Implications of digital instrumentation on nuclear cybersecurity

With all nuclear power plants now required to have a cybersecurity plan, regulations and guidelines are in place that pertain to the protection of critical digital assets.

By Tony Spear and Noel Smith

In an energy market challenged by low-cost natural gas and public subsidization of alternative zero-carbon energy technologies, the nuclear power industry is responding by actively developing methods to reduce the cost of nuclear energy by 30 percent through the Delivering the Nuclear Promise initiative. Updating nuclear control rooms with modern digital instruments to replace the old analog instruments offers a significant cost-saving opportunity. A majority of these control rooms, however, still rely on mechanical instruments using moving-needle technology that was invented in the late 1800s.

Concerns about the cybersecurity aspects of digital instruments have stymied more widespread use despite successful, long-term implementation by the forward thinking owner-operators of a number of nuclear power plants. Given that all nuclear licensees and applicants are now required to have a cybersecurity plan (CSP) in place, a process for adding digital devices at a nuclear plant is a requirement of the CSP and is now a relatively straightforward, if rigorous, undertaking.

This article provides an overview of applicable cybersecurity regulations and guidelines pertaining to the protection of critical digital assets, a summary of the benefits of digital instrumentation, and the specific characteristics related to infrastructure, design, procedures, and training by both the original equipment manufacturer (OEM) and the plant required to ensure cybersecurity. The authors' goal is to provide a road map by which all stakeholders can work together to create additional cost-saving opportunities in support of the Nuclear Promise while protecting the nuclear fleet, and ultimately the public, from the very real dangers posed by cyber threats.

Background

Cybersecurity became an area of emphasis for the Nuclear Regulatory Commission in the wake of the September 11, 2001, terrorist attacks. A number of requirements, regulations, and guidelines subsequently emerged.

The NRC requirements were finalized in March 2009 as 10 CFR 73.54, *Protection of Digital Computer and Communication Systems and Networks,* establishing the requirement for all operators and applicants to have a CSP. According to 10 CFR 73.54, all licensees must establish a CSP that addresses how the licensee will maintain the capability for timely detection and response to cyber attacks, mitigate the consequences of cyber attacks, correct exploited vulnerabilities, and restore systems, networks, and/or equipment affected by cyber attacks.[1]

In January 2010, the NRC issued Regulatory Guide (RG) 5.71, *Cyber Security Programs for Nuclear Facilities,* to provide guidance on how to meet cybersecurity requirements called for in 10 CFR 73.54. This regulatory guide included best practices from several stakeholder organizations, including the International Society of Automation, the Institute of Electrical and Electronics Engineers (IEEE), and the Department of Homeland Security. The Nuclear Energy Institute (NEI) also provided guidance to help operators better understand the following:

- The key components of a CSP.
- A method for determining critical digital assets (CDA).
- The implementation of security defensive architecture, including the determination of cybersecurity defensive levels, boundaries, and acceptable and controlled communications and access between those levels.
- A template for a CSP.
- A number of technical security controls to be implemented within the CSP.
- Operational and management security controls to be implemented with the CSP. [2]

In April 2010, NEI created NEI 08-09, *Cyber Security Plan for Nuclear Power Reactors,* independent of RG 5.71. NEI 08-09 also provides guidance to nuclear facilities about how to comply with NRC regulations and guidelines to implement a CSP.[3] In June 2012, NEI 08-09 (Rev. 6) became the de facto CSP road map when the NRC staff found NEI 08-09 (Rev. 6) "acceptable for use by industry . . . in meeting the requirements set forth in 10 CFR 73.54. This document provides an-

Tony Spear (<tony@otekcorp.com>) is Director of Sales and Marketing at Otek Corporation. Noel Smith (<noel@otekcorp.com>) is Chief Engineer at Otek Corporation.

other template that nuclear power plants can use when submitting CSPs to the NRC for review and approval."[4]

According to NEI, "Every nuclear power plant has an NRC-approved cybersecurity plan."[5] This statement implies that as of this writing, every plant has identified its CDAs, and every plant has also defined a security infrastructure to protect those assets as specified in NEI 08-09 (Rev. 6).

