INL/EXT-14-33609
Revision 0

Light Water Reactor Sustainability Program

Cyber Security Evaluation of II&C Technologies

November 2014

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-14-33609
Revision 0

Cyber Security Evaluation of II&C Technologies

Ken Thomas
Idaho National Laboratory

Michael Thow
Todd Kenny
Lee Watkins
AREVA Inc.

November 2014

Idaho National Laboratory
Light Water Reactor Sustainability Program
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.SDepartment of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

EXECUTIVE SUMMARY

The Light Water Reactor Sustainability (LWRS) Program is a research and development program sponsored by the Department of Energy, conducted in close collaboration with industry to provide the technical foundations for licensing and managing the long-term, safe and economical operation of nuclear power plants. The LWRS Program serves to help the US nuclear industry adopt new technologies and engineering solutions to facilitate the continued safe operation of the plants and extension of the current operating licenses.

Within the LWRS Program, the Advanced Instrumentation, Information, and Control (II&C) Systems Technologies Pathway conducts targeted research and development (R&D) to address aging and reliability concerns with the legacy instrumentation and control and related information systems of the US operating light water reactor (LWR) fleet. The II&C Pathway is conducted by Idaho National Laboratory (INL).

Cyber security is a common concern among nuclear utilities and other nuclear industry stakeholders regarding the digital technologies that are being developed under the II&C Pathway. More specifically, the concern is whether the information contained in these technologies could be compromised and whether the technologies could be exploited for access to plant systems and components.

To address this concern, a cyber security control assessment was conducted for these technologies. The objective was to determine whether they constitute a threat beyond the scope of what nuclear plants manage within their regulatory-required cyber security program.

The evaluation was conducted by a cyber security team with expertise in nuclear utility cyber security programs and experience in conducting these evaluations. The evaluation was based on NEI 08-09, which is the industry's standard program for cyber security programs and evaluations, accepted by the Nuclear Regulatory Commission (NRC) in meeting the requirements found in 10 CFR 73.54. This program requires that each digital asset be analyzed for criticality to safety, important-to-safety, security, and emergency preparedness functions. If determined to be critical, these components are classified as Critical Digital Assets (CDA).

The notable results from the assessments were:

1. An evaluation of the II&C technologies for compliance with the cyber security controls prescribed in NEI 08-09 determined that six technologies would be categorized as CDAs. One additional technology would also be a CDA, but, in fact, would not be allowed at all under the current cyber security requirements. The major threat vector introduced by the technologies is the use of wireless communications, particularly with safety-related and important-to-safety systems.
2. Human performance and process improvement technologies that are limited to planning and utilization of computer-based procedures that do not require real time, qualified, plant process parameter monitoring or control will most likely fall in business security level and will not be CDAs. They would likely be classified as "tools", similar to M&TE.
3. Hybrid control room technologies will generally be categorized as CDAs depending on the functionality and system being monitored and controlled. If wireless technology is utilized, they are not allowed to be used on devices that perform safety-related or important-to-safety functions as dictated by the plant's approved cyber security plan.
4. Continuous Real Time On-Line Monitoring for the purposes of planning, maintenance or equipment prognosis (not used for control or operator decision making) that obtains the data from a Security Level 2 business server is not a significant cyber security concern and would not be a CDA.

CONTENTS

FIGURES

TABLES

ACRONYMS

AAS	Advanced Alarm System
BOP	Balance of Plant
CDA	Critical Digital Asset
CFR	Code of Federal Regulations
COTS	Commercial, Off-the Shelf
CS	Critical System
CSAT	Cyber Security Assessment Team
DCS	Distributed Control System
DOE	Department of Energy
EOP	Emergency Operating Procedure
FERC	Federal Electric Reliability Commission
II&C	Instrumentation, Information and Control
INL	Idaho National Laboratory
LWR	Light Water Reactor
LWRS	Light Water Reactor Sustainability
M&TE	Measuring and Test Equipment
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OCR	Optical Character Recognition
PDA	Personal Digital Assistant
PMMD	Portable Media and Mobile Devices
RFID	Radio Frequency Identification
R&D	Research and Development
SGI	Safeguards Information
SQA	Software Quality Assurance
SSEP	Safety, Security, Emergency Preparedness
TS	Technical Specification
VoIP	Voice over Internet Protocol
V&V	Verification and Validation

Cyber Security Evaluation of II&C Technologies

1. INTRODUCTION

The Advanced Instrumentation, Information, and Control (II&C) Systems Technologies Pathway is part of the Department of Energy (DOE) Light Water Reactor Sustainability (LWRS) Program [1]. It conducts targeted research and development (R&D) to address aging and reliability concerns with the legacy instrumentation and control and related information systems of the U.S. operating light water reactor (LWR) fleet. This work involves two major goals: (1) to ensure that legacy analog II&C systems are not life-limiting issues for the LWR fleet and (2) to implement digital II&C technology in a manner that enables broad innovation and business improvement in the nuclear power plant (NPP) operating model. Resolving long-term operational concerns with the II&C systems contributes to the long-term sustainability of the LWR fleet, which is vital to the nation's energy and environmental security.

The II&C Pathway is conducting a series of pilot projects that enable the development and deployment of new II&C technologies in existing nuclear plants. The pilot projects serve as stepping stones to achieve longer-term outcomes of sustainable II&C technologies. They are designed to emphasize success in some crucial aspect of plant technology refurbishment and sustainable modernization. They provide the opportunity to develop and demonstrate methods to technology development and deployment that can be broadly standardized and leveraged by the commercial nuclear power fleet.

Cyber security for has been a particular concern for nuclear utilities and industry stakeholders in regard to eventual implementation of the pilot project technologies. Questions have been raised on the potential compromise of information that will be contained in these types of technologies and whether the technologies themselves will serve as attack vectors for adversaries. These concerns are particularly heightened in regard to the use of wireless capabilities for the pilot project technologies. This has resulted in uncertainty as to how these technologies will be classified under the Nuclear Regulatory Commission (NRC) requirements for cyber security protection and in some cases, whether they will even be permitted to be used.

1.1 Purpose of Evaluation

The purpose of this evaluation is to gain insight into how the II&C digital technologies would be classified under a typical nuclear utility's cyber security program. It is important for nuclear utilities to have some basis for planning the implementation of these technologies with respect to how they will affect their cyber security posture. In addition, a number of nuclear industry stakeholder organizations have expressed concern that cyber security regulations could potentially become a barrier for technology implementation.

By conducting this evaluation, uncertainty can be reduced regarding the implementation of these technologies and nuclear utilities can have a higher degree of confidence in pursuing them. While it is recognized that only a general assessment can be performed on these prototype technologies, since many of the installation details are not known, the evaluation will still provide early insight on how to classify and protect these new digital technologies. Additional evaluations might become warranted as the technologies are further developed and expanded in capabilities.

It is also important to understand any limitations on the technologies that will be imposed by cyber security considerations. Through this understanding, the concepts of the technologies can be shaped by any restrictions imposed by the current licensing basis for cyber security. For example, wireless communication is prohibited from use in safety related and important to safety systems under current nuclear utility cyber security programs. Insights such as this will need to be factored into the development plans for future technologies to avoid barriers to implementation.

1.2 Definition and Scope of Cyber Security

Cyber Security in the nuclear industry is defined in Title 10, Part 73, "Physical Protection of Plants and Materials," Section 54, "Protection of Digital Computer and Communication Systems and Networks," of the United States Code of Federal Regulations [2]. 10 CFR 73.54 requires licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks up to and including the design basis threat. The licensee is required to protect these assets that are associated with:

a) Safety-related and important-to safety functions;

b) Security functions;

c) Emergency preparedness functions, including offsite communications; and

d) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Cyber protection prevents cyber-attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data and/or software; deny access to systems, services, and/or data, and; impact the operation of systems, networks, and associated equipment.

Compliance with cyber security regulations entails establishing, implementing, and maintaining a cyber-security plan that implements the cyber security program requirements dictated in 10 CFR 73.54. As prescribed in 10 CFR 73.54 (e), any plan must:

a) Describe how the requirements will be implemented and must account for the site-specific conditions that affect implementation, and

b) Include measures for incident response and recovery for cyber-attacks, which includes the following:
   - Maintain the capability for timely detection and response to cyber-attacks.
   - Mitigate the consequences of cyber-attacks.
   - Correct exploited vulnerabilities.
   - Restore affected systems, networks, and/or equipment affected by cyber-attacks.

2. BACKGROUND OF NUCLEAR CYBER SECURITY

2.1 Development of Cyber Security Environment

2.1.1 Regulatory Background

In 2003, the NRC issued a new Design Basis Threat Order [3] which included a cyber-attack for the first time, began work on a cyber-assessment methodology (NUREG 6847) [4], and started conducting pilot assessments of four nuclear plants. The pilot assessments unofficially became the basis for new rule making. The NRC issued proposed rule changes to Part 73 which became the new cyber security rule, 10 CFR 73.54 The NRC also began working on Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," [5] to provide guidance on the proposed cyber security rule. The new rule, 10 CFR 73.54, was issued in May, 2009 and RG 5.71 and was completed in January 2010. In 2011, the NRC accepted the cyber security plans of the nuclear facilities.

2.1.2 Industry Response

To address these new regulatory requirements, the Nuclear Energy Institute (NEI) formed a Cyber Security Task Force. This task force began work on NEI 04-04 [6] to provide interim guidance to address NUREG 6847. NEI 04-04 was endorsed by the NRC and voluntarily committed to by the majority of the nuclear industry. In 2008, in response to the NRC's upcoming cyber security rule, NEI began work on NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," [7] which became the industry standard

template for a cyber security plan for existing nuclear facilities. NEI 08-09 was completed before RG 5.71 and therefore, almost all operating plants choose to implement this guidance. RG 5.71 and NEI 08-09 are very similar in that they both contain cyber security controls based on National Institute of Standards and Technology (NIST) SP 800-52, "Security and Privacy Controls for Federal Information Systems and Organizations" [8] and NIST SP 800-82, "Guide to Industrial Control System (ICS) Security." [9] RG 5.71 also provides additional information relating to implementation of the cyber security program and identification of critical digital assets (CDAs).

NEI developed additional guidance to aid implementation of cyber security plans and conduct control assessments:

- NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule" [10]
- NEI 10-08, "Cyber Security Program Review" [11]
- NEI 10-09, "Addressing Cyber Security Controls for Nuclear Power Reactors" [12]
- NEI 13-10, "Cyber Security Control Assessments" [13]

The NRC has endorsed NEI 10-04, NEI 10-08 and NEI 13-10, but has not endorsed NEI 10-09.

The nuclear industry submitted cyber security plans based on NEI 08-09. The NRC issued 136 Requests for Additional Information (RAI) after the initial filings. The nuclear industry and the NRC met to resolve these issues and reached an agreement on a set of seven interim 'milestones' for plan implementation. The milestones are:

Milestone 1 – Establish the Cyber Security Assessment Team (CSAT)

Milestone 2 – Identify Critical Systems (CSs) and Critical Digital Assets (CDAs)

Milestone 3 – Install a deterministic one-way device between lower level devices (Level 0,1,2) and higher level devices (Level 3,4). (See Section 2.3.1 for explanation of Levels)

Milestone 4 – Implement the security control "Access Control for Portable and Mobile Devices"

Milestone 5 – Implement observations and identification of obvious signs of cyber related tampering to existing insider mitigation rounds

Milestone 6 – Identify, document, and implement cyber security controls as per "Mitigation of Vulnerabilities and Application of Cyber Security Controls" for CDAs that could adversely impact the design function of physical security target set equipment

Milestone 7 – Commence ongoing monitoring and assessment activities for those targets set CDAs whose security controls have been implemented

Milestones 1-7 were required to be completed by 12/31/2012, and full implementation of the cyber security plan is required to be completed by the date specified in the each site's license amendment. [10].

2.2 Corporate IT Requirements

Corporate IT standards will apply to any digital device in the plant. These may be best practices or driven by the Sarbanes-Oxley Act [14], Health Insurance Portability and Accountability Act (HIPAA) [15], or other regulatory requirements. Digital assets not defined as CDAs are generally still required to comply with these requirements.

