Things to Consider When Upgrading a Non-Power Reactor to a Digital I&C System

M. D. Muhlheim,[a] L. A. Hardin, Jr.,[b] D. A. Hardesty,[b] and T. L. Wilson, Jr.[a]

[a]*Oak Ridge National Laboratory*
P.O. Box 2008, Oak Ridge, TN 37831
muhlheimmd@ornl.gov, wilsontljr@ornl.gov

[b]*U.S. Nuclear Regulatory Commission*
Washington, DC 20555
leroy.hardin@nrc.gov, duane.hardesty@nrc.gov

INTRODUCTION

Non-Power Reactor (NPR) licensees are increasing their use of state-of-the-art digital technology in instrumentation and control (I&C) systems because digital systems offer improved reactor control, information processing, and information storage.[1]

DIGITAL CONTROL SYSTEMS

Digital I&C systems at NPRs range from experimental systems for reactor control research, to measurement and display systems designed and fabricated by licensees, to complete reactor console replacements.

Obsolescence

As with power reactors, it has become increasingly difficult for operators of many old NPRs to find spare parts for their original analog I&C systems. Many organizations have begun or have plans to upgrade, refurbish, or replace their old analog I&C systems with digital systems.

The perception is that upgrading to a digital I&C system will solve all of a facility's obsolescence problems. However, experience with NPRs on an international level has shown that upgrades to hardware and software may be necessary as frequently as every 2 years, with software updates being especially problematic. In fact, one of the dominant causes of application software failure is latent faults introduced during maintenance because of software modifications, setpoint changes, and version revisions in spare parts.[2] Even though a part may have the same product code or parts list number, it may perform differently because the software has been updated by the vendor.[3]

Complicating matters is that as part complexity increases, product lifetime decreases. In addition, the short production cycles of today's digital components means that components likely will become obsolete within 5 years. Whereas power reactors may have adequate resources or contracts that ensure long useful lives (i.e., they buy and store critical parts to ensure availability for 10–20 years), NPRs may have to upgrade more frequently because of the high cost to acquire, store, and maintain a long-term supply of spare parts.

Availability of Technical Support

The transition to digital equipment requires experienced staff with skill sets very different from those required to maintain the current analog equipment. In the nuclear power industry, a variety of expert personnel are responsible for the operations, maintenance, and testing of I&C, electrical, and mechanical systems. In the case of an NPR, however, one person may be responsible for maintaining many of these systems, while also overseeing the overall operations of the facility. Increasing the complexity of the I&C system exacerbates this potential technical overload on limited NPR staff.

Sensor Signals and Control Power

The control room of an NPR, which contains the control console and other status display instruments, is the hub of reactor facility operation. It is the location to which all information necessary and sufficient for safe and effective operation of the facility is transmitted, and the primary location from which control and safety devices are actuated either manually or automatically. The console contains most of the circuitry and hardware for organizing and processing the information either analytically or digitally, applying decision logic, or routing signals to display devices or automatic action of other subsystems or both. However, the sensors and monitored signals from other systems are located outside the control room; these are the inputs on which the reactor trip system and engineered safety features actuation system (if needed) act. Typically, the hardware and software architecture should meet the single failure criterion, and maintain channel separation and separation between Class 1E and non-1E systems.

Notice: This manuscript has been co-authored by UT-Battelle, LLC, under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The information presented in this paper represents the views and assessments of the authors and are not necessarily those of the U.S. NRC or ORNL. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

Because these criteria did not exist at the time many of the NPRs were constructed, they do not fully meet the separation criterion. In addition, although some NPRs installed nuclear power plant–qualified I&C systems, the control room is not qualified for a seismic event. If seismic protection is required, it should apply to the entire facility.

New Failure Mechanisms May Be Introduced

It must be recognized that the introduction of software and microprocessors could create new failure mechanisms, such as software errors and electromagnetic interference.[4] These failure mechanisms may cause the reactor to malfunction in a way not previously considered. For example, at one NPR, after replacing an analog system with a digital system, the new system performed as expected under steady state conditions. However, with regard to transients in process variables, spikes that were filtered out in the analog system were not filtered out in the digital system, causing a spurious reactor trip. Capacitors were added to solve the new and unexpected failure mode.

Serious Accidents Can Occur at Very Small or Zero-Power Reactors

The level of risk for an NPR is small because of the low thermal power level, the short operating cycle, strong inherent safety, mild environments, and less tendency for fuel damage following a loss-of-coolant accident or core uncover event. History, however, has shown that low power does not necessarily equate to no hazards. The reality is that three of the four accidents with fatalities at NPRs occurred at essentially zero-power facilities (RB in Vinca, Serbia, October 1958; SF3 in Kurchatov, Russia, May 1971; RA-2 in Buenos Aires, Argentina, September 1983).[5] Fortunately, all the lessons learned from these events (and the SL-1 accident in Idaho in January 1961) are currently considered in the design and operation of NPRs.[6] These accidents show that the reviews of digital I&C upgrades must ensure that the public health and safety are not compromised.

Operating experience in the United States indicates that NPRs have good overall safety performance. None of the presently operating NPRs has had recent incidents affecting public health and safety and none of the recent operating events has resulted in fuel damage or radiation releases in excess of regulatory limits.

CONCLUSIONS

In Generic Letter GL 95-02, the NRC recognized that the design characteristics specific to the new digital electronics could result in failure modes and system malfunctions that either were not considered during the initial plant design or not evaluated in sufficient detail in the safety analysis report.[7] These concerns include potential common mode failures. A conversion from analog to digital I&C systems in NPRs solves some problems while potentially introducing others. Good design, engineering, review, and testing can identify and minimize these risks.

REFERENCES

1. A. Adams, Jr., “Regulatory Issues Concerning the Installation of Digital Systems at Non-Power Reactors,” ANS 1991 Winter Meeting, November 10–14, 1991, San Francisco, CA.
2. R. Torok, EPRI Project Manager, *Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions*, May 16, 2008. (ML090860465)
3. W. Petrick, *Requirements Engineering for Digital Upgrades, Specification, Analysis, and Tracking*, TR-108831, Electric Power Research Institute, Palo Alto, CA, December 1997.
4. K. Korsah, *An Investigation of Digital Instrumentation and Control System Failure Modes*, ORNL/TM-2010/32, Oak Ridge National Laboratory, Oak Ridge, TN, March 2010.
5. T. P. McLaughlin et al., *A Review of Criticality Accidents, 2000 Revision*, LA-13638, Los Alamos National Laboratory, Los Alamos, New Mexico, May 2000. (ML003731912)
6. U.S. NRC, *Survey of Non-Power Reactors.* (ML003706367)
7. U.S. NRC, “Use of NUMARC/EPRI Report TR-102348, ‘Guideline on Licensing Digital Upgrades,’ in Determining the Acceptability of Performing Analog-to-Digital Replacements under 10 CFR 50.50,” NRC Generic Letter 95-02, April 26, 1995. (ML031070081)