What is a CDA?

According to 10 CFR 73.54, a critical digital asset is any digital computer and communication system and network associated with safety-related and important-to-safety functions; security functions; emergency preparedness functions, including off-site communications; and support systems and equipment that if compromised would adversely impact safety, security, or emergency preparedness.[1, 6]

The above four criteria are commonly referred to as the safety, security, and emergency preparedness (SSEP) functions of the nuclear power plant.

Cybersecurity audits

According to the Office of the Inspector General report, *Audit of NRC's Cyber Security Inspection Program for Nuclear Power Plants* (OIG-14-A-15), "NRC expects licensees to implement their respective Milestone 8 cybersecurity programs beginning in late calendar year 2014 through the end of calendar year 2017."[7] The authors understand that NRC cybersecurity audits have begun and that every licensee and applicant is scheduled to be audited between now and the end of next year. Once these audits are completed and the CSPs are approved, nuclear power plants not currently implementing digital meters as CDAs may incorporate them as such and begin to take advantage of the associated cost and operational benefits of digital. Plants that have already implemented digital instrumentation will be more able to expand their applications and benefits. Provisions for the addition of CDAs within an existing CSP are specified under Section 4.5 of NEI 08-09 (Rev. 6).[3]

Digital versus analog

Modern digital instruments are readily available as form, fit, and function replacements for their analog ancestors. Modern digital instruments feature easy-to-read LED displays and bar graphs to replicate the analog movement of the mechanical needle. A quick summary of the benefits of digital instruments would include the following:

■ *Lower cost*—Fully qualified analog instruments are selling for as much as $10,000 to $25,000 each. Digital instruments suitable for Class 1E applications are available for 40 to 60 percent less.

■ *Improved reliability*—Analog instruments continue to be plagued by stuck needles and the need for frequent calibration. Modern digital products have no moving parts, require little or no calibration after initial setup, and have a calculated mean time between failures of over 25 years.

■ *Better precision*—Where analog instruments read as low as 2 percent of full scale, a four-digit digital readout can display within 0.1 percent. The opportunities for greater operating efficiency of the plant are apparent.

■ *Improved safety*—Digital instruments have the ability to detect over/under input signal conditions and send an alert to the operator and/or network.

Adding digital

As mentioned above, Section 4.5 of NEI 08-09 (Rev. 6) calls for a procedure to add CDAs within the CSP using the same procedures used for initial identification and assessment of CDAs. A process for considering existing analog instruments for replacement would include the following:

■ Identification of any analog instruments that are candidates for digital replacement.

Continued

■ Analysis and identification of those analog instruments that are serving SSEP functions as CDAs that will need to be protected under the CSP. Detailed guidelines for the identification of CDAs appear in both NEI 08-09 (Rev. 6) and NEI 10-04 (Rev. 2), *Identifying Systems and Assets Subject to the Cyber Security Rule*.[6]

■ Incorporation of this new list of CDAs into the existing CSP, using the approved procedures for assessment, analysis, review, and approval.

It is important to note that the implication of the current NEI guidelines and NRC regulations is that any analog instrument not serving an SSEP function would not need to be covered under the CSP. In order to comply with very broad NRC guidelines, however, it has become common for licensees to identify many digital assets as requiring protection, including those with no connection to SSEP. NEI petitioned the NRC in 2014 to revise the working of its cybersecurity rule to eliminate wasteful activity and to focus precious resources on those digital assets necessary to protect the safety and security of the plant.[8]

OEM requirements

In order for an original equipment manufacturer to supply digital instruments to a nuclear power plant to be used as CDAs, there are requirements in the areas of facility infrastructure, development process, and product features that the OEM must implement and identify. These practices will ultimately need to be documented, verified, and incorporated into the CSP.

OEM software development

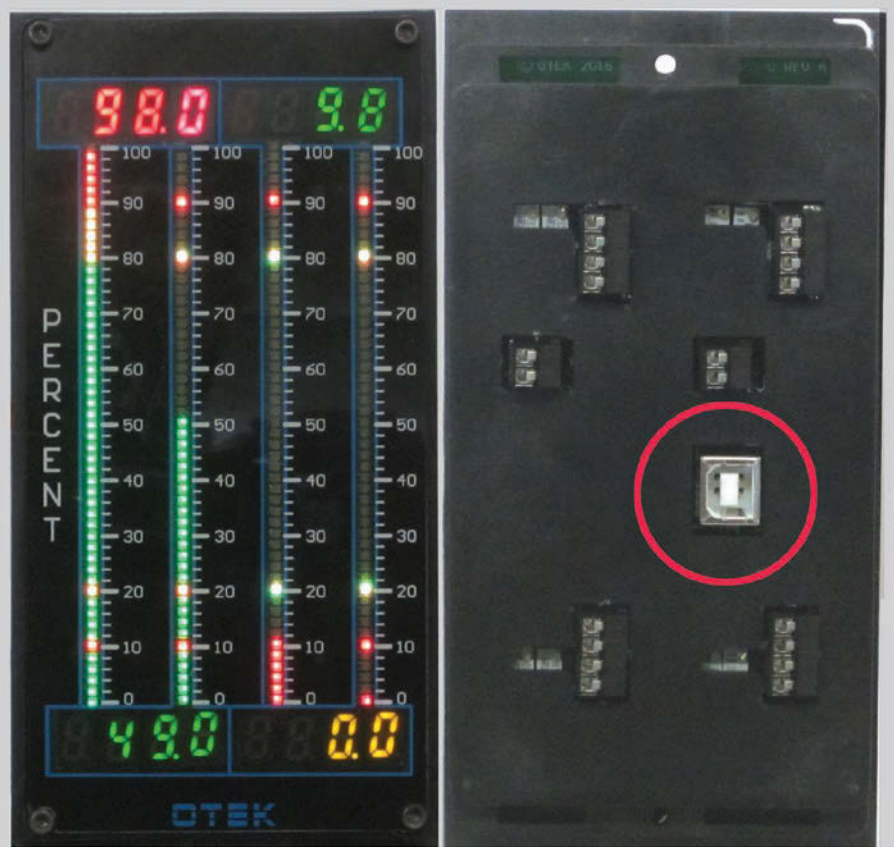
● *Software quality assurance (SQA) plan*—OEMs that develop executable code to be used in a CDA must develop that software in accordance with accepted SQA standards such as IEEE 730-2014, *IEEE Standard for Software Quality Assurance Processes*. Under the IEEE standard, SQA activities are organized into three groups: SQA Process Implementation, Product Assurance, and Process Assurance. In short, the goals of these activities are to define and establish an SQA process that exists separately from individual projects, to evaluate whether the software conforms to product requirements and accepted industry standards, to measure products for quality, and to evaluate and measure the processes used to produce the product.[9]

● *Software Verification and Validation Process (SV&V)*—Any digital product to be implemented as a CDA must go through a stringent SV&V process as part of its qualification for Class 1E safety-related applications. The SV&V will verify the reliable performance of all critical characteristics of the device necessary to perform the required safety function and identify the abnormal conditions and events (ACE) that could interfere with the safety function of the device. A failure modes and effects analysis (FMEA) process can be used to identify the ACEs. The SV&V should also contain specific information about process and product features designed to protect the CDA from cyber attack. The nuclear power plant will review the SV&V document as part of its procurement engineering and dedication procedures.