2.3 General Approach to Cyber Security

10 CFR 73.54 establishes an overall requirement to ensure the functions of digital assets are protected from cyber-attack. As such, the NRC does not recognize risk-based assessments of digital assets but rather requires a defensive strategy consisting of a defensive architecture and the cyber security controls outlined in Appendixes D and E of NEI 08-09, or Appendixes B and C of RG 5.71.

2.3.1 Network Security Defense Architecture

As a part of the defensive strategy outlined in the site cyber security plan, the licensee maintains a network security defensive architecture. The network security defensive architecture in RG 5.71 describes a five level approach to defense in depth. The network security levels are as follows:

a) Level 0 – Public Internet

b) Level 1 – Corporate wide area network

c) Level 2 – Site local area network

d) Level 3 – Control system monitoring networks

e) Level 4 – Control system control networks, safety systems, or other logically isolated, 'air-gapped' networks

Figure 1 illustrates typical defensive architectures under the control of the licensee (Levels 1-4). Data can only flow from one level to an adjacent level through a device that enforces security policies between levels, and data communication can only be initiated from devices at a higher security level. Level 4 networks may be connected using a firewall and intrusion detection system or a data diode to level 3 networks. If the Level 4 / Level 3 interface uses a firewall and intrusion detection system, then the Level 3 / Level 2 interface must use a data diode. Otherwise, the Level 3 / Level 2 interface can use a firewall and intrusion detection system.

These security levels do not dictate what security controls are required for a particular device. In theory, any digital asset, including the assets described in 10 CFR 73.54, can be placed in any of the security levels. From a practical perspective, placement in Level 3 or 4 allows the licensee to utilize the defensive network architecture to protect the assets. For this reason, most sites do not place CDAs outside of Level 3.

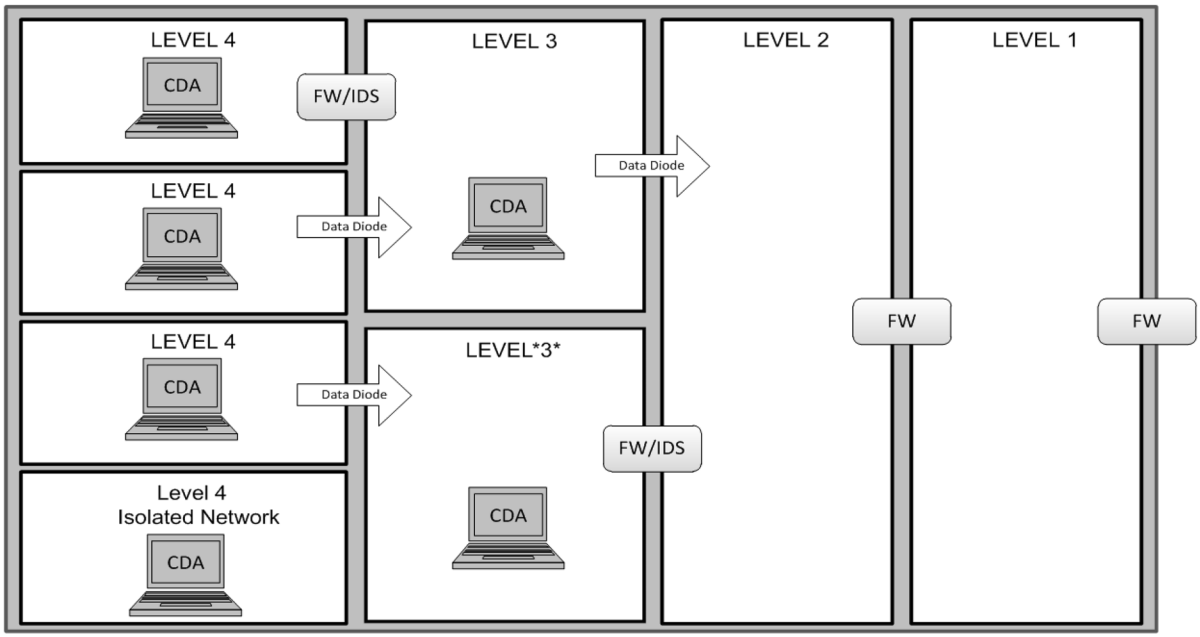

Figure 1: Security Defensive Architecture

2.3.2 Attack Vectors

The cyber security controls in the cyber security plan are in place to protect CDAs across any applicable attack vectors. The NRC recognizes five separate cyber security attack vectors in the NRC Inspection Manual 0609 [16]:

a) Physical Access –This attack vector describes the ability of an attacker to cause adverse impact to a digital asset by physically interacting with the device. These attacks can range from altering configuration of cables to malicious human machine interaction.

b) Wired Network Connections – This attack vector describes the ability of an attacker to cause adverse impact to a digital asset over a hard-wired logical network. The network can be a conventional Ethernet network, or a proprietary field bus.

c) Wireless Network Connections – This attack vector describes the ability of an attacker to cause adverse impact to a digital asset utilizing a wireless network. Wireless networks include 802.11 Wi-Fi networks, Bluetooth, Zigbee, Near-Field communication, or other proprietary wireless networks using various frequencies.

d) Portable Media and Mobile Devices (PMMD) – This attack vector describes the ability of an attacker to cause adverse impact to a digital asset utilizing a separate, non-permanent digital device. This device can be a USB flash-based memory drive, laptop computer, smartphone, or other maintenance equipment.

e) Supply Chain – This attack vector describes the ability of an attacker to infiltrate the digital asset to cause adverse impact before the final owner has taken possession. The infiltration can occur at any point in the supply chain.

2.3.3 Software Quality Assurance

New digital equipment applied in the nuclear industry must meet quality assurance requirements as stated in 10 CFR 50 Appendix B [17], and as clarified in Branch Technical Position (BTP) 7-14 of NUREG 0800. [18] BTP 7-14 outlines various components of a proper software quality assurance (SQA) program.

SQA is not cyber security, but proper SQA enhances cyber security. All digital devices must undergo proper SQA and verification and validation (V&V) to ensure appropriate functionality, and this will include appropriate defense against cyber security compromises.

The technologies under development in the II&C research program are designed to direct personnel and/ or provide real time monitoring and control to the plant's operating systems and therefore, the products will be required to have a QA program that meets the same requirements as installing a digital-based control system into a nuclear power plant.

2.3.4 General Security Controls

The implementation of 10 CFR 73.54 requires all CDAs to have all of the controls outlined in the plant cyber security plan addressed in one of three ways:

1. Applied: This control is being implemented on this device as written.
2. Not Applicable: This control is not being implemented on this device because the device does not have the capabilities addressed by this control (i.e., password controls do not apply on a device with no password capability).
3. Alternately Controlled: This control is not being implemented as written. Other controls or procedures are in place that provides at least equal security for this vulnerability.

The cyber security plans approved by the NRC have over 138 cyber security controls, which are further subdivided into more than 500 cyber security sub-controls. These controls fall into two categories, Technical and Administrative controls. A small representative sample of controls is listed in Table 1.

Control Name	NEI 08-09 Section
Account Management	D 1.2
Access Control for Portable and Mobile Devices	D 1.19
Wireless Access Restrictions	D 1.17
Removal of Unnecessary Services and Programs	D 5.1
Time Stamps	D 2.8
Auditable Events	D 2.2
Unauthorized Remote Activation of Services	D 3.10
Training	E 9
Baseline Configuration	E 10.3

Table 1: Sample NEI 08-09 Controls

2.4 Overview of Utility Assessment Process

Most currently-operating nuclear power plants use NEI 08-09 as the basis for their cyber security plan, with a very few using the similar guidance found in RG 5.71. The process starts with the creation of a Cyber Security Assessment Team (CSAT), which is comprised of a number of individuals with broad knowledge in the areas of information and digital system technology; nuclear power plant operations, engineering, and nuclear safety; and physical security and emergency preparedness.

The CSAT identifies and evaluates each digital asset in the nuclear plant for its role in safety, security, and emergency planning (SSEP) functions, as well as its overall nexus to radiological health and safety, to determine if the asset is a critical digital asset (CDA). This determination is based on the guidance in NEI 10-04.

If the asset is not a CDA, it is referred to as a digital asset (DA) and is not within the scope of 10 CFR 73.54. Therefore, there are no NRC-mandated security control requirements. For the assets that are determined to be CDAs, an assessment process is conducted as illustrated in Figure 2.

The CSAT combines generic and common cyber security controls and specific information regarding the CDA, and determines if any vulnerability exists. Once a security control analysis is conducted, the specific controls for the CDA and evidence of mitigated attack vectors are documented. If there are any gaps, the CSAT initiates corrective action to close the gap and reinitiates the assessment.

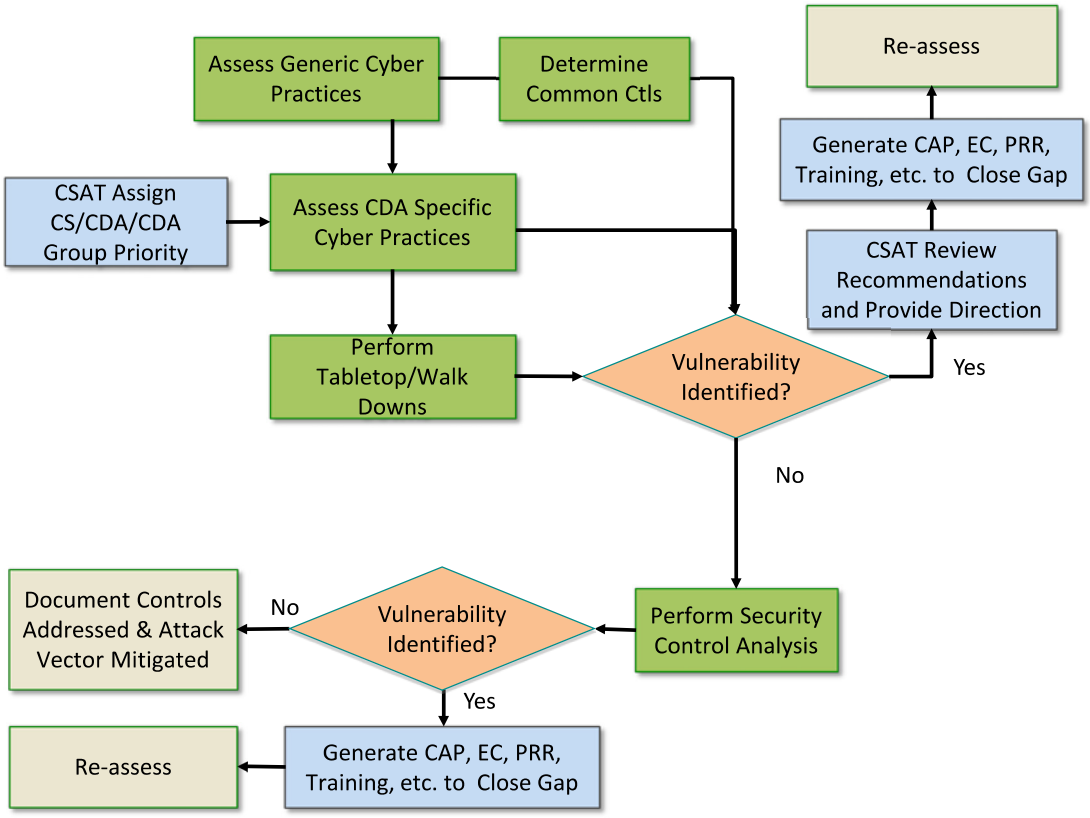

Figure 2: High Level CDA Assessment Process

3. LWRS PROGRAM II&C EVALUATION METHODOLOGY

3.1 Process

To conduct an evaluation for the II&C technologies, AREVA formed a mock CSAT of three individuals with experience / knowledge in cyber security, plant I&C systems and plant modifications and upgrades. (Brief resumes for the CSAT can be found in Appendix A.) AREVA and INL performed a CSAT session on October 8 and 9, 2014, at the INL facility. The CSAT session consisted of INL Principal Investigators presenting their respective II&C technologies to the CSAT team. After each presentation, the CSAT team and INL discussed the operational considerations of the technology and potential impacts to the plant systems, thereby establishing criteria for CDA determination for the various digital technologies and with respect to appropriate protection levels. Given that these are prototype technologies and do not represent specific utility implementations, certain assumptions had to be made concerning the range of use and configurations that a given utility might undertake.

