ISSUE STATEMENT

Operating nuclear plants are gradually transitioning much of their aging and obsolete instrumentation and control (I&C) equipment from analog to digital technology. However, plants have experienced significant unanticipated costs, delays and operating events associated with digital system implementations. As a result, the risks associated with I&C upgrades are often judged to be greater than the risks of continuing to operate with obsolete analog equipment. New nuclear plants will be ‘all digital;’ they will use more extensive and highly integrated I&C systems than existing plants. While their digital issues are largely the same, the increased complexity will often require new or extended solutions, with corresponding cost and schedule risks. The industry needs updated methods and tools that address digital-specific technical issues and help engineers anticipate and mitigate potential vulnerabilities before putting the digital systems into operation in the plants.

DRIVERS

Much of the current analog equipment has aged to the point where replacement is inevitable, plants implementing new digital I&C systems are experiencing unexpected and costly problems, and new build I&C systems will use approaches not yet proven or licensed in nuclear plants.

Aging and Obsolete Equipment

In many cases existing analog equipment has become difficult or impossible to maintain. Suppliers have discontinued support, spare parts are no longer available, and expertise has been lost through attrition and retirement. License renewal and extended fuel cycles exacerbate this problem. While it is possible to extend the lives of some analog systems by using enhanced maintