Denmark or Malaysia for instructions. If it cannot find WinCC, it tries to copy itself on to other USB devices. It can also spread across local networks via shared folders and print spoolers. The main idea is to reprogram the PLCs and drop the new code onto the PLCs

The methods used by Stuxnet are considered “zero-day vulnerabilities” and are not unusual in the cyber world. WinCC uses the PLC/STL rootkit to enable control of the Siemens industrial control system. The STL stands for the Statement List that runs inside the PLC. Once Stuxnet is installed inside the control system, attackers are capable of injecting code into the control system and will hide this code from the designers and operators. The term “rootkit” is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware. Once a system is “rooted”, the attacker can exploit full control over the day-to-day functionality of the physical industrial control system. Other ways that Stuxnet spread was by using methods as peer-to-peer RPCs (remote process calls) to other computers. The size of the Stuxnet malware was unusually large at half a megabyte in size which is irregular for malware. The Windows component of spread relatively quickly and indiscriminately and will be topic of many IA discussions to come.

Though Stuxnet infected a PLC-based system, it is also possible that this kind of malware could infect a VME-based or embedded-controller based system.

IA Controls – Implementing Industrial Controls to prevent the next Attack.

In this section, we would like to show what preventative measures and controls will be put in place for the PCM to maintain effective information assurance.

Preventing unauthorized personnel from installing software on a system

One of the controls listed in Table 1 that involves preventing unauthorized personnel from installing software onto the system is called IAAC-1, Account Control. The IA control IAAC-1 is in the category of Identification and Authentication. By following the process prescribed in the control, safeguards will be put in place to prevent unauthorized access to the PCM. There will be user authentication to verify that the user is certified to operate or maintain the equipment. Software should not be allowed to be modified except through strict controls. Some additional controls that would help in the area of Account Control are:

- Fingerprint recognition for user authentication
- Encrypted storage of user information in a secure database
- Inactive accounts will be automatically deactivated
- Use hard copy logs for sign-on and sign-off, Security Officer will compare with computer logs.
- Strict process control for upgrading software. Consider only allowing at local station for reprogramming PLC software. For the case of the PCM on the DDG-51 this also applies to VME and embedded controller software.

Design of Ports, Protocols, and Services in the PCM and Machinery Control System.

Relying on the DIACAP DCCP-1, Account Control, Ports, Protocols, and Services, controls will be put in place to identify network ports, protocols, and services they plan to use in the MCS. This should start as early in the deployment process as soon as possible. Examples of security measures to prevent unwanted access to these Ports and Services are:

- Intrusion detection systems
- VPN connections
- Firewall
- IPsec

In order to support these security measures, the information is saved in a protected description file. This file would contain the protocol, ports and system information that would be granted access to the network. For example, a firewall system would have to read a description file which contained ports, IP addresses and protocols. Those system resources which are not listed in the descriptor file, would be excluded from access.

Using anti-malware software to detect anomalies.

Bypassing the security software installed in many industrial control systems (ICS) can be inevitable. It is fruitful for any system to use anti-malware software to detect any anomalies installed on the system. Anomalous detection can occur anywhere within the ICS and can be independent of the PLC system.

In the case of the MCS and PCM, control data is already being fed back to the Power Manager. The concept would be to red flag data which looked like it was not behaving as a normal system. These data values may well be within the performance envelope of the ICS, but by taking historical snapshots of the data, patterns can be

recognized and captured in archived data which can be compared by anti-malware software.

Any deviations from predetermined data patterns would be flagged to the operator for maintenance inspection.

Industrial Control Systems Cyber Emergency Response Team

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors. ICS-CERT partners with law enforcement agencies and the intelligence community to coordinate efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. [12]

As more vulnerabilities are exposed in ICS applications, information needs to be collected, disseminated and distributed to prevent the next cyber-attack. As shown in Figure 10, these numbers are increasing at an ever increasing rate. The ICS-CERT team develops the long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts. ICS-CERT leads this effort by

- responding to and analyzing control systems-related incidents
- conducting vulnerability, malware, and digital media analysis
- providing onsite incident response services
- providing situational awareness in the form of actionable intelligence
- coordinating the responsible disclosure of vulnerabilities and associated mitigations
- sharing and coordinating vulnerability information and threat analysis through information products and alerts.