IEEE Standard 7-4.3.2-2003, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,* provides extensive guidance on a process for ensuring the safety functions of an integrated software and hardware system, including the identification of the safety functions to be performed, the critical characteristics the system must possess in order to perform the safety functions, and testing to validate the implementation of the critical characteristics. The standard also provides guidance for the evaluation of external ACEs and identifies FMEA as an acceptable process for analyzing safety hazards.[10, 11]

A number of the abnormal conditions

and failure modes identified in the SV&V report might be indications of a cyber attack. As part of the ACE and FMEA analysis, the SV&V will identify how the failure is detected, the effect of the failure on the device, and the correct procedure by which to recover from the failure.



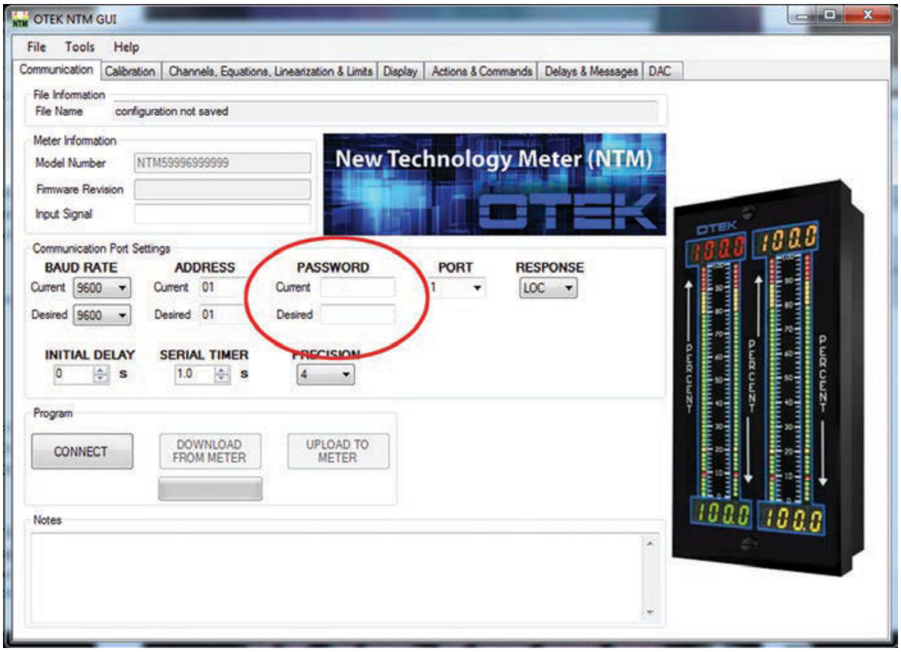
An Otek NTM5 meter with rear-access serial input/output (I/O) port

OEM development environment

OEMs that wish to provide digital products as CDAs to nuclear power plants must also develop those products in an environment that is secure from cyber attack. Certain best practices must be followed and should include, at a minimum, the following:

- Hardware and software development systems should reside behind a firewall. Regular virus protection scans should be performed and documented.
- Source code and compiled code should reside on an “air-gapped” workstation—that is, a computer not connected to the Internet. This workstation should be backed up and virus scanned regularly.
- A “zero-knowledge” backup system, where the host of the backup copy has no access to the unencrypted version of the code, eliminates the possibility of corruption during backup and restore procedures.
- Redundant code techniques such as cyclic redundancy check (CRC) should be added to the executable code stored in the CDA. As part of the manufacturing process, the CRC is recalculated and compared after the executable code is burned into the device to verify that the code has not been corrupted during installation. This process also ensures that neither the source nor the compiled code have been altered by a virus or cyber attack.

All critical characteristics of the digital device, as called out in the SV&V report, are verified by the OEM as part of a final acceptance test. The procedures for this test may be developed jointly by the OEM and the nuclear power plant in order to verify that the device can perform the required SSEP functions. A test report with traceability to the serial number of each device will accompany the devices upon shipment to the plant.