AREVA took the discoveries from the mock CSAT sessions and assessed the technology with recommendations based on NEI 10-04 guidelines. Each technology was evaluated using the abbreviated CS/CDA assessment form found in Appendix B. The form implements the guidance found in NEI 10-04 and is derived from current industry forms.

The assessment process looks at the whole asset to make the determination. Individual technologies (e.g. Wi-Fi, barcode scanning, novel software use) cannot be assessed separately from the asset in which it is utilized.

This form is prepared by a member of the CSAT or designated preparer. The checklists for safety, important-to-safety, security, emergency preparedness, and support systems and equipment are filled out, and any 'Yes' response indicates that the assessed digital asset is a CDA.

3.2 Limitations

The assessment was performed based on very preliminary and general information provided during the CSAT sessions. No design based documentation or technology specifications were reviewed.

NEI 10-04 was used for guidance in the assessment; however, no complete assessments of any component or system were performed. Major components were assessed for CDA and protection layer determination.

The results of the assessment are based on generalities for the type of digital asset being utilized.

4. II&C TECHNOLOGY EVALUATION AND DISPOSITION

This section describes the results of the mock CSAT sessions. The pilot projects that were assessed are grouped into three main categories: Human Performance and Process Improvement (HPPI), Hybrid Control Room (HCR), and Online Monitoring (OLM). Each project is screened using the abbreviated CS/CDA assessment form, and the results are summarized below. The assessment forms are found in Appendix B.

4.1 Human Performance and Process Improvement (HPPI)

Human performance and process improvement are critical needs in the nuclear industry today, to reduce operating costs and to reduce challenges to nuclear safety. A series of pilot projects have been conducted in the II&C Pathway to develop and demonstrate human performance and process improvement technologies for workers involved in field activities. For many years, the nuclear industry has relied on focused worker behaviors, checklists, and peer checks for job quality and event avoidance. These techniques have imposed an additional burden on workers and have created some work inefficiencies. Technology has been greatly underutilized in reducing mental burden on workers. Likewise, it has been underutilized in improving productivity and job quality. In many cases, the human error prevention tools can be directly embedded in the technologies such that they occur as a natural part of the work and are essentially transparent to the worker. This enables workers to focus their attention on the actual work rather than the human performance measures, resulting in higher productivity.

4.1.1 Mobile Field Worker Technology

4.1.1.1 Description

Mobile Field Worker Technology uses a variety of hand-held or wearable devices to integrate technology directly into the activities of field workers. These include tablets, personal digital assistants (PDAs), smart phones, and heads-up displays, with certain types of devices being more suitable for the various job settings. These devices serve as the host for multiple applications that support the work activities. These include computerized procedures, work instructions, and work packages. They provide direct access to important station work processes such as generating a work request or making an entry into the corrective action program upon discovery of an adverse condition.

These devices can also be used to correctly identify the component to be worked on, using a bar code reader (or camera) to match a component tag to the procedure in use. In the future, additional identification technologies may be incorporated such as optical character recognition (OCR) and radio frequency identification (RFID).

These devices also enable real-time communications (using wireless technology) to outage and work control centers, supervisors, and other workers; transmitting voice, data, pictures, and video. These communication capabilities provide an array of needed functions in work coordination, status reporting, problem solving, and general collaboration among remote parties. They can be used to retrieve additional documents on the job site when needed such as drawings, vendor manuals, operating experience, updated work packages, etc. Where wireless communications are limited or undesirable, these capabilities will operate on a near-time basis using locally-distributed sync stations.

These devices serve as the mobile platform for more advanced technologies being developed under the II&C pilot projects. Therefore, the cyber security considerations for the mobile technologies extend to these additional technologies as well.

4.1.1.2 Assessment

The assessment considered two assets for this system: a base server and the mobile devices used in the plant. This assessment assumed the server is installed on the plant business network (Level 2) and is thus isolated from the plant control network. The mobile devices can either 'sync' to this server using a wired connection or use a wireless technology. The mobile devices do not have the capability to connect to Level 3 or 4 networks.

This assessment is INL-HPPI-MFW-001, found in Appendix B. The assessment concluded that this is not a Critical System, and therefore there are no Critical Digital Assets present. The mobile devices will likely be entered into the M&TE program.

4.1.2 Computer Based Procedures for Field Workers

4.1.2.1 Description

Computer-based procedures (CBP) are resident on the mobile devices described in Section 4.1.1.1 to provide a number of productivity and error-prevention capabilities in the use of plant procedures. These functions are resident in the CBP application on the mobile devices and perform such tasks as automatic place-keeping, procedure flow guidance, computational routines, correct component verification, and other error-prevention functions. Future versions will use wireless technology to enable real-time procedure coordination where sequence of steps by remote parties is critical. Also, CBPs permit the automatic real-time transmission of work status and triggers for support functions. Eventually, they will be able to communicate directly with plant data sources (e.g. plant I&C systems, plant process computer) to directly acquire data that must be entered into the procedure.

4.1.2.2 Assessment

This assessment considered two assets for this system: a base server and the mobile devices used in the plant. This assessment assumed the server is installed on the plant business network (Level 2) and is thus isolated from the plant control network. The mobile device can either 'sync' to this server using a wired connection or using a wireless technology. The mobile device does not have the capability to connect to Level 3 or 4 networks. The mobile device does not have any control capability.

This assessment is INL-HPPI-CBP-001, found in Appendix B. The assessment concluded that this is not a Critical System, and therefore, there are no Critical Digital Assets present. The mobile devices will likely be entered into the M&TE program.

4.1.3 Automated Work Packages

4.1.3.1 Description

Automated work packages (AWPs) will also reside on the mobile technology platforms described in Section 4.1.1.1 and will operate in a similar, but expanded, manner as CBPs, including features such as correct component identification, computations, validity checking, and human error prevention techniques, and other typical functions that are found in work order packages today. Such functions include the use and sequencing of CBPS as well as controlling the sequence for more generalized work instructions. They will provide for real-time access and retrieval of plant data and documents. Finally, they will support real-time communications for work status and collaboration with remote parties.

A special case of AWPs will be those that will be self-generating based on pre-set triggers from wireless (or hardwired) data inputs from advanced plant instrumentation. This will provide the ability to have automatic documentation of surveillance requirements where a work package serves as the document of record. An example would be a surveillance requirement to verify that certain containment isolation valves are locked closed, in which intelligent lock-out devices communicate directly to an application that

periodically creates and routes the required documenting work package. They could be triggered on pre-set schedules or based on data values. This has the potential to reduce workload and cost in conducting these surveillance activities.

4.1.3.2 Assessment

Two assessments were conducted on this system. The first assessment was conducted under the assumption that the mobile devices do not directly connect to plant assets for data, while the second assessment assumed such a direct connection. In the second assessment, the mobile devices would be forbidden by the plant cyber security plan from connecting to safety or important-to-safety devices over a wireless medium.

The assessments are INL-HPPI-AWP-001 and INL-HPPI-AWP-002, found in Appendix B. In both cases, the assessment concluded that this is not a Critical System, and therefore, there are no Critical Digital Assets present. This conclusion applies to both the conventional and self-generating AWPs. The mobile devices will likely be entered into the M&TE program.

4.1.4 Advanced Outage Control Center

4.1.4.1 Description

The Advanced Outage Control Center (AOCC) pilot project is focused on the development of a series of work collaboration technologies, which are a collection of capabilities that support the communication, coordination, and interaction of disperse teams working to a common goal. A typical example would be an outage control center that interacts with multiple work function control centers (e.g. radiation protection) and field work activities. Today, these coordination activities occur mostly through phone and email means, and do not include the real-time sharing of data and documents. Another key concept is immediate collaboration for remote parties, enabling an early shared understanding of emergent conditions and resolution options. Finally, there are a number of routine coordination functions that can be handled completely by the technology, freeing the control center staff to work on higher priority items that affect the key outage goals.

Typical technologies employed in these concepts consist of smart boards, large video displays, decision support software, and shared data files from of inputs including work management systems, work schedules, risk management systems, etc. These technologies will interact with all of the previously-described human performance and process improvement technologies, including the mobile work technologies, CBPs, and AWPs, They will rely on wireless communication and require transmission of large quantities of data (e.g. video) between and among control centers and work sites. They will receive a number of video feeds from major (or critical) work activities for display in an array of monitors in a control center. They will allow remote (including off-site) managers, suppliers, and consultants to receive real-time information and participate in the collaboration sessions. This might potentially be extended to include video conferencing between the AOCC and the main control room.

4.1.4.2 Assessment

This assessment, INL-HPPI-AOC-001, assumed the integration of several distinct commercial-off-the-shelf (COTS) technologies into a single unified package. This system has no nexus to radiological health or safety, and failure of this system does not have the ability to directly impact any SSEP function. This system is not a CDA.

.

4.2 Hybrid Control Rooms

Hybrid control rooms are ones that have a mixture of traditional analog II&C technology and newer digital technology. Virtually all U.S. nuclear plants have undertaken some number of digital upgrades over the lifetime of the stations. Introducing digital systems into the control rooms creates opportunities for improvements in control room functions that are not possible with analog technology. These can be implemented in measured ways such that the proven features of the control room configuration and

functions are preserved, while addressing gaps in human performance that have been difficult to eliminate. Pilot projects have been defined to develop the needed technologies and methodologies to achieve performance improvement through incremental control room enhancements as legacy II&C systems are replaced with digital upgrades. These pilot projects are targeted at realistic opportunities to improve control room performance with the types of digital technologies most commonly being implemented, notably distributed control systems (DCS) and plant computer upgrades.

4.2.1 Large Display Systems

4.2.1.1 Description

Large displays will be used in hybrid control rooms to depict plant overview information and tailored presentations of data for specified plant conditions. The display information will generally be selected by the operators based on plant mode and other operating conditions. In some cases, information might be "pushed" to the operators to alert them to changing conditions in some portion of the plant's systems. The displays will be able to depict alarm information graphically, employing forms more suited to human cognition. The displays will be able to depict trends and data relationships as plant transients occur. The large displays will be able to be partitioned by the operators for multiple focus areas of interest. They will also be able to display information in the context of plant process information, such as integrating alarm depictions directly into plant system schematics.

The large displays will be controlled by a computer system that can obtain plant data from a variety of sources, including the plant control system, plant protection system, and plant process computer, as well as various monitoring systems such as a turbine vibration monitoring. It will be capable of integrating information from local control panels located throughout the plant.

4.2.1.2 Assessment

This assessment, INL-HCR-LDU-001, is based on the most complex implementation of the system. This includes touch screen panels providing control and replacing current physical control boards. Since this involves intelligent, interactive displays with control authority, this is classified as a CDA.

4.2.2 Advanced Alarm Systems

4.2.2.1 Description

Advanced alarm systems (AAS) involve processing of alarm signals so that only relevant alarm information is presented to the operators, although all alarm inputs are retained and can be readily accessed by the operators if needed. This way, the visual clutter of expected and non-consequential alarms that are triggered due to (and not as the cause of) an event can be suppressed or filtered from control room actuation. The advanced alarm system can be state-based and operating mode sensitive, so that only alarms that are relevant to plant conditions are displayed. Advanced alarm systems will improve the usability of alarms (e.g., manageable numbers, salience, acoustic design, display and organization, etc.) resulting in improved operator performance during the time-critical phase of an event, Therefore, the goal of an advanced alarm system would be to alert the operating crew to valid plant conditions (i.e., for the mode and condition of the plant) with accurate and understandable information that enables effective decision-making and action.

Advanced alarms systems are very similar to current plant annunciator systems on the input side. The systems will receive alarm inputs from the plant I&C systems and process the alarm inputs according to the established alarm logic. For output, in addition to driving alarm panels and light boxes, the systems will create and present information-rich graphics to control room and operator workstation displays. The system will interface to the control room computer-based procedure system to automatically initiate procedures that are required by the alarms, including verification of entry conditions. In some cases, the systems will make multiple notifications, such as notifying Radiation Protection of a radiation monitor alarm state at the same time the control room alarm is initiated. The systems will also provide inputs to the computerized operator support systems (refer to Section 4.2.4).

4.2.2.2 Assessment

This assessment, INL-HCR-AAS-001, assumed the AAS is comprised of a server residing on the control network. This server reads values directly from the network, performs some logical processing, and displays a result to the operators.

Due to use in emergency operating procedures (EOPs) and providing plant status to plant operators during transients, an AAS is classified as a CDA.