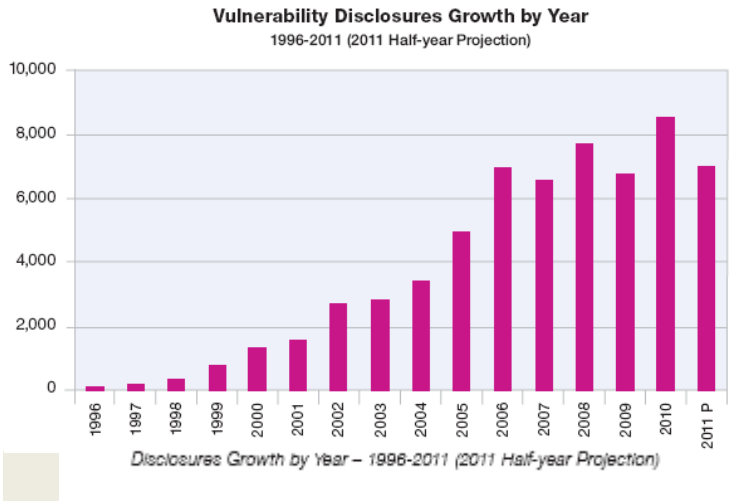

Figure 10: ICS Vulnerability Disclosures by Year 1996 - 2011

Industry leaders such as ABB, Emerson, GE, Honeywell, Invensys, Rockwell, Schneider, Siemens, Dow Chemical, Prime Controls McAfee and other vendors provide a well-represented technical expertise for industrial control.

The ICS-CERT team is part of the National Cybersecurity and Integration Center (NCCIC), and is a division of the Department of Homeland Defense (DHS) Office of Cybersecurity and communications. ICS-CERT is a key component of DHS' Strategy for Securing Control Systems.

Conclusions and Next Steps

It has been shown in this paper that Information Assurance controls are needed as PCMs are integrated on Aegis Class destroyers. With the increase of complexity in Navy electric power plants, information controls will be used to prevent risk to the mission and safety of personnel. The Navy has instituted the DOD DIACAP to mitigate that risk. Keeping an eye on future security threats and the evolution of the C&A process will keep the PCM and MCS secure for future naval missions.

Acknowledgement

The authors would like to acknowledge and thank Mr. Joe Borraccini for supporting this work as the ONR Program Officer for Compact Power under ONR 331, and the NSWCCD Compact Power Manager Team for contributing to the evolving concepts summarized in the paper.

Author Biographies

John Mochulski is the Project Manager for the Compact Power Converter Technologies (CPCT) Program at NAVSSES, working in the Automation and Control Research and Development Branch. His experience includes both Industry and Government lead roles developing a broad range of large-scale Navy and DOD Information Systems, Communications Systems, and Information Assurance products. At L-3 Communications, John was a lead engineer performing concept design, systems analysis, and software development on major DOD programs, including the F-35 Joint Strike Fighter Program. He also worked on the Navy's future destroyer platform, DD-21, (now DDG-1000), where he developed the shipboard network security architecture. Prior to L-3, John worked for the Naval Air Warfare Center, Aircraft Division, supporting the development of Navy standard computer hardware and software for tactical aircraft mission planning applications. He received his B.S. in Electrical Engineering from Drexel University in 1984, and a M.S. in Engineering from Penn State University in 1992.

Rick Silverman is a Senior Principal Systems Engineer for the General Dynamics Information Technology Corporation, and has served as a Machinery Control System Engineer for the Compact Power Converter Technologies (CPCT) Program, AMDR and DDG 1000 programs at NAVSSES-PHL. Prior to GDIT, Rick has worked on control systems for RCA/GE, Martin Marietta, Sperry Marine, AlliedSignal and Raytheon. Rick is a commercially rated FAA pilot and has flown for US Airways Express. Rick graduated with a B.S.E.E. from the Worcester Polytechnic Institute in 1986.

[1] Timothy Scherer and Jeffrey Cohen , The Evolution of Machinery Control Systems Support at the Naval Ship Systems Engineering Station, Naval Engineer's Journal, 2011 #2.

[2] Kokoska, Mark, "Information Security for Afloat Systems Hull, Mechanical & Electrical (HM&E) Perspective" 06/23/2011.

[3] Gigabit Ethernet Data Multiplex System (GEDMS) – Supporting the Modernization of Navy Combatants, Scott Meier and Thomas Morris

[4] DOD DESIGN CRITERIA STANDARD ARCHITECTURE OF SHIPBOARD MACHINERY CONTROL SYSTEMS DRAFT, DOD-STD-X628, 16 February 2013

[5] http://www.public.navy.mil/surfor/ddg53/Pages/FirstDDGModernizationWarshipDepartsonDeployment.aspx

[6] Personnel Readiness Information Management website www.prim.osd.mil/cap/cio-ia.html

[7] http://en.wikipedia.org/wiki/DIACAP

[8] DOD Directive 8500.1, "Information Assurance," 6 February 2003

[9] DODI 8500.2, "Information Assurance" (IA) Implementation February 6, 2003

[10] https://diacap.iaportal.navy.mil/login.htm

[11] The Economist – "A worm in the centrifuge" Sept 30, 2010 http://www.economist.com/node/17147818

[12] The Industrial Control Systems Cyber Emergency Response Team homepage http://ics-cert.us-cert.gov/index.html