File Information
File Name: configuration not saved

Meter Information
Model Number: NTM59996999999
Firmware Revision:
Input Signal:

Communication Port Settings

BAUD RATE	ADDRESS	PASSWORD	PORT	RESPONSE
Current 9600	Current 01	Current	1	LOC
Desired 9600	Desired 01	Desired		

INITIAL DELAY: 0 s
SERIAL TIMER: 1.0 s
PRECISION: 4

Program

Notes

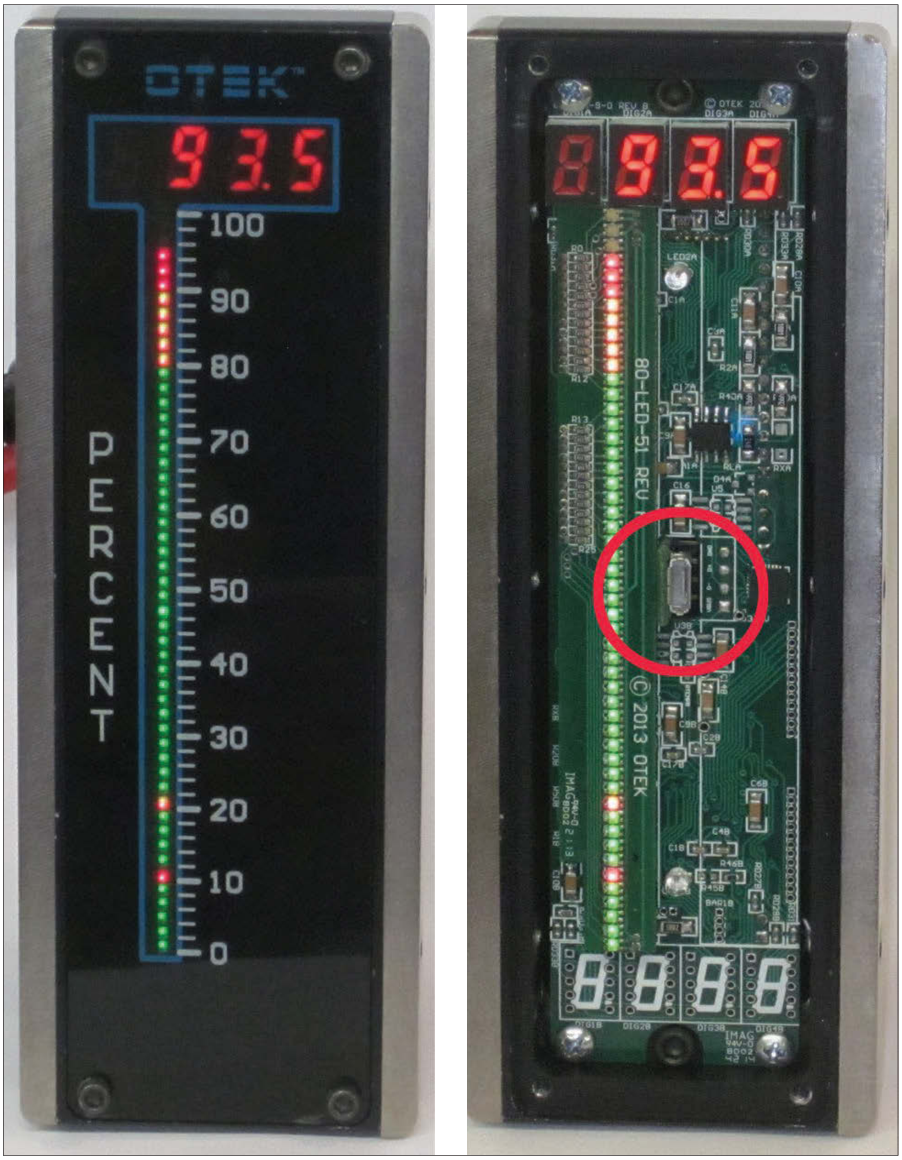
Fig. 1. A screen shot of Otek’s user software interface showing the password protection of the NTM meter configuration

OEM product cybersecurity features

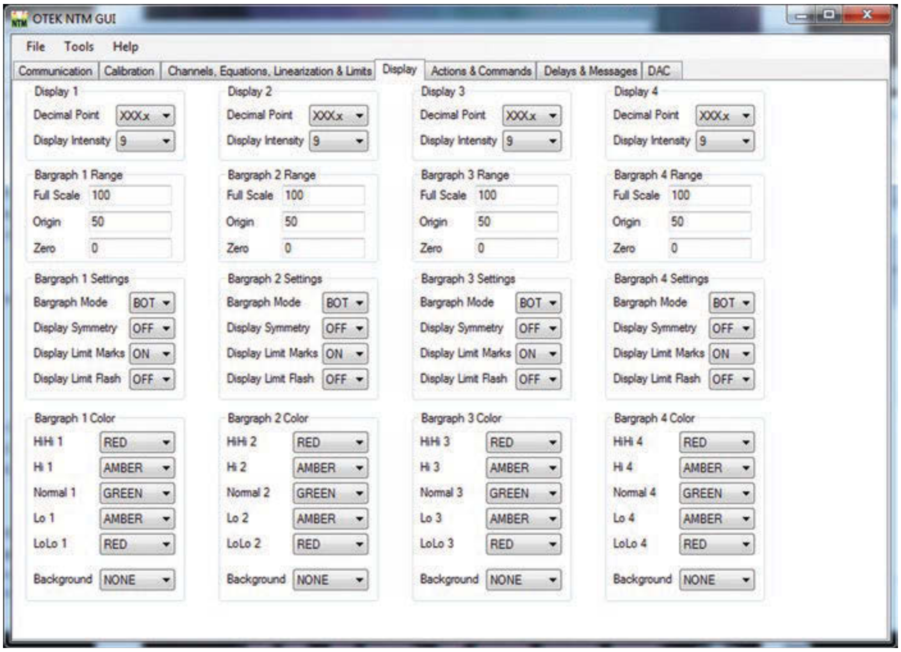
Not only must products be developed in a cyber-secure environment, the device must also be designed with cybersecurity in mind in order to perform its SSEP functions in the field. Product cybersecurity design features should include the following considerations:

- *Physical and logical device access*—Physical access to device functions should be restricted. As an example, access ports for Otek’s New Technology Meter (NTM) series of digital instruments can be specified to be either internal to the CDA or placed behind the control panel (see accompanying photos).

  Logical access to device functions should be password protected with a user-programmable password. User software should be provided with the device in order to ensure a secure user interface. As an example, the NTM series graphical user interface provides this function (Fig. 1).
- *Device code storage*—Executable code should be stored on nonvolatile memory. Field updatable features or configuration data should be stored on the device in a separate location from the executable code. Field updates require the device password and can be performed only through the user software (Fig. 2).
- *Device configurability*—The device configuration function should generate a CRC code to accompany user-editable configuration data. The CRC for the configuration



An Otek NTM9 meter with under-the faceplate access to serial I/O port



Display 1
Decimal Point XXX.x
Display Intensity 9

Bargraph 1 Range
Full Scale 100
Origin 50
Zero 0

Bargraph 1 Settings
Bargraph Mode BOT
Display Symmetry OFF
Display Limit Marks ON
Display Limit Flash OFF

Bargraph 1 Color
HiHi 1 RED
Hi 1 AMBER
Normal 1 GREEN
Lo 1 AMBER
LoLo 1 RED
Background NONE

Display 2
Decimal Point XXX.x
Display Intensity 9

Bargraph 2 Range
Full Scale 100
Origin 50
Zero 0

Bargraph 2 Settings
Bargraph Mode BOT
Display Symmetry OFF
Display Limit Marks ON
Display Limit Flash OFF

Bargraph 2 Color
HiHi 2 RED
Hi 2 AMBER
Normal 2 GREEN
Lo 2 AMBER
LoLo 2 RED
Background NONE