4.2.3 Computer-Based Procedures for Control Rooms

4.2.3.1 Description

A CBP system in the control room will have similar capabilities to those described for plant field workers in Section 4.1.2.1. The CBP system will host all normal, abnormal, and emergency procedures in a seamless manner in which operators can directly transition from one procedure to another. The CBP system can be implemented in two levels of capability - with and without soft controls interfaced to the plant control systems. In either case, the CBP system will be able to acquire plant data for verification of plant status and plant response to control actions.

The CBP system will be resident on a dedicated processor and wireless interfaced to hand-held devices for the operators to use in a mobile fashion. This will allow them to move about the hybrid control room, observing data and taking control actions on both the control boards and the hand-held devices. The CBP system will be interfaced to large dedicated overhead displays so that the control room supervisor and the other operators can view the procedure steps being addressed by any operator.

4.2.3.2 Assessment

Two assessments were conducted on this system. The first assessment, NL-HCR-CBP-001, assumed the CBP system does not have any control capability and derives data from a read-only source. These CBPs could be wired or wireless devices. The second assessment, INL-HCR-CBP-002, assumed the CBP have control capability and are directly connected onto the control network. These CBPs are wired only.

The information-only CBPs are classified as CDA's because of their use in EOPs. Control-based CBPs are classified as CDAs due to their potential control authority, and their use in EOPs.

4.2.4 Computerized Operator Support Systems

4.2.4.1 Description

A computerized operator support system (COSS) is a collection of capabilities to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for current or projected plant conditions. They generally have the following features:

- Monitoring a system or process to detect off-normal conditions
- Diagnosis of plant faults
- Prediction of future plant states
- Recommendation of mitigation alternatives
- Decision support in selecting mitigation actions.

Through these capabilities, a COSS provides operators with timely information that aids in assessing the current plant status, safety margins, and deviations from expected operations. Through advanced simulation techniques, a COSS predicts where the plant is going operationally and how long the operators have to intercede in undesirable plant trends. Finally, a COSS recommends selected actions to the operators that will mitigate undesirable plant events and trends, and return the plant to a safe operating condition with the least amount of upset possible. As an optional feature, a COSS will be able to take control actions by directly driving the CPB system when authorized by the operators.

A COSS will be composed of an aggregate of technologies such as plant sensor inputs (wired and wireless), sensor validation and diagnostic processors, control room computer-based procedures with soft controls, outputs to control board and operator workstation displays, and faster-than-real-time simulators.

4.2.4.2 Assessment

The assessment, INL-HCR-COSS-001 assumed that the COSS was installed on the plant control network, with a display available to the operators. The assessment determined that a COSS is a CDA due to use with EOPs, providing plant status to plant operators during transients, and potential control authority.

4.2.5 Advanced Concepts of Operation

4.2.5.1 Description

The control room staffing and protocols for the current LWR fleet are based on operational concepts that go back to the beginning of the industry. While this operating model has been very successful in safe and productive operation of the LWR fleet, it drives a number of inefficiencies in staffing because operators who are monitoring the plant systems generally cannot be involved in other activities. Therefore, additional operators are required for work management functions, system tag-out developments, plant rounds and field operations, and monitoring special processes such as reactor refueling or dry cask storage loading.

In the future, it will be possible to gain significant efficiencies by employing new concepts of operation made possible by the combined technologies for control room upgrades and enhanced operator performance. With advanced technology, operators will be more able to conduct ancillary duties without loss of effectiveness in plant monitoring. Some of these technologies are:

- Portable interface devices (e.g., tablets and heads-up displays) that will provide continual plant status and control capability anywhere in the plant. These are discussed previously in Sections 4.1.1.1 and 4.1.2.1.
- Computerized operations support systems (COSS) that detect deviations and trends very early and provide much more response time to operators to react to and intervene in the situation. This is discussed in Section 4.2.3.1.
- Ability of qualified operators to assist with certain tasks from where they are (i.e., at home, in remote parts of the plant facility, or at a sister nuclear unit).
- New control capabilities that automate large operational sequences such as power maneuvers and putting systems into service. Further, they could diagnose and manage (without manual operator actions) the early portions of transients and accidents for the time required for operators to return to the control room. These capabilities can transform required operator actions from long sequences of individual control actions to broad, high-level outcome-based commands (e.g., “place alternate letdown in service”) These types of complex control actions ae possible with a modern DCS.
- For operators in the control room, technology would enable them to participate in activities that today would require them to be present in other parts of the facility (e.g., pre-job briefings). This capability would rely on real-time video, collaboration tools, and virtual meeting software to allow participation in these activities from their normal operating station. These technologies are discussed in Section 4.1.4.1.

Technologies to support these advanced operational concepts include high-fidelity control room displays on portable devices (such as digital tablets), high-speed data connections to the plant I&C systems (including wireless), COSS systems (as previously described), real-time collaboration technologies (as described in Section 4.1.1.1., and new control system capabilities (typically resident in the DCS) to automate sequences of plant control actions.

4.2.5.2 Assessment

This set of technologies resulted in one new assessment, INL-HCR-ACO-001, regarding the ability of qualified operators to assist remotely. The other technologies have been discussed separately or are native features of a modern DCS. While such a system would be hypothetically classified as a CDA due to its broad control authority, remote access to CDAs is disallowed by current network defensive architectures.

4.3 Online Monitoring

On-line monitoring systems provide capabilities to automatically gather information, analyze it for pre-specified concerns, and issue alerts or otherwise inform plant staff of pertinent information for decision-making and required actions. They can be applied to the complete range of monitoring requirements – from immediate plant status and degraded operating conditions to long-term component health monitoring for plant life extension. In many cases, they directly offset labor requirements to gather and analyze this information on whatever frequency is required. Properly constructed, they become repositories of the "knowledge-base" that is associated with performing the monitoring activities with trained and qualified staff. They can operate on a continuous basis in contrast to the intermittent sampling when performed as a discrete work activity.

4.3.1 Continuous On-Line Condition Monitoring

4.3.1.1 Description

Continuous On-Line Condition Monitoring systems consist of specialized sensors and signal processing systems that collect plant real time data and perform analysis for anomaly detection, pattern recognition, diagnostics, and prognostics (remaining useful life).They are able to calculate remaining margins in plant components for confirming that design basis functions can be performed.

The sensors for these systems are either attached or embedded in the components and provide data either on a continuous or intermittent basis, depending on requirements. The sensors are directly connected to the processing systems where the data is collected and analyzed. The real-time data can be grouped with periodically-acquired data (periodic tests and analyses) as inputs into complex diagnostic and prognostic models to arrive at a set of conclusions as to type of fault, cause of the fault, and remaining useful life of the asset. The systems have capabilities to directly notify organizations and individuals of analysis results, through messages and email. The systems generally do not have any control functions or other types of connections to plant equipment.

4.3.1.2 Assessment

In general, this information is not used for directly controlling the plant and therefore is not considered a plant CDA under 10 CFR 73.54. However, some of the information could be business sensitive and could potentially have NERC-CIP implications.

4.3.2 On-Line Monitoring of Plant Configuration Status

4.3.2.1 Description

On-line monitoring technology is being developed for plant status and configuration data utilizing wireless instrumentation. This information can be used to meet surveillance requirements or to confirm that plant components are in the correct alignment for current or upcoming plant conditions. The communication paths for this information are not business critical and would not run on the I&C communication circuits. If this technology would become unavailable or inaccurate, then manual means of conducting the verifications would be invoked.

These systems consist of sensors attached to components generally in a non-intrusive manner, in which they are able to sense a parameter (e.g. component position) and transmit that parameter to a processing system that integrates all of the acquired data and determines whether certain specified configurations have been met. These systems can directly output the results of the analysis or put it in the form of a work

package as discussed in Section 4.1.4. These systems could involve wireless transmission and power harvesting.

4.3.2.2 Assessment

These systems could not be used on safety-related or important-to-safety systems due to the restriction of wireless communication on safety systems.

This assessment, found in INL-OLM-CPSI-001, finds that this system is a CDA based on this system being the primary means to meet the acceptance criteria of a Technical Specification (TS) surveillance requirement.

4.4 Summary of Assessments

A summary of the assessment results for individual II&C technologies evaluated by the CSAT are presented in Table 2 below.

Section	Technology	Assessment Number	Results
4.1.1	Mobile Field Worker Technology	INL-HPPI-MFW-001	Not a CDA, most likely M&TE
4.1.2	Computer Based Procedures	INL-HPPI-CBP-001	Not a CDA, most likely M&TE
4.1.3	Automated Work Packages	INL-HPPI-AWP-001	Not a CDA, most likely M&TE
		INL-HPPI-AWP-002	Not a CDA, most likely M&TE
4.1.4	Advanced Outage Control Center	INL-HPPI-AOCC-001	Not a CDA
4.2.1	Large Display System	INL-HCR-LDU-001	CDA
4.2.2	Advanced Alarm Systems	INL-HCR-AAS-001	CDA
4.2.3	Computer Based Procedures	INL-HCR-CBP-001	CDA
		INL-HCR-CBP-002	CDA
4.2.4	Computerized Operator Support Systems	INL-HCR-COSS-001	CDA
4.2.5	Advanced Concepts of Operations	INL-HCR-ACO-001	Not allowed under current regulations
4.3.1	Continuous On-Line Condition Monitoring	INL-OLM-COLM-001	Non-CDA, information/business use only
4.3.2	On-Line Monitoring of Plant Configuration Status	INL-OLM-CPSI-001	CDA, when used for TS compliance

Table 2: Summary of Cyber Security Assessments

5. OBSERVATIONS AND CONCLUSIONS

5.1 General Findings

An evaluation of the II&C technologies for compliance with the cyber security controls prescribed in NEI 08-09 determined that six technologies would be categorized as a CDA. One additional technology would also be a CDA, but, in fact, would not be allowed at all under the current cyber security requirements.

The major threat vector introduced by the technologies is the use of wireless communications, particularly with safety-related and important-to-safety systems.

Since the II&C technologies are prototypes and lack, at this stage, lack the implementation specifications of commercial-level products, the assessments are necessarily based on certain assumptions and generalizations. Future evaluations by utilities based on known implementation specifications might vary somewhat with the results presented in this report.

The general findings of the assessment are as follows:

- Human performance and process improvement technologies that are limited to planning and utilization of computer-based procedures (in lieu of hard copy procedures) that do not require real time, qualified, plant process parameter monitoring or control will most likely fall in business security level and will not be a CDA. They would likely be classified as "tools", similar to M&TE. The servers and communication networks will need to be secured similar to the current hard copy procedures (creation, storage, updates and access), which typically reside on the company's Security Level 2 business network.
- Human performance and process improvement technologies that include 'intelligent' procedures or other automated decision making might be classified as CDAs. The current NPP fleet does not have similar technologies in place to compare. It was the majority opinion of the CSAT that - when used for field work and not control room operation - the intermediate step of the physical operator action isolates the devices sufficiently to preclude their classification as CDAs. More conservative plants/utilities might classify these devices as CDAs.
- Human performance and process improvement technologies that utilize wireless networking for real time monitoring of operator decision making purposes (or operator actions) and automatic control are not allowed on safety-related or important-to-safety systems.
- Human performance and process improvement technologies that utilize streaming video and/ or pictures would need to be evaluated for physical security concerns regarding the potential of providing information on target set or tactical position locations – although this concern is tempered by the growing use of video in monitoring outage activities.
- Human performance and process improvement technologies that utilize VoIP was not discussed in any detail, however this technology would need to be evaluated for security and operational concerns regarding compromised instructions provided to field personnel over the VoIP.
- The use of large displays in the control room can result in additional CDAs. Generally, if a display is 'dumb,' with only video inputs and display output, the display is not considered a CDA. If the display contains any sort of digital communication beyond video input, the display can be considered a CDA. If the display is interactive, it will likely be considered a CDA.
- Hybrid control room technologies will generally be categorized as CDAs depending on the functionality and system being monitored and controlled. If wireless technology is utilized, they are not allowed to be used on devices that perform safety-related or important-to-safety functions as dictated by the plant's approved cyber security plan.
- Continuous Real Time On-Line Monitoring for the purposes of planning, maintenance or equipment prognosis (not used for control or operator decision making) that obtains the data from a Security Level 2 business server is not a significant cyber security concern and would not be a CDA. If the new technology obtains its data from the plant's process computer or control system directly, the technology will be categorized as a CDA and must apply cyber security mitigation methodologies. Note: if this information is used to evaluate existing analytical margins, the technology will need to be assessed for security concerns to ensure the data could not be used to compromise plant systems.
- The II&C technologies that are being developed possess features that will rely heavily on wireless communications in order to transfer real time data to the field workers using the mobile devices and

to transmit procedural step status, pictures, and parameter data back to central servers and computers. These will need to be assessed individually based on the function of the information and the impact on the plant's support systems that could cause a reactor trip, power transient, or negatively impact security status or emergency preparedness.

