INVESTIGATION OF INSTRUMENTATION CONTAINING AN EMBEDDED DIGITAL DEVICE

T. Jacobi, D. Floyd, and R. Wood
The University of Tennessee
Knoxville, TN 37996-2300
woodrt@utk.edu

A. Hashemian, H.M. Hashemian, and B. Shumaker
Analysis and Measurement Services (AMS) Corporation
9119 Cross Park Drive, Knoxville, TN 37923
alex@ams-corp.com; hash@ams-corp.com; bshumaker@ams-corp.com

ABSTRACT

The U.S. nuclear power industry primarily relies on mature, well-proven analog technology as the basis for most instrumentation and control (I&C) equipment employed in its nuclear power plants (NPPs). However, the market for this legacy instrumentation is very small and availability of such equipment for spare parts or replacement is increasingly limited. Frequently, modern I&C equipment contains embedded digital devices (EDDs), such as microprocessors and programmable logic devices. While the enhanced functional capabilities provided by the digital components offer improved performance, reliability, and maintainability, the corresponding complexity of sophisticated digital implementations also exacerbate concerns about an increased potential for undetected systematic faults, which can lead to common-cause failure (CCF).

As part of a research project sponsored by the U.S. Department of Energy, an investigation has been conducted of commercially available instrumentation marketed for nuclear or industrial application. The objective was to identify the usage of EDDs and to determine the types of functional roles allocated to the devices. Examples of the equipment surveyed include smart sensors, sequencers for emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, and uninterruptible power sources. Where sufficient detail was found, an evaluation was performed to ascertain the nature and role of the digital technology implemented in the instrumentation.

The information gained through this investigation serves as technical input for defining a classification approach for EDDs based on the functional impact of the device. For example, the role of an EDD can involve any of the following functions: performance monitoring and diagnostics, information extraction and communication, instrument condition monitoring and protection, or execution of core instrument functions. Classifying digital devices according to their role in the operation of the instrumentation in which they are embedded can enable determination of the potential functional impact of failure of that device and contribute to determination of the potential safety significance of a CCF event disabling all instances of that device.

This paper will report on the findings of the investigation of instrumentation with EDDs and indicate considerations for the emerging classification approach. The higher-level goal of this effort is to determine whether a graded approach to qualification testing may be possible based on classification.

Key Words: instrumentation and control, embedded digital device, common cause failure

1 INTRODUCTION

The instrumentation and control (I&C) equipment used in currently operating U.S. nuclear power plants (NPPs) is primarily based on mature analog technologies that are progressing towards obsolescence. The continued reliance on this legacy analog technology, which is also being propagated into new NPP designs, imposes performance penalties and maintenance burdens in comparison with newer digital I&C alternatives that contain embedded digital devices (EDDs) such as microprocessors and programmable logic devices [1]. Experience in other industries such as avionics has shown that digital I&C equipment containing EDDs can provide significant benefits over analog-based equipment in terms of performance, reliability, and maintainability. In recent years, due to the high demand for digital technologies in the industrial I&C marketplace, it is becoming increasingly difficult for NPPs to acquire instrumentation that is not equipped with an EDD. However, the nuclear power industry has been slow to adopt digital technology, especially in safety-related systems, in large part as a result of regulatory concerns about common-cause failure (CCF) vulnerabilities of equipment with EDDs [2].

This paper summarizes some of the current regulatory issues regarding the use of EDDs in safety-related systems, and reports on research performed by the authors to identify the functional roles of EDDs in use in the nuclear industry. The goal of the research is to develop a classification system for EDDs according to their role in the operation of the device in which they are embedded to facilitate the determination of the potential safety significance of a CCF event disabling all instances of that device. The higher-level goal of this effort is to determine whether a graded approach to qualification testing may be possible based on classification that will help simplify the process of qualifying and implementing digital I&C in NPPs.

2 SUMMARY OF REGULATORY ISSUES

In 2016, the U.S. Nuclear Regulatory Commission (NRC) issued a Regulatory Issue Summary (RIS) on potential safety issues associated with the use of equipment with EDDs in safety applications [2]. The NRC RIS defines an EDD as "a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, and that is integrated into equipment to implement one or more system safety functions." It further notes that firmware includes "programmable logic devices, field programmable gate arrays, application specific integrated circuits, erasable programmable read only memory, electrically erasable programmable read only memory, and complex programmable logic devices." Equipment with EDDs can include sensors, breakers, priority logic modules, time-delay relays, pumps, valve actuators, motor control centers, and uninterruptible power supplies. The RIS discusses the issues associated with EDDs and identifies prevailing regulatory positions and guidance. In particular, NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-19 is cited in regard to assessing and mitigating the impact of CCFs [3].