Display 3
Decimal Point XXX.x
Display Intensity 9

Bargraph 3 Range
Full Scale 100
Origin 50
Zero 0

Bargraph 3 Settings
Bargraph Mode BOT
Display Symmetry OFF
Display Limit Marks ON
Display Limit Flash OFF

Bargraph 3 Color
HiHi 3 RED
Hi 3 AMBER
Normal 3 GREEN
Lo 3 AMBER
LoLo 3 RED
Background NONE

Display 4
Decimal Point XXX.x
Display Intensity 9

Bargraph 4 Range
Full Scale 100
Origin 50
Zero 0

Bargraph 4 Settings
Bargraph Mode BOT
Display Symmetry OFF
Display Limit Marks ON
Display Limit Flash OFF

Bargraph 4 Color
HiHi 4 RED
Hi 4 AMBER
Normal 4 GREEN
Lo 4 AMBER
LoLo 4 RED
Background NONE

Fig. 2. A screen shot of Otek's user software interface displaying the NTM meter configuration settings

data should be checked on every device power up to verify that settings have not been altered or corrupted.

- *Safety features*

Watchdog timer: The device should have some type of watchdog timer function that detects a failure of the microprocessor or a failure to receive input signals at certain predefined intervals and that notifies the operator and/or network in the event of a timeout.

Loss of power indication: The loss of power to a CDA should be detectable by the instrument and a signal sent to an external monitoring or alarm function.

Fail-safe control outputs: Digital instruments may contain control functions such as analog output signals or relay contacts. For CDAs, these control functions should be designed to offer a fail-safe operation and generate a reliable external notification in the absence of power or input signal.

ACE and FMEA analysis: As mentioned above in the SV&V discussion, OEMs should design their devices in the context of ACEs and failure modes as possible manifestations of a cyber attack, and should take into consideration the design of device capabilities to detect failures, indicate the nature of the failure to the end user, mitigate the effect of the failure on the rest of the system, and provide procedures by which the end user can recover from the failure.

Digital instruments

Among available digital instruments is Otek's NTM series, designed with nuclear cybersecurity applications in mind. While not intended as a comprehensive list, the following design features of these instruments are included in the product SV&V[10] and are given here as an example of actual product features required for a CDA:

- Password protection of the configuration and calibration of each unit through proprietary user software.
- An internal watchdog timer within the software and a hardware timer external to the microprocessor that work together to guarantee timely operation of the main software loop, as well as constant monitoring of all critical external systems.
- Executable code stored in nonvolatile memory.
- A "signal fail" indication begins immediately after a loss of power and broadcasts for 30 to 60 seconds after the loss of signal power.
- Control relays that contain both normally closed and normally open contact points in order to accommodate fail-safe interaction with the control system.
- Hardware safety limits for output signals to prevent damage to downstream equipment in the event of a failure or cyber attack.

End-User Cybersecurity: In-Plant Best Practices

End-User Cybersecurity of CDA	In-Plant Best Practice
Access of CDA by Network	■ Networked CDAs are protected within plant CSP ■ No networked capability to reconfigure CDA ■ No external access to network containing CDAs
Access of CDA by Personnel	■ Access to privileged functions managed under CSP ■ Each CDA personalized with a unique password at installation ■ Password access limited under operational and security program of CSP ■ Logging, review, and approval of initial/final readings, configuration changes ■ Separation of duties as defined in CSP
Tamper Prevention and Detection	■ Tamper-resistant tape over COMM ports ■ Locking termination hardware
Identification and Recovery from Attack	■ CDA failure modes identified by OEM ■ CDA recovery procedures identified by OEM ■ Network failure modes identified as part of CSP ■ Plant personnel trained to recognize possible failure modes and manifestations within the system ■ Plant personnel trained in recovery procedures as specified by OEM and CSP

CDA = critical digital asset CSP = cybersecurity plan OEM = original equipment manufacturer

End-user requirements

Of course, the end-user nuclear power plants have the greatest share of responsibilities to prevent a cyber attack on their CDAs. The strategies listed below do not represent a comprehensive list, and each plant will need to integrate the CDA within all the provisions of its plant CSP. The following examples reflect those the authors have encountered while working with plants that have implemented digital instruments successfully.