For any digital assets identified as a CDA that contain integrated wireless technologies, additional cyber security mitigations will be needed due to inherent losses of some defense-in-depth measures, such as physical barriers and access control.

- Any digital assets that are not considered CDAs are not exempt from SQA and V&V activities. Additionally, all digital assets must comply with any corporate or other plant cyber security policies. Digital assets may exist within the BOP that are not governed by 10 CFR 73.54, but are regulated by NERC-CIP.

5.2 General Attack Vector Considerations

5.2.1 Wired Network Access

Most II&C technologies utilize some sort of server/client architecture. It is important to maintain the network defensive architecture when designing these systems, as discussed in Section 2.3.1. Generally, systems that do not require qualified data directly from the control system should be installed on the Level 2 business network to ensure continued protection for Level 3 and Level 4 assets.

5.2.2 Wireless Network Access

The II&C Technologies are inherently reliant upon wireless communication. All of the NRC approved cyber security plans specifically prohibit the use of wireless functions on CDAs for safety and important to safety functions.

The wireless technology does present added Cyber Security concerns and complexity when providing for proper CDA protection. The technologies that will provide real time data for real time automatic control, operator control and operator decision making will require mitigation methodologies (encryption, distance limits, signal mapping) to be developed to achieve the required level of protection.

5.2.3 Supply Chain

The II&C Technologies try to utilize commercial/ off the shelf ready hardware. The supply chain of these components is a Cyber Security concern and when a component is to be categorized as a CDA, sourcing of the component will be critical to meeting the cyber security protection requirements.

5.2.4 Portable Media & Mobile Devices

Portable Media & Mobile Device access to CDAs should be reduced as much as possible to mitigate the risks associated with this attack vector. Human Performance becomes a potential issue in the mitigation of this control, due to the universal use of flash drives for document transfer or laptops as M&TE Several II&C technologies utilized a mobile device as an integral asset within the system, thus this vector develops the greatest risk for compromise.

5.2.5 Physical Security

The potential use of cameras in the field for Mobile Field Worker Technologies may have physical security implications. Physical Security will have to be consulted before the deployment of integrated camera technologies into areas that may contain important physical safeguards, to ensure the integrity of safeguards information (SGI).

5.3 Implications for Future Technologies

For future technologies to be used on safety-related or important-to-safety CDAs, mitigations for the wireless access attack vector must meet regulatory requirements so that provided protections are equivalent to or exceed those of hardwire network communications. As previously stated, current

versions of regulatory guidance do not allow wireless technologies on safety-related or important-to-safety systems and equipment and so, the requirements will have to be amended. Additionally, plants will have to amend their cyber security plans to allow the technology.

6. REFERENCES

1. Department of Energy, Light Water Reactor Sustainability Program Plan, Fiscal Year 2009, Washington, DC, September, 2008
2. U.S. Code of Federal Regulations, 10 CFR 73.54, "Protection of digital computer and communication systems and networks"
3. NRC Order EA-03-086, April 2003, "Design Basis Threat for Radiological Sabotage"
4. Nuclear Regulatory Commission, NUREG/CR-6847 "Cyber Security Self-Assessment Method for US Nuclear Power Plants", October 2004
5. Nuclear Regulatory Commission, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities", January, 2010
6. Nuclear Energy Institute, NEI 04-04, Revision 1, "Cyber Security Program for Operating Reactors", November 20005
7. Nuclear Energy Institute, NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors", April, 2010
8. National Institute of Standards and Technology (NIST), SP 800-53, Revision 2, "Security and Privacy Controls for Federal Information Systems and Organizations"
9. National Institute of Standards and Technology (NIST), SP 800-82, Final Public Draft, "Guide to Industrial Control System (ICS) Security.
10. Nuclear Energy Institute, NEI 10-04, Revision 2, July 2012, "Identifying Systems and Assets Subject to the Cyber Security Rule"
11. Nuclear Energy Institute, NEI 10-08, Revision 0, "Cyber Security Program Review", April 2012
12. Nuclear Energy Institute, NEI 10-09, Revision 0, "Addressing Cyber Security Controls for Nuclear Power Reactors" September 2011
13. Nuclear Energy Institute, NEI 13-10, Revision 1, "Cyber Security Control Assessments", September 2014
14. Sarbanes-Oxley Act of 2002, PL 107-204, 116 Stat 745, Codified in Sections 11, 15, 18, 28, and 29 USC, July 2002
15. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C§ 1320d-9, 2010
16. Nuclear Regulatory Commission, Inspection Manual 0609, Appendix E, "Significance Determination Process" (Security-related information)
17. U.S. Code of Federal Regulations, 10 CFR 50 Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
18. Nuclear Regulatory Commission, NUREG-0800, BTP 7-14 Revision 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" , March, 2007.

APPENDIX A: TEAM QUALIFICATIONS

Michael Thow, CSAT Chair (AREVA, Inc.)

Mr. Michael Thow has over eighteen years' experience in computer systems management in the power generation and manufacturing industries. He has nine years of experience at the HB Robinson Nuclear Plant, most recently as the Cyber Security Administrator and CSAT Chair. Mr. Thow's experience includes computer systems engineer, 10CFR73.54 Cyber Security, and software quality assurance. Mr. Thow completed implementation of the RNP Cyber Security Plan Milestones one through seven on time including the performance of over 160 self-assessments on plant systems. He has experience performing engineering reviews of new digital plant modifications, developing Cyber Security common controls, implementing employee cyber awareness training, and implementing log and network monitoring, Mr. Thow strengthened portable media controls and modified procedures to comply with the new cyber regulations. Mr. Thow was also the Progress Energy Fleet Technical lead for LP Turbine Digital Instrumentation upgrade during which time he identified vendor system malware prior to install preventing malware infection in the plant operational environment. He led the technical forensic investigation, and issued formal industry OE which determined the incident to be non-malicious. Mr. Thow initiated corrective actions which resulted in strengthening Progress Energy internal supply chain and contract controls. Other experience includes roles as OSI/PI Server Administrator, project manager for implementation of WebEOC for emergency preparedness across the Progress Energy nuclear fleet, and Systems integrator of several control systems using OPC, OSI/PI, Modbus, SQL, and other database interfaces.

Todd Kenney, CSAT Member (AREVA, Inc.)

Mr. Todd Kenney has over 30 years of experience in the design of control, electrical and mechanical systems for electric utility power plants, cogeneration and industrial facilities. Mr. Kenney has specific experience in large DCS/PLC Controls, Power Distribution, Power Generation, Energy Efficiency, HVAC, Fire Protection and Electrical Transmission Support projects. Mr. Kenney has been with AREVA for over 26 years and is currently an Advisory Engineer in the I&C group with experience in both the Non-Nuclear and Nuclear side of the industry (last 10 years being primarily Nuclear). Recent projects Mr. Kenney has been involved with in the design and/ or reviews include Digital Turbine Control System Upgrades at DC Cook and Comanche Peak Nuclear Power Plants, Digital Fire Alarm Upgrades at Nine Mile and Turkey Point Nuclear Power Plants, Instrument Uncertainty Power Uprates at McGuire and Catawba Nuclear Power Plants and Spent Fuel Pool Level monitoring upgrades at Oconee and Brunswick Nuclear Power Plants.

Lee Watkins, CSAT Member (AREVA, Inc.)

Mr. Lee Watkins joined AREVA as a Cyber Security Engineer. In July 2014, Mr. Watkins received his MS in Aerospace Engineering from Old Dominion University, with an emphasis in aerospace vehicle dynamics and control. Mr. Watkins most recently worked at Siemens Energy, where he worked on various control system projects for nuclear customers at Bellefonte (performing HFE and I&C guidance), Grand Gulf (SPPA-D3000 V&V Engineer), and Calloway (V&V Engineer for digital feed water and main turbine control). In addition, Mr. Watkins has also installed SPPA-T3000 system upgrades at the Calgary and Delta Energy Centre combined cycle facilities. Mr. Watkins also developed Step7 and PCS 7 systems.

APPENDIX B: CDA DETERMINATION CHECKLIST

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**

System Description

CDA Validation	
# of CDAs in Critical System:	
CDAs added to Scope	**CDAs removed from Scope**

Safety	ITS	Security	EP	Support

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:						
New System:	Yes:		No:			
Assessment Number:						
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						
Is the SSC described as safety-related within Maintenance Rule (MR) SSC function?						
For new modifications, is the system or specific DA designated as safety-related?						
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						
(2) Fire Protection?						
(3) Seismic monitoring?						
(4) Post-Accident Monitoring?						
(5) Station Blackout protection?						
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						
(7) Alternate/Safe Shutdown?						
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						
(2) Inoperable Technical Specification Function ?						
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?						
(2) Is used in EOPs?						
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		
Does the system perform a function to control access into protected and vital areas?		
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		
Does the system perform a function for intrusion detection?		
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		
Does the system perform a function for interdiction and neutralization?		
Does the system provide secondary power for intrusion detection or alarm annunciation?		
Does the system provide secondary power for alarm assessment?		
Does the system provide secondary for non-portable communications?		
Does the system provide secondary power for an active vehicle barrier system?		
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		
Is the SSC used for communication in during a radiological emergency?		
Does the SSC impact emergency declaration and notification capabilities?		
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Support Systems and Equipment	Y	N
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		
Could the compromise of the support system have an adverse impact on a security function?		
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		

If any of the above questions are answered 'Yes,' then the device is considered a CDA If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	Y	N
Does an adversary have logical access to the Asset via a hardwired network?		
Does an adversary have logical access to the Asset via a wireless network?		
Does an adversary have physical access to the Asset?		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	HPPI Mobile Field Worker Technology	MFW	001

Assessment: INL-HPPI-MFW-001

System Description
Mobile Field Worker Technology utilizes a variety of hand-held or wearable devices to integrate technology directly into field work activities. These include tablets, PDAs, smart phones, and heads-up displays, with different types of devices being more suitable for different job settings. These devices serve as the host for various applications that support the work activities. These include computerized procedures, work instructions, and work packages. They provide direct access to important station work processes such as generating a work request or making an entry into the corrective action program upon discovery of an adverse condition. These devices can also be used to correctly identify the component to be worked on, using a bar code reader (or camera) to match a component tag to the procedure in use. In the future, additional identification technologies may be incorporated such as optical character recognition (OCR) and radio frequency identification (RFID). These devices are also enable real-time communications (using wireless technology) to outage and work control centers, supervisors, and other workers transmitting voice, data, pictures, and video. They can also be used to retrieve additional documents on the job site when needed such as drawings, vendor manuals, operating experience, updated work packages, etc. Where wireless communications are limited or undesirable, they will function on a near-time basis using locally-distributed sync stations. These devices serve as the mobile platform for more advanced technologies being developed under the pilot projects. Therefore, the cyber security considerations for the mobile technologies extend to these additional technologies as well. This assessment considers two assets for this system: a base server and the mobile units used in the plant. This assessment assumes the server is installed on the plant business network (Level 2) and is thus isolated from the plant control network .The mobile device can either 'sync' to this server using a wired connection or using a wireless technology. The mobile device does not have the capability to connect to Level 3 or 4 networks.