BTP 7-19 identifies two design attributes that are acceptable for eliminating CCF concerns: (1) diversity or (2) testability (specifically, 100% testability). Either solution can result in high costs and remaining licensing uncertainty. For increasingly complex digital devices, it is not practical to achieve exhaustive testing with conventional methods due to the enormous number of test vectors (e.g. all combinations of state and inputs) needed to effectively approach 100% test coverage for the device [4]. Consequently, many utilities and reactor designers have limited or avoided more extensive use of digital technology to minimize licensing, scheduling, and financial risk. Without development of cost effective qualification methods to satisfy regulatory requirements and address the potential for CCF vulnerability associated with embedded digital devices, the nuclear power industry may not be able to realize the benefits of digital technology achieved by other industries.

Although the acceptable design attributes of diversity or 100% testability described in BTP 7-19 may not be practically achievable for some digital I&C implementations, experience at U.S. NPPs resulting from

issues with communications and electromagnetic compatibility (EMC) reiterate the importance of ensuring quality and reliability of safety-related equipment with EDDs:

- In August 2006, a manual reactor trip occurred following the loss of 3A and 3B reactor recirculation pumps. The pump variable frequency drive (VFD) controllers became unresponsive, and the condensate demineralizer controller (CDC) failed simultaneously with the VFD controllers. Both the CDC and VFD controllers are connected to the Ethernet-based plant integrated computer system network, and due to excessive network traffic, they failed simultaneously resulting in a manual reactor trip [5].
- The manufacturer of time delay relays redesigned them to use a complex programmable logic device (CPLD) in place of the original solid-state integrated circuit logic chip. This design change was not identified by the dedicating entities, and as a result, the design change was not evaluated. During an emergency diesel generator (EDG) loading test, it was determined that EDGs 3 and 4 could simultaneously been unable to tie to their respective emergency buses, resulting in a loss-of-safety function of the onsite standby alternating current power source. This was due to the time delay relays in the breaker control logic that were susceptible to electrical noise from electrically connected or nearby relays de-energizing, which could have prevented the output breakers from properly closing under certain conditions [6].

In these cases, the CCFs associated with these devices resulted or could have resulted in concurrent failure of critical functionality. However, not all functionality implemented by EDDs, such as digital displays, are necessarily critical for operation of the devices. Nevertheless, the NRC guidance requires utilities to achieve diversity or 100% testability for safety-related applications to eliminate the need to consider potential CCF regardless of the ultimate effect on critical functionality resulting from a CCF.

As an alternative to the strict diversity or 100% testability requirements, the authors are researching the practicality of defining a classification approach for EDDs based on the functional impact of the device to facilitate a graded approach to qualification testing. The focus of the classification approach is to better characterize the role of the embedded digital device in accomplishing the safety function of the instrument. Basically, the approach is to determine and/or verify the various responsibilities of EDDs so that the potential impact on the safety function(s) of CCF in the EDD can be classified to enable establishment of a graded scheme for determining the level of evidence and extent of analysis necessary to assess whether a device is subject to CCF. As part of this research, an investigation of available "smart" devices was conducted to identify the type of equipment on the market and determine the range of functions performed by the EDDs.

3 IDENTIFICATION OF EQUIPMENT WITH EDDS

The first step in defining a classification approach for qualifying EDDs involved surveying equipment vendor catalogs, websites, and industry personnel to compile a listing of the digital equipment containing EDDs that are available for implementation by nuclear facilities. The purpose of the survey was twofold: (1) to generate a representative list of equipment with EDDs that are being marketed to the nuclear industry, and (2) to evaluate the functionality that the EDDs provide in terms of the functionality of the devices in which they are embedded. Table I shows the listing of the types of devices that were investigated in this research and the number of devices that were evaluated.

Note that several other devices were also investigated as part of the research, but Table 1 only lists the devices that were determined to contain EDDs. The devices listed in Table 1 are current products of several manufacturers including Rosemount, Yokogawa, Foxboro, Siemens, Eaton, Trippline, and Westinghouse. Although the listing in Table 1 is not exhaustive, it served as a starting point to begin the investigations of the EDD functionality of the devices that are presented in the next section.