■ *Access to network*

It may be necessary for CDAs to be connected to a network as part of a particular nuclear plant's system design. If this is the case, the network must be protected under the provisions of the CSP as detailed in NEI 08-09 (Rev. 6).

It is currently considered a best cybersecurity practice for plant personnel not to attempt to provide any network capability to reconfigure or disable the digital instrument. This practice would guarantee that the instrument could be reconfigured only when taken out of operation by personnel with correct access privileges.

■ *Access to operating personnel*

● Any updates to the configuration or calibration of the CDA are identified as a privileged function, and access would be managed under the dictates of the CSP.

● Best practice is to change the password of each CDA upon initialization and installation and to assign each CDA a unique password.

● Access to password information should be restricted under the licensee's operational and security program within its CSP.

● Logins to the CDA, initial and final readings, or configuration changes should be logged, reviewed, and approved.

● Separation of duties should be practiced as specified in the CSP.

■ *Tamper prevention*

● Tamper-resistant tape can be used to secure CDA communications ports or faceplates.

● Locking termination hardware can be used to secure signal connections to CDAs.

● Logging of updates to the CDA includes review and approval as specified in the CSP.

■ *Cyber attack identification and response*

● Operating personnel should be trained to recognize any symptoms of possible cyber attack (including specific CDA failure modes as documented in the SV&V) or evidence of tampering.

● Implications of a failed or cyber-attacked CDA upon SSEP function should be analyzed and documented as called for in the CSP.

● Steps to minimize impact to SSEP as a result of failed or cyber-attacked CDA should be incorporated into overall system design.

● Licensee personnel should be trained in the response and recovery procedures specified by the SV&V as well as the CSP.

See table above for a summary of end-user best practices for cybersecurity of CDAs.

References

1. NRC 10 CFR 73.54, *Protection of Digital Computer and Communication Systems and Networks,* <www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html>.

2. NRC Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities,* <www.nrc.gov/docs/ML0903/ML090340159.pdf>.

3. NEI 08-09 (Revision 6) *Cyber Security Plans for Nuclear Power Reactors,* <www.nrc.gov/docs/ML1011/ML101180437.pdf>.

4. *The Nuclear Regulatory Commission Cyber Security Roadmap*; James T. Wiggins, Director, Office of Nuclear Security and Incident Response, SECY-12-0088, June 25, 2012. <www.nrc.gov/reading-rm/doc-collections/commission/secys/2012/2012-0088scy.pdf>.

5. *Nuclear Power Plant Security and Access Control,* <www.nei.org/Master-Document-Folder/Backgrounders/Fact-Sheets/Nuclear-Power-Plant-Security-and-Access-Control>.

6. NEI 10-04 (Revision 2); *Identifying Systems and Assets Subject to the Cyber Security Rule,* July 2012. <http://pbadupws.nrc.gov/docs/ML1218/ML12180A081.pdf>.

7. *Audit of NRC's Cyber Security Inspection Program for Nuclear Power Plants,* (OIG-14-A-15), <www.nrc.gov/docs/ML1412/ML14127A138.pdf>.

8. NEI Policy Statement, *Cyber Security for Nuclear Power Plants*, July 2016. <www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants>.

9. IEEE Standard 730-2014, *IEEE Standard for Software Quality Assurance Processes,* IEEE Computer Society, Software and Systems Engineering Standards Committee, March 27, 2014.

10. V&V Report VVR-351022519-1, Revision 0, Verification *and Validation Report for Otek NTM Meter,* AZZ Nuclear, Feb. 2015 (proprietary).

11. IEEE Standard 7-4.3.2-2003, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,* Nuclear Power Engineering Committee, Sept. 11, 2003. NN