CDA Validation	
# of CDAs in Critical System:	No CDAs present in Mobile Field Technology
CDAs added to Scope	**CDAs removed from Scope**
None	N/A

Safety	ITS	Security	EP	Support

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HPPI Mobile Field Worker Technology					
New System:	Yes:	X	No:			
Assessment Number:	INL-HPPI-MFW-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?						**X**
(2) Is used in EOPs?						**X**
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						**X**
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						**X**

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**

Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		**X**
Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
Base Unit/Server: The base unit/server has a hardwired network on the plant business network This network connection is used to maintain current information. Mobile Device: The mobile device can have a hardwired network connection to the Base Unit/Server, or directly to the business network This connection is used to synchronize data on the device with the data on the server		
Does an adversary have logical access to the Asset via a wireless network?	**X**	
Base Unit/Server: The base unit/server does not have wireless capabilities. Mobile Device: The mobile device will have wireless capabilities The device could use Wi-Fi for a network-based synchronization The device could also use Bluetooth, Near-Field Communication or Radio Frequency ID networks to identify SSCs within the field.		
Does an adversary have physical access to the Asset?	**X**	
Base Unit/Server: The base unit/server will be stored in a locked server closet on the plant business network Plant-specific access security controls will be in place for this asset. Mobile Device: The mobile device will be carried by plant personnel throughout the OCA, PA and VA An adversary would be able to access the asset physically		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
Both devices will be based on standard, COTS devices An adversary has the ability to infiltrate the device at any point in the supply chain unless plant specific supply chain security controls are applied to a non-CDA.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?	**X**	
Base Unit: An adversary has physical access to the mobile device is taken into the field No other devices will connect to this Asset. Mobile Device: The mobile device is, by definition, a mobile device The adversary has access to this device No extraneous devices will connect to this asset.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	HPPI Computer Based Procedures	CBP	001

Assessment: INL-HPPI-CBP-001

System Description
Computer-based procedures (CBP) are resident on the mobile devices described in Section 4.1.1.1 to provide a number of productivity and error-prevention capabilities in the use of plant procedures. These functions are resident in the CBP application on the mobile device and perform such tasks as automatic place-keeping, procedure flow guidance, computational routines, correct component verification, and other error-prevention functions. Future versions will use wireless technology to enable real-time procedure coordination where sequence of steps by remote parties is critical. Also, CBPs permit the automatic real-time transmission of work status and triggers for support functions. Eventually, they will be able to communicate directly with plant data sources (e.g. plant I&C systems, plant process computer) to directly acquire data that must be entered into the procedure It is further envisioned that some of the CBPs will have soft controls to directly operate field equipment where advantageous. This assessment considers two assets for this system: a base server and the mobile units used in the plant This assessment assumes the server is installed on the plant business network (Level 2) and is thus isolated from the plant control network. The mobile device can either 'sync' to this server using a wired connection or using a wireless technology. The mobile device does not have the capability to connect to Level 3 or 4 networks The mobile device does not have any control capabilities.

CDA Validation	
# of CDAs in Critical System:	No CDAs present in CBP
CDAs added to Scope	**CDAs removed from Scope**
None	N/A

Safety	ITS	Security	EP	Support

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HPPI Computer-Based Procedures					
New System:	Yes:	X	No:			
Assessment Number:	INL-HPPI-CBP-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?						**X**
(2) Is used in EOPs?						**X**
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						**X**
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						**X**

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
Base Unit/Server: The base unit/server has a hardwired network on the plant business network This network connection is used to maintain current information. Mobile Device: The mobile device can have a hardwired network connection to the Base Unit/Server, or directly to the business network This connection is used to synchronize data on the device with the data on the server		
Does an adversary have logical access to the Asset via a wireless network?	**X**	
Base Unit/Server: The base unit/server does not have wireless capabilities. Mobile Device: The mobile device will have wireless capabilities. The device could use Wi-Fi for a network-based synchronization The device could also use Bluetooth, Near-Field Communication or Radio Frequency ID networks to identify SSCs within the field.		
Does an adversary have physical access to the Asset?	**X**	
Base Unit/Server: The base unit/server will be stored in a locked server closet on the plant business network Plant-specific access security controls will be in place for this asset. Mobile Device: The mobile device will be carried by plant personnel throughout the OCA, PA and VA An adversary would be able to access the asset physically		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
Both devices will be based on standard, COTS devices An adversary has the ability to infiltrate the device at any point in the supply chain unless plant specific supply chain security controls are applied to a non-CDA.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?	**X**	
Base Unit: An adversary has physical access to the mobile device is taken into the field No other devices will connect to this Asset. Mobile Device: The mobile device is, by definition, a mobile device The adversary has access to this device No extraneous devices will connect to this asset.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	HPPI Mobile Field Worker Technology	AWP	001

Assessment: INL-HPPI-AWP-001

System Description
Automated work packages (AWPs) will also reside on the mobile technology platforms described in Section 4.1.1.1 and will operate in a similar, but expanded, manner as CBPs, including features such as correct component identification, computations, validity checking, and human error prevention techniques. They will address the functions that are found in work order packages today. They will include the use and sequencing of CBPS. They will provide for more generalized work instructions in a controlled, sequenced manner. They will provide for the real-time access and retrieval of plant data and documents. Finally, they will support real-time communications for work status and collaboration with remote parties. A special case of AWPs will be those that will be self-generating based on pre-set triggers and wireless (or hardwired) data inputs from advanced plant instrumentation. This will provide the ability to have automatic documentation of surveillance requirements where a work package serves as the document of record. An example would be a surveillance requirement to verify that certain containment isolation valves are locked closed, in which intelligent lock-out devices communicate directly to an application that periodically creates and routes the required documenting work package. They could be triggered on pre-set schedules or based on data values. This has the potential to reduce workload and cost in conducting these surveillance activities. This assessment considers two assets for this system: a base server and the mobile units used in the plant. This assessment assumes the server is installed on the plant business network (Level 2) and is thus isolated from the plant control network. The mobile device can either 'sync' to this server using a wired connection or using a wireless technology. The mobile device does not have the capability to connect to Level 3 or 4 networks.

CDA Validation	
# of CDAs in Critical System:	No CDAs present in AWP
CDAs added to Scope	**CDAs removed from Scope**
None	N/A

Safety	ITS	Security	EP	Support

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HPPI Automated Work Packages					
New System:	Yes:	X	No:			
Assessment Number:	INL-HPPI-AWP-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?						**X**
(2) Is used in EOPs?						**X**
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						**X**
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						**X**

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
Base Unit/Server: The base unit/server has a hardwired network on the plant business network This network connection is used to maintain current information. Mobile Device: The mobile device can have a hardwired network connection to the Base Unit/Server, or directly to the business network This connection is used to synchronize data on the device with the data on the server		
Does an adversary have logical access to the Asset via a wireless network?	**X**	
Base Unit/Server: The base unit/server does not have wireless capabilities. Mobile Device: The mobile device will have wireless capabilities The device could use Wi-Fi for a network-based synchronization The device could also use Bluetooth, Near-Field Communication or Radio Frequency ID networks to identify SSCs within the field.		
Does an adversary have physical access to the Asset?	**X**	
Base Unit/Server: The base unit/server will be stored in a locked server closet on the plant business network Plant-specific access security controls will be in place for this asset. Mobile Device: The mobile device will be carried by plant personnel throughout the OCA, PA and VA An adversary would be able to access the asset physically		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
Both devices will be based on standard, COTS devices An adversary has the ability to infiltrate the device at any point in the supply chain unless plant specific supply chain security controls are applied to a non-CDA.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?	**X**	
Base Unit: An adversary has physical access to the mobile device is taken into the field No other devices will connect to this Asset. Mobile Device: The mobile device is, by definition, a mobile device The adversary has access to this device No extraneous devices will connect to this asset.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	HPPI Mobile Field Worker Technology	AWP	002

Assessment: INL-HPPI-AWP-002

System Description
Automated work packages (AWPs) will also reside on the mobile technology platforms described in Section 4.1.1.1 and will operate in a similar, but expanded, manner as CBPs, including features such as correct component identification, computations, validity checking, and human error prevention techniques. They will address the functions that are found in work order packages today. They will include the use and sequencing of CBPS They will provide for more generalized work instructions in a controlled, sequenced manner. They will provide for the real-time access and retrieval of plant data and documents. Finally, they will support real-time communications for work status and collaboration with remote parties. A special case of AWPs will be those that will be self-generating based on pre-set triggers and wireless (or hardwired) data inputs from advanced plant instrumentation. This will provide the ability to have automatic documentation of surveillance requirements where a work package serves as the document of record. An example would be a surveillance requirement to verify that certain containment isolation valves are locked closed, in which intelligent lock-out devices communicate directly to an application that periodically creates and routes the required documenting work package. They could be triggered on pre-set schedules or based on data values This has the potential to reduce workload and cost in conducting these surveillance activities. This assessment considers two assets for this system: a base server and the mobile units used in the plant. This assessment assumes the server is installed in the security level corresponding to security level of the mobile device. The mobile device is at the security level of the devices to which it connects one of these systems will be required for each security Level serviced by the mobile device.

CDA Validation	
# of CDAs in Critical System:	0
CDAs added to Scope	**CDAs removed from Scope**
None	N/A

Safety	ITS	Security	EP	Support

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HPPI Automated Work Packages					
New System:	Yes:	X	No:			
Assessment Number:	INL-HPPI-AWP-002					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?						**X**
(2) Is used in EOPs?						**X**
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						**X**
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						**X**

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
Base Unit/Server: The base unit/server has a hardwired network on the plant business network This network connection is used to maintain current information. Mobile Device: The mobile device can have a hardwired network connection to the Base Unit/Server, or directly to the business network This connection is used to synchronize data on the device with the data on the server The mobile might have a hardwired connection to digital assets to directly read process data.		
Does an adversary have logical access to the Asset via a wireless network?	**X**	
Base Unit/Server: The base unit/server does not have wireless capabilities. Mobile Device: The mobile device will have wireless capabilities The device could use Wi-Fi for a network-based synchronization The device could also use Bluetooth, Near-Field Communication or Radio Frequency ID networks to identify SSCs within the field and to directly obtain data from a digital asset in the plant.		
Does an adversary have physical access to the Asset?	**X**	
Base Unit/Server: The base unit/server will be stored in a locked server closet on the plant business network Plant-specific access security controls will be in place for this asset. Mobile Device: The mobile device will be carried by plant personnel throughout the OCA, PA and VA An adversary would be able to access the asset physically		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
Both devices will be based on standard, COTS devices An adversary has the ability to infiltrate the device at any point in the supply chain unless plant specific supply chain security controls are applied to a non-CDA.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?	**X**	
Base Unit: An adversary has physical access to the mobile device is taken into the field No other devices will connect to this Asset. Mobile Device: The mobile device is, by definition, a mobile device The adversary has access to this device No extraneous devices will connect to this asset.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	HPPI	AOCC	001

Assessment: INL-HPPI-AOCC-001

System Description
The Advanced Outage Control Center pilot project is focused on the development of a series of work collaboration technologies, which Work collaboration technologies are a collection of capabilities that that support the communication, coordination, and interaction of among disperse teams working to a common goal. A typical example would be an outage control center that needs to interact with multiple work function control centers (e.g. radiation protection) and field work activities. Today, these coordination activities occur mostly through phone and email efforts, as opposed to real-time sharing of data and documents. Another key concept is immediate collaboration for remote parties, enabling an early shared understanding of emergent conditions and resolution options. Finally, there are a number of routine coordination functions that can be handled completely by the technology, freeing the control center staff to work on the highest priority decisions higher priority items that affect the key outage goals. Typical technologies employed in these concepts consist of smart boards, large displays, decision support software, and shared data files from work management systems, work schedules, risk management systems, etc. These technologies will integrate interaction with all of the human performance and process improvement technologies, including the mobile work technologies, CBPs, and AWPs. These technologies will rely on wireless communication and the ability to transmit large quantities of data (e.g. video) between and among control centers and work sites. They will take receive a number of video feeds from major (or critical) work activities for display in an array of monitors in a control center. They will allow remote (including off-site) managers and consultants to receive real-time information and participate in the collaboration sessions. This can potentially be extended to include VoIP or video conferencing between the control center and the control room. The Advanced Outage Control Center combines several technologies in novel ways The AOCC is not a CDA.