Table I. Devices with EDDs evaluated for this project

Device Type	Number of Devices
Transmitter	88
Actuator	55
Uninterruptible Power Supply (UPS)	145

4 SUMMARY OF EDD FUNCTIONALITY

This section provides details regarding the functionality of the EDDs in the devices that were researched as part of this project. Table II provides a breakdown of the device types that were researched and the functionality that EDDs provide in the devices.

Table II. EDD functionality by device type and application

Device Type	Application	EDD Functionality
Transmitter	Temperature, Pressure, Flow, and Level Measurement	Communications, Diagnostics, Calibration
Actuator	Motor Control Center, Positioner, Solenoid Driver, Linear Actuators, Rotary Actuators, Electric Actuators	Communications, Diagnostics
Uninterruptible Power Supply (UPS)	Line-Interactive, Online Double-Conversion, Standby	Output monitoring, Communications, Diagnostics

A recurring feature and function of EDDs is self-diagnosis. Though the actual instrumentation method for a digital component may be the same as its analog counterpart, self-diagnostics detect and report faults, which potentially save maintenance effort. Self-diagnosis is represented in all of the transmitters, actuators, and UPSs evaluated as part of this research. Self-calibration, another common feature, is a natural extension of detecting deviations from normal operation. These devices usually do not actually lack any calibration step; rather, they can be digitally set to a previously-performed calibration, so that a long calibration step is shortened. These self-diagnostic and self-calibrating features are often accessed with software that comes with the purchase of the device. There is no baseline software common to each of these devices, nor even an accepted set of consensus software functions; each vendor supplies their own brand of management software, which poses potential challenges that could compromise reliability independent of the fundamental design of the instrument—thus, the software quality and reliability must be evaluated as well.

4.1 Transmitters

The surveyed transmitters consisted of 26 temperature transmitters, 20 ultrasonic flow meters, 19 flowmeters, 6 level transmitters, and 17 pressure transmitters. In many cases, EDDs in transmitters involve a microprocessor and/or microcontrollers that are critical components for measurement. Figure 1 shows a typical case, adapted from the Siemens SITRANS TH200 schematic, where the circuit path must go through the microcontroller.

Transmitters with EDDs typically use one or more of several protocols to communicate digitally: Highway Addressable Remote Transducer (HART) Communication protocol, FOUNDATION fieldbus protocol, PROFIBUS PA protocol, or WirelessHART protocol.

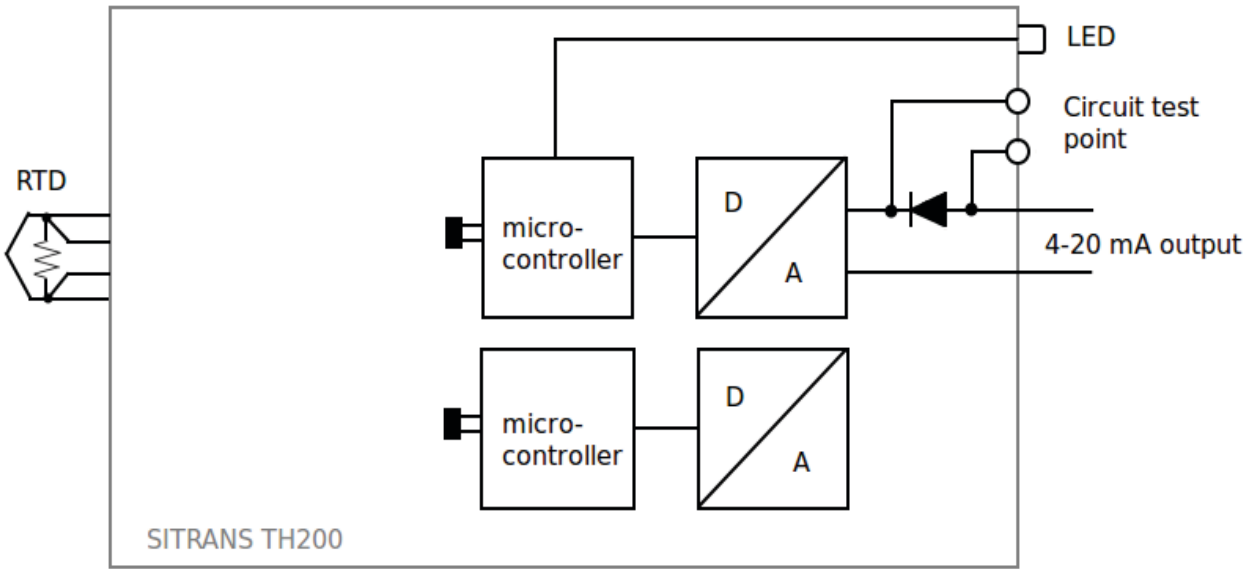

Figure 1. Simplified schematic of the Siemens SITRANSTH200 temperature transmitter