CDA Validation	
# of CDAs in Critical System:	0
CDAs added to Scope	**CDAs removed from Scope**
None	N/A

Safety	ITS	Security	EP	Support

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HPPI Advanced Outage Control Center					
New System:	Yes:	X	No:			
Assessment Number:	INL-HPPI-AOCC-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?						**X**
(2) Is used in EOPs?						**X**
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						**X**
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						**X**

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
This asset involves servers connected to the plant network using wired connections.		
Does an adversary have logical access to the Asset via a wireless network?	**X**	
This asset includes wireless access via smartphones, tablets, laptops and other devices.		
Does an adversary have physical access to the Asset?	**X**	
This asset does not reside in the PA or VA The physical controls on this asset are substantially lower.		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
This physical asset relies on COTS hardware and software		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?	**X**	
The adversary can have access to any portable media used to connect to assets in the systemThe adversary will have access to the portable media used within the system.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	HCR	LDU	001

Assessment: INL-HCR-LDU-001

System Description
Large displays will be used in hybrid control rooms to depict plant overview information and tailored presentations of data for certain plant conditions. The display information will generally be selected by the operators based on plant mode and other operating conditions. In some cases, information might be "pushed" to the operators to alert them to changing conditions in some portion of the plant's systems. The displays will be able to depict alarm information graphically, such as superimposed over plant system diagrams to aid in understanding. The displays will be able to depict trends and data relationships as plant transients occur. The large displays will be able to be partitioned by the operators for multiple focus areas of interest. The large displays will be controlled by a computer system that can obtain plant data from a variety of sources, including the plant control system, plant protection system, and plant process computer, as well as various monitoring systems such as a turbine vibration monitoring. It will be capable of integrating information from local control panels located throughout the plant. This assessment is based on the most complex implementation of the system. This includes touch screen panels providing control and replacing current physical control boards. Since this involves intelligent, interactive displays with control authority, this will be classified as a CDA.

CDA Validation	
# of CDAs in Critical System:	1
CDAs added to Scope	**CDAs removed from Scope**
Large Display Units	None

Safety	ITS	Security	EP	Support
X	**X**			**N/A**

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification				
System Name:	HCR Large Display Units			
New System:	Yes:	X	No:	
Assessment Number:	INL-HCR-LDU-001			

Safety Related	Y	N
Is the SSC qualified as safety-related?	X	
Is the SSC described as safety-related within MR SSC function?	X	
For new modifications, is the system or specific DA designated as safety-related?	X	
Important to Safety	**Y**	**N**
Is the SSC used for:		
(1) Radioactive Waste monitoring?	X	
(2) Fire Protection?	X	
(3) Seismic monitoring?	X	
(4) Post-Accident Monitoring?	X	
(5) Station Blackout protection?	X	
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?	X	
(7) Alternate/Safe Shutdown?	X	
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?	X	
Does SSC have the potential to cause one or more of the following:		
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?	X	
(2) Inoperable Technical Specification Function ?	X	
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?	X	
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?	X	
Is this a digital SSC that:		
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?	X	
(2) Is used in EOPs?	X	
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?	X	
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?	X	
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?	X	
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?	X	
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?	X	

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		

Could the compromise of the support system have an adverse impact on a security function?		
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	Y	N
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
The asset will heavily use network connections.		
Does an adversary have logical access to the Asset via a wireless network?		**X**
The asset will interact with Safety and Important to Safety assets, therefore it will not have wireless capability		
Does an adversary have physical access to the Asset?	**X**	
The adversary has physical access to the Asset The Asset will be in the Control Room as well as the computer rooms, both located within the Vital Area, therefore there are significant pre-existing physical security controls.		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
The asset will be an application of COTS hardware, therefore and adversary will have access to the asset during the procurement process.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?		**X**
Portable media and mobile devices will not be allowed on the system.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	Hybrid Control Rooms	AAS	001

Assessment: INL-HCR-AAS-001

System Description
The advanced alarm system could be state-based and operating mode sensitive, so non-meaningful alarms would be suppressed or filtered. It will improve the usability of alarms (e.g., manageable numbers, salience, acoustic design, display and organization, etc.) so the operator is not distracted with superfluous information during the time-critical phase of an event. Rather, the goal of an advanced alarm system would be to alert the operating crew to valid plant conditions (i.e., for the mode and condition of the plant) with valid and understandable information that serves as a conduit for effective decision-making and action. From a technology standpoint, advanced alarms systems are very similar to current plant annunciator systems on the input side. They will receive alarm inputs from the plant I&C systems and process the alarm inputs according to the established alarm logic. On the output side, in addition to driving alarm panels, they will create and present information-rich graphics to control room and operator workstation displays. They will interface to the control room computer-based procedure system to automatically initiate procedures that are required by the alarms, including verification of entry conditions. In some cases, they will make multiple notifications, such as notifying Radiation Protection of a radiation monitor alarm state at the same time the control room alarm is initiated. They will also provide inputs to the Computerized Operator Support System. This assessment assumes the AAS is comprised of a server residing on the control network. This server reads raw values from the network, performs some logical processing and displays a result to the operator. The AAS can interface with any system connected to the control network The AAS can be placed in level 3 for monitoring-only interfaces.

CDA Validation	
# of CDAs in Critical System:	1
CDAs added to Scope	**CDAs removed from Scope**
Advanced alarm system server units	N/A

Safety	ITS	Security	EP	Support
X	**X**			**N/A**

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HCR Advanced Alarm Systems					
New System:	Yes:	X	No:			
Assessment Number:	INL-HCR-AAS-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?					**X**	
Is the SSC described as safety-related within MR SSC function?					**X**	
For new modifications, is the system or specific DA designated as safety-related?					**X**	
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?					**X**	
(2) Fire Protection?					**X**	
(3) Seismic monitoring?					**X**	
(4) Post-Accident Monitoring?					**X**	
(5) Station Blackout protection?					**X**	
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?					**X**	
(7) Alternate/Safe Shutdown?					**X**	
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?					**X**	
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?					**X**	
(2) Inoperable Technical Specification Function ?					**X**	
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?					**X**	
(2) Is used in EOPs?					**X**	
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?					**X**	
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?					**X**	
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?					**X**	

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
An adversary can have logical access to the Asset via a hardwired network The Asset resides on the control network and is connected via conventional network infrastructure.		
Does an adversary have logical access to the Asset via a wireless network?		**X**
The adversary does not have logical access to the Asset via a wireless network.		
Does an adversary have physical access to the Asset?		**X**
The server is assumed to reside within the VA The server is protected by several layers of physical security		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
The server is based on a COTS product		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?		**X**
The server will have no portable media or mobile device capability.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	Hybrid Control Rooms	CBP	001

Assessment: INL-HCR-CBP-001

System Description
A computer based procedure (CBP) system in the control room will have similar capabilities to those described for plant field workers in INL-HPPI-CBP-001. The CBP system will host all normal, abnormal, and emergency procedures in a seamless manner in which operators can directly transition from one procedure to another. The CBP system will have two operating modes – both with and without soft controls directly interfaced to the plant control systems In either case, the CBP system will be able to acquire plant data for verification of plant status and plant response to control actions. The CBP system will be interfaced to large dedicated overhead displays so that the control room supervisor and the other operators can view the procedure steps being addressed by any operator. This assessment assumes the CBP derives procedure data from read-only sources, and does not have any control capability. Devices relating to Important to Safety CBPs will not be wireless.

CDA Validation	
# of CDAs in Critical System:	1
CDAs added to Scope	**CDAs removed from Scope**
Computer Based Procedure	N/A

Safety	ITS	Security	EP	Support
	X			**N/A**

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HCR Computer Based Procedures					
New System:	Yes:	X	No:			
Assessment Number:	INL-HCR-CBP-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?					**X**	
(2) Is used in EOPs?					**X**	
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?					**X**	
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?					**X**	

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
An adversary can have logical access to the Asset via a hardwired network The Asset is connected to the control network in a manner that allows the asset to directly control the plant.		
Does an adversary have logical access to the Asset via a wireless network?		**X**
The asset has no wireless capabilities.		
Does an adversary have physical access to the Asset?	**X**	
The asset is assumed to reside within the VA The asset is protected by several layers of physical security		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
The asset is based on a COTS product and is therefore vulnerable to an attack on the physical supply chain.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?	**X**	
The asset may be vulnerable to attack through M&TE mobile devices.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	Hybrid Control Rooms	CBP	002

Assessment: INL-HCR-CBP-002

System Description
A computer based procedure (CBP) system in the control room will have similar capabilities to those described for plant field workers in INL-HPPI-CWB-001. The CBP system will host all normal, abnormal, and emergency procedures in a seamless manner in which operators can directly transition from one procedure to another. The CBP system will have two operating modes – both with and without soft controls directly interfaced to the plant control systems In either case, the CBP system will be able to acquire plant data for verification of plant status and plant response to control actions. The CBP system will be resident on a dedicated processor and wireless interfaced to hand-held devices for the operators to use in a mobile fashion. This will allow them to move about the hybrid control room observing data and taking control actions on both the control boards and the hand-held devices. The CBP system will be interfaced to large dedicated overhead displays so that the control room supervisor and the other operators can view the procedure steps being addressed by any operator. This assessment assumes the CBP do have control capability and are directly connected onto the control network. These CBPs are wired only Control-based CBPs will be classified as CDAs due to their potential control authority, and use in EOPs.

CDA Validation	
# of CDAs in Critical System:	1
CDAs added to Scope	**CDAs removed from Scope**
Computer Based Procedures	N/A

Safety	ITS	Security	EP	Support
X	**X**			**N/A**

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HCR Computer Based Procedures					
New System:	Yes:	X	No:			
Assessment Number:	INL-HCR-CBP -002					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?					**X**	
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?					**X**	
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?					**X**	
(2) Fire Protection?					**X**	
(3) Seismic monitoring?					**X**	
(4) Post-Accident Monitoring?					**X**	
(5) Station Blackout protection?					**X**	
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?					**X**	
(7) Alternate/Safe Shutdown?					**X**	
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?					**X**	
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?					**X**	
(2) Inoperable Technical Specification Function ?					**X**	
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?					**X**	
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?					**X**	
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?					**X**	
(2) Is used in EOPs?					**X**	
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?					**X**	
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?					**X**	

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
An adversary can have logical access to the Asset via a hardwired network The Asset resides on the control network and is connected via conventional network infrastructure.		
Does an adversary have logical access to the Asset via a wireless network?		**X**
The adversary does not have logical access to the Asset via a wireless network.		
Does an adversary have physical access to the Asset?		**X**
The server is assumed to reside within the VA The server is protected by several layers of physical security		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
The asset is based on a COTS product with custom-developed software.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?		**X**
The asset will have no portable media or mobile device capability.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	Hybrid Control Rooms	COSS	001

Assessment: INL-HCR-COSS-001

System Description
A computerized operator support system (COSS) is a collection of capabilities to assist operators in monitoring overall plant performance and making timely, informed decisions on appropriate control actions for the projected plant condition. They generally have the following features: • Monitoring a process to detect off-normal conditions • Diagnosis of plant faults • Prediction of future plant states • Recommendation of mitigation alternatives • Decision support in selecting mitigation actions. Through these capabilities, a COSS can provide operators with advanced information systems that aid in assessing the current plant status, safety margins, and deviations from expected operations. Further, through advanced simulation techniques, it cannot predict where the plant is going operationally and how long the operators have to intercede in undesirable plant trends. Finally, the technology can recommend to an operator selected actions that can mitigate undesirable plant events and trends and return the plant to a safe operating condition with the least amount of upset possible. A COSS will aggregate technologies to such as plant sensor inputs (wired and wireless), sensor validation and diagnostic processors, control room computer-based procedures with soft controls, outputs to control board and operator workstation displays, and faster-than-real-time simulators. This assessment assumes the COSS is installed on the control network. The COSS will be relied upon to drive operator decisions.

CDA Validation	
# of CDAs in Critical System:	1
CDAs added to Scope	**CDAs removed from Scope**
Computerized Operator Support System server units	N/A

Safety	ITS	Security	EP	Support
X	**X**			**N/A**

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification					
System Name:	HCR Computerized Operator Support Systems				
New System:	Yes:	X	No:		
Assessment Number:	INL-HCR-COSS-001				

Safety Related	Y	N
Is the SSC qualified as safety-related?		X
Is the SSC described as safety-related within MR SSC function?		X
For new modifications, is the system or specific DA designated as safety-related?	X	
Important to Safety	**Y**	**N**
Is the SSC used for:		
(1) Radioactive Waste monitoring?		X
(2) Fire Protection?		X
(3) Seismic monitoring?		X
(4) Post-Accident Monitoring?		X
(5) Station Blackout protection?		X
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?	X	
(7) Alternate/Safe Shutdown?	X	
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?	X	
Does SSC have the potential to cause one or more of the following:		
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?	X	
(2) Inoperable Technical Specification Function ?	X	
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?		X
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?		X
Is this a digital SSC that:		
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?	X	
(2) Is used in EOPs?	X	
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?	X	
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?		X
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?		X
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?		X
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?	X	

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
An adversary can have logical access to the Asset via a hardwired network The Asset resides on the control network and is connected via conventional network infrastructure.		
Does an adversary have logical access to the Asset via a wireless network?		**X**
The adversary does not have logical access to the Asset via a wireless network.		
Does an adversary have physical access to the Asset?		**X**
The server is assumed to reside within the VA The server is protected by several layers of physical security		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
The server is based on a COTS product		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?		**X**
The server will have no portable media or mobile device capability.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	HCR	ACO	001

Assessment: INL-HCR-ACO-001

System Description
This system allows qualified operators to assist with certain tasks from where they are (i.e., at home, in remote parts of the plant facility, or at a sister nuclear unit). This assessment assumes that the system involves some sort of VPN connection from a secure site into the plant control system. This system would be classified as a CDA, but the system would not be allowed in the current regulatory environment prohibiting remote connections to CDAs.