HART is a standard method of embedding additional digital information in an analog signal, as part of the same current. The current is as normal for transmitters, between 4mA and 20mA, and is interpreted normally by analog devices. However, waves are also superimposed on the analog waveform, so that its current output varies slightly but does not disrupt the analog reading. The frequencies of these waves represent the digital signal—1200 Hz as a 1 bit, or 2200 Hz as a 0 bit. The HART protocol transmits 1200 bits per second. WirelessHART is digital-only, and communicates the digital signal wirelessly in the same frequency-dependent way. FOUNDATION fieldbus is digital-only, but can be used with wired or wireless signals, and has a significantly higher bandwidth than HART.

Both WirelessHART and FOUNDATION devices typically use these protocols to act as a self-organizing, self-healing network, which increases reliability and ease-of-use over hierarchical data collection. Like other device types, available information on the transmitters does not explicitly address provisions for mitigating microprocessor failure, with the notable exception of the HART version of the Rosemont 3144P. In that case, an independent circuit triggers an alarm if the microprocessor fails, whether the failure takes place in hardware or software. A typical EDD transmitter will condition its output signal with its microprocessor, so a failure in the microprocessor cuts off the output signal.

The level transmitters with EDDs largely rely on a method for which digital response is crucial: Guided Wave Radar (GWR). A GWR level transmitter sends a microwave pulse down a partially-submerged probe in the location where the liquid level is to be determined, and records the time it takes for the pulse to reflect off the liquid's surface where the probe enters the liquid. The high speed of the pulse requires a microprocessor to measure this time, and is further necessary to convert time into liquid level. GWR is an advantageous method for level transmitters, because it is largely unaffected by the conditions surrounding the liquid level—liquid density, pressure, and temperature will not affect the reading, which would suit this technology well for the extreme environment of a reactor vessel, after qualification.

4.2! Actuators

A total of 55 actuators of various designs were found to be marketed as intelligent or digital actuators. Among these were motor control centers, positioners, solenoid drivers, linear actuators, rotary actuators, and electric actuators. Similar to the transmitters, the smart capabilities of these devices range from

communication protocols to advanced diagnostic and monitoring functions. The advanced capabilities of these devices provide a deeper view into the operation of the device along with being able to increase the reliability of the device.

The most common digital enhancement is the usage of digital communication protocols such as Modbus, Profibus, and FOUNDATION field bus communications and some forms of Ethernet communications along with some instances of the HART communication protocol. Commonly, advanced diagnostic functions provide more information concerning the health and reliability of the device, via the on-board electronics of the device and manufacturer-specific software. For software-based devices, the software allows for remote access and real-time monitoring of the device. The software can also provide decreased set up times via faster calibration and easy access to the device.

Almost all actuator devices advertise diagnostic functions, but there is little information concerning the exact nature of provided diagnostic functions—rather that they simply improve operation. There are some instances of specifically stated diagnostic functions. These devices can conduct partial and full-stroke tests on the attached valve and can be conducted using the manufacturer's software, performed over digital communication protocol. Some of the software provides a diagnostic function that allows for predictive maintenance and for scheduled maintenance intervals. This is possible through the provided software because the software helps to monitor the health of the device.

Intelligent motor control centers are provided with a wide range of communication and advanced capabilities. These motor control centers have provided communication protocols such as Ethernet connectivity, Modbus RTU, Modbus TCP/IP, and PROFINET along with some others. There are also some models that support the use of the communication protocol DeviceNet that allows the motor control center to directly connect to distributed controls systems and programmable logic controllers. Along with this, some models support fault monitoring and the ability to provide the status of the device. Some models come with vendor-specific monitoring software and/or self-diagnostics.

Multiple valve actuators such as electric, rotary, and linear actuators are marketed with a variety of smart capabilities. Some of these smart capabilities are provided through the use of digital communication protocols, and for some models, this provides simultaneous control over multiple actuators. These, too, often have self-diagnostics and can be calibrated remotely, the latter being useful for the often-hazardous environments of valves.

4.3 Uninterruptible Power Supplies (UPS)

Of the 145 surveyed uninterruptible power supplies (UPSs), 76 are line-interactive, 49 are on-line double-conversion, and 11 are standby UPSs. The nine remaining were described differently, with five as simply "on-line", one as "on-line single phase", one as "on-line three phase", and two using an undetermined ferro-resonant topology.