CDA Validation	
# of CDAs in Critical System:	1
CDAs added to Scope	**CDAs removed from Scope**
ACO	N/A

Safety	ITS	Security	EP	Support
X	**X**		**X**	**N/A**

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	HCR Advanced Concepts of Operation					
New System:	Yes:	X	No:			
Assessment Number:	INL-HCR-ACO-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within Maintenance Rule (MR) SSC function?						**X**
For new modifications, is the system or specific Digital Asset (DA) designated as safety-related?					**X**	
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?					**X**	
(2) Fire Protection?					**X**	
(3) Seismic monitoring?					**X**	
(4) Post-Accident Monitoring?					**X**	
(5) Station Blackout protection?					**X**	
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?					**X**	
(7) Alternate/Safe Shutdown?					**X**	
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?					**X**	
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?					**X**	
(2) Inoperable Technical Specification Function ?					**X**	
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?					**X**	
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?					**X**	
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?					**X**	
(2) Is used in EOPs?					**X**	
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?					**X**	
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?					**X**	
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?					**X**	
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?					**X**	
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?					**X**	
Security					**Y**	**N**

Does the system perform a function of the Active Vehicle Barrier System?		**X**
Does the system perform a function to control access into protected and vital areas?		**X**
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		**X**
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		**X**
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		**X**
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		**X**
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		**X**
Does the system perform a function for intrusion detection?		**X**
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		**X**
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		**X**
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		**X**
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		**X**
Does the system perform a function for interdiction and neutralization?		**X**
Does the system provide secondary power for intrusion detection or alarm annunciation?		**X**
Does the system provide secondary power for alarm assessment?		**X**
Does the system provide secondary for non-portable communications?		**X**
Does the system provide secondary power for an active vehicle barrier system?		**X**
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?	**X**	
Is the SSC used for communication in during a radiological emergency?	**X**	
Does the SSC impact emergency declaration and notification capabilities?	**X**	
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?	X	
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		**X**
Could the compromise of the support system have an adverse impact on a security function?		**X**

Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA Check the appropriate box on Page 1. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
This asset involves servers connected to the plant network using wired connections.		
Does an adversary have logical access to the Asset via a wireless network?		**X**
Does an adversary have physical access to the Asset?	**X**	
This asset does not reside in the Protected or Vital Area The physical controls on this asset are substantially lower.		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
This physical asset relies on commercial, off the shelf hardware and software		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?	**X**	
The adversary can have access to any portable media used to connect to assets in the systemThe adversary will have access to the portable media used within the system.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	Online Monitoring	COLM	001

Assessment: INL-OLM-COLM-001

System Description
Continuous On-Line Condition Monitoring systems consist of specialized sensors and signal processing systems that collect plant real time data and perform analysis for anomaly detection, pattern recognition, diagnostics, and prognostics (or remaining useful life). They are able to calculate remaining margins in plant components for confirming that design bases have been met. The sensors for these systems are either attached or embedded in the components and provide date either on a continuous or intermittent basis, depending on requirements. The sensors are directly connected to the processing systems where the data is collected and analyzed The real-time data can be grouped with periodically-acquired data (periodic tests and analyses) as inputs into complex diagnostic and prognostic models to arrive at a set of conclusions as to type of fault, cause of the fault, and remaining useful life of the asset. The systems have capabilities to directly notify organizations and individuals of analysis results, through messages and email. The systems generally do not have any control functions and other types of connections to plant equipment. In general, this information is not used for directly controlling the plant and would not be considered a plant CDA under 10 CFR 73.54. However, some of the information could be business sensitive and could potentially have NERC-CIP implications.

CDA Validation	
# of CDAs in Critical System:	0
CDAs added to Scope	**CDAs removed from Scope**
None	N/A

Safety	ITS	Security	EP	Support

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	OLM Continuous Online Monitoring					
New System:	Yes:	X	No:			
Assessment Number:	INL-OLM-COLM-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?						**X**
(2) Is used in EOPs?						**X**
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						**X**
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						**X**

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-safety function?		X

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
An adversary can have logical access to the Asset via a hardwired network The Asset resides on the business network.		
Does an adversary have logical access to the Asset via a wireless network?	**X**	
The asset has wireless capabilities outside of the plant control network This does not wirelessly connect to any CDAs.		
Does an adversary have physical access to the Asset?	**X**	
The asset will be stored in a locked server closet on the plant business network Plant-specific controls will be in place for this asset		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
Both devices will be based on standard, COTS devices An adversary has the ability to infiltrate the device at any point in the supply chain unless plant specific supply chain security controls are applied to a non-CDA.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?		**X**
The server will have no portable media or mobile device capability.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

System Information			
Station	**System Name**	**System Designator**	**Unit**
INL	Online Monitoring	CPSI	001

Assessment: INL-OLM-CPSI-001

System Description
On-line monitoring technology is being developed for plant status and configuration data utilizing wireless instrumentation. This information can be used to meet surveillance requirements or to confirm that plant components are in the correct alignment for current or upcoming plant conditions. The communication paths for this information are not business critical and would not run on the I&C communication circuits If this technology would become unavailable or inaccurate, then manual means of conducting the verifications would be invoked. These systems consist of sensors attached to components generally in a non-intrusive manner, in which they are able to sense a parameter (e.g. component position) and transmit that parameter to a processing system that integrates all of the acquired data and determines whether certain specified configurations have been met. These systems can directly output the results of the analysis or put it in the form of a work package. These devices could not be used on Safety Related or Important to Safety systems due to the restriction of wireless communication on Safety. This assessment, found in INL-OLM-CPSI-001, finds that this system is a CDA based on this system being the primary means to meet acceptance criteria of TS surveillance requirement.

CDA Validation	
# of CDAs in Critical System:	1
CDAs added to Scope	**CDAs removed from Scope**
Online Monitoring of Plant Configuration Status	N/A

Safety	ITS	Security	EP	Support
	X			**N/A**

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Critical System Identification						
System Name:	OLM Continuous Plant Status Indication					
New System:	Yes:	X	No:			
Assessment Number:	INL-OLM-CPSI-001					
Safety Related					**Y**	**N**
Is the SSC qualified as safety-related?						**X**
Is the SSC described as safety-related within MR SSC function?						**X**
For new modifications, is the system or specific DA designated as safety-related?						**X**
Important to Safety					**Y**	**N**
Is the SSC used for:						
(1) Radioactive Waste monitoring?						**X**
(2) Fire Protection?						**X**
(3) Seismic monitoring?						**X**
(4) Post-Accident Monitoring?						**X**
(5) Station Blackout protection?						**X**
(6) Anticipated Transient Without Scram (ATWS)/ATWS Mitigation System Actuation Circuitry (AMSAC)?						**X**
(7) Alternate/Safe Shutdown?						**X**
Does the SSC Implement a regulatory commitment affecting an SSEP function, including reactivity?						**X**
Does SSC have the potential to cause one or more of the following:						
(1) Reactor trip or forced shutdown (non-Limiting Condition for Operation [LCO])?						**X**
(2) Inoperable Technical Specification Function ?						**X**
(3) Maintenance rule high safety significant functional failure where a performance criteria of 0 (zero) failures is allowed?						**X**
(4) Failure of a component that causes a Mitigating System Performance Indicator (MSPI) failure?						**X**
Is this a digital SSC that:						
(1) Provides the primary means to meet acceptance criteria of a Technical Specification Surveillance Requirement?					**X**	
(2) Is used in EOPs?						**X**
Does the SSC provide real-time or near real-time plant status of an SSEP parameter to the operators for the safe operation of the plant during transients, and accidents?						**X**
Is this an SSC for which a probabilistic risk assessment has shown that a non-safety related component function is significant to public health and safety?						**X**
Is this an SSC used to establish the defense-in-depth protective strategy, as described in CSP Section 4.3?						**X**
Is this an SSC that performs a non-safety-related function within the scope of the MR and whose compromise could adversely impact the MR function?						**X**
Is this an SSC which has component(s) that could directly or indirectly affect reactivity of a nuclear power plant and could result in an unplanned reactor shutdown or transient?						**X**

Security	Y	N
Does the system perform a function of the Active Vehicle Barrier System?		X
Does the system perform a function to control access into protected and vital areas?		X
Does the system perform a function to the access control system to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions?		X
Does the system perform a function to control keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise?		X
Does the system perform a function associated with issuing a numbered photo identification badge system for all individuals authorized unescorted access to the protected area and vital areas?		X
Does the system perform a function associated with controlling access to keys, locks, combinations, passwords, and related access control devices used to control access to protected areas, vital areas, and security systems?		X
Does the system perform a function for protected area searches (e.gmetal detection, explosive detection, X-ray)?		X
Does the system perform a function for intrusion detection?		X
Does the system perform a function associated with adversary assessment (including realtime and play-back video image system)?		X
Does the system provide a function for an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply?		X
Does the system perform a function to ensure that all areas of the facility are provided with illumination necessary to satisfy the design requirements of 10 CFR 73.55(b) and implement the protective strategy?		X
Does the system perform a function to establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations?		X
Does the system perform a function for interdiction and neutralization?		X
Does the system provide secondary power for intrusion detection or alarm annunciation?		X
Does the system provide secondary power for alarm assessment?		X
Does the system provide secondary for non-portable communications?		X
Does the system provide secondary power for an active vehicle barrier system?		X
Emergency Preparedness	**Y**	**N**
Does the Emergency Plan or implementing procedures require this SSC during a radiological emergency?		X
Is the SSC used for communication in during a radiological emergency?		X
Does the SSC impact emergency declaration and notification capabilities?		X
Does the SSC satisfy self-imposed requirements identified in the Emergency Plan?		X
Support Systems and Equipment	**Y**	**N**
Could the compromise of the support system have an adverse impact on a safety or important-to-		X

safety function?		
Could the compromise of the support system have an adverse impact on a security function?		**X**
Could the compromise of the support system have an adverse impact on an emergency preparedness function including offsite communications?		**X**

If any of the above questions are answered 'Yes,' then the device is considered a CDA. If all questions are answered 'No' then the device is not a CDA and 10 CFR 73.54 does not apply to this device.

Attack Vectors	**Y**	**N**
Does an adversary have logical access to the Asset via a hardwired network?	**X**	
An adversary can have logical access to the Asset via a hardwired network The Asset resides on the business network.		
Does an adversary have logical access to the Asset via a wireless network?		**X**
The asset does not have wireless capabilities.		
Does an adversary have physical access to the Asset?	**X**	
The asset will be stored in a locked server closet on the plant business network Plant-specific controls will be in place for this asset		
Does an adversary have physical or logical access to the Asset prior to or during the licensee's procurement?	**X**	
Both devices will be based on standard, COTS devices An adversary has the ability to infiltrate the device at any point in the supply chain unless plant specific supply chain security controls are applied to a non-CDA.		
Does an adversary have physical access to the portable media and mobile devices that will be used with the Asset?		**X**
The server will have no portable media or mobile device capability.		

CRITICAL SYSTEM AND CRITICAL DIGITAL ASSET ASSESSMENT CHECKLIST --ABBREVIATED--	
	Abbreviated CDA Guidance Form

Cyber Security Assessment Team Approval			
	Print Name	Signature	Date
Preparer:			
Reviewer (Independent Qualified CSS):			
CSAT:			
Final Approval (Site Digital Process Systems Manager or designee):			