The primary function of EDDs in the surveyed UPSs was monitoring output, and to that end, there exist a variety of models with various networking ports, often multiple at once. Most vendors carry at least one series of models with a Simple Network Management Protocol (SNMP) card, allowing the UPS to be accessed remotely, or even over the Internet. These report the UPS's electrical variables in real time—voltage, frequency, battery charge, load, etc.. Most UPSs were also compatible with a vendor-specific monitoring software—the Intelligent Power Software Suite for Eaton models, PowerPanel Business Software for CyberPower models, and PowerAlert for Tripplite.

These UPSs also sometimes allowed for battery health monitoring, and as a rule, provide more thorough self-diagnostics than other devices. Because the most capable UPSs can connect to the Internet outright, some models send notices and reports to its operators, allowing for notifications such as emails to be sent to maintenance technicians to address a developing fault. This capability is seldom seen in other

types of surveyed devices. Though it ensures that faults can be addressed proactively, cybersecurity provisions would be necessary to ensure protection of nuclear-qualified UPSs.

5 CONCLUSIONS AND FUTURE WORK

An investigation of available "smart" devices was conducted to both identify the type of equipment on the market and determine the range of functions performed by the EDDs. A primary objective of this task is to support definition of a classification approach for equipment with an EDD based on the functional impact of the device. Classifying digital devices according to their role in the operation of the instrumentation in which they are embedded can enable determination of the potential functional impact of failure of that device and contribute to determination of the potential safety significance of CCF disabling all instances of that device. Consequently, a graded approach to qualification testing may be possible based on classification.

The focus of the classification approach is to better characterize the role of the embedded digital device in accomplishing the safety function of the instrument. The approach is to determine and/or verify the various responsibilities of EDDs so that the potential impact on the safety function(s) of CCF in the EDD can be classified to enable establishment of a graded scheme for determining the level of evidence and extent of analysis necessary to assess whether a device is subject to CCF. The high (integral to execution of the safety function) and low end (no role in the safety function) of the classification structure are obvious but the intermediate levels (and any thresholds for graded treatment of CCF) are not obvious.

Ongoing research involves an analysis of the findings of this investigation to enable development of an initial classification approach. In related work, a process for accounting for equipment with EDDs in a diversity and defense-in-depth analysis has been defined. This process provides a framework for accommodating a graded treatment of equipment with an EDD based on its classification according to the functional role assigned to the EDD [7].

6 ACKNOWLEDGMENTS

This material herein is based upon work supported by the U.S. Department of Energy, Office of Nuclear Energy, under the Nuclear Energy Enabling Technology (NEET) Advanced Sensors and Instrumentation (ASI) Program. The authors would like to acknowledge Suibel Schuppner, the DOE NEET ASI program manager, for her oversight and assistance on this project. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

7 REFERENCES

1. E. Quinn, J. Mauck, and K. Thomas, "Digital Technology Qualification Task 2 – Suitability of Digital Alternatives to Analog Sensors and Actuators," INL/EXT-12-27215, Idaho Falls, ID, INL (2012).
2. U.S. Nuclear Regulatory Commission (NRC), "NRC Regulatory Issue Summary 2016-05 Embedded Digital Devices in Safety-Related Systems," NRC, ADAMS Accession No. ML15118A015, Washington, D.C. (2016).

3. U.S. Nuclear Regulatory Commission (NRC), NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” (SRP), Chapter 7, Branch Technical Position 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 6, ADAMS Accession No. ML110550791 (July 2012).
4. National Institute of Standards and Technology (NIST), “Practical Combinatorial Testing”, NIST Special Publication 800-142 (October 2010).
5. U.S. Nuclear Regulatory Commission (NRC), "Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," NRC Information Notice: 2007-15, ADAMS Accession No. ML071010303, Washington, D.C. (2007).
6. U.S. Nuclear Regulatory Commission (NRC), "Recent Issues Related to the Commercial Grade Dedication of Allen Bradley 700-RTC Relays," NRC Information Notice 2016-01, ADAMS Accession No. ML15295A173, Washington, D.C. (2016).
7. R. Wood, J. Mauck, and E. Quinn, “Addressing Embedded Digital Devices in Safety-Related Systems of Nuclear Power Plants,” *Proc. of NPIC&HMIT 2017*, San Francisco, CA, June 11-15 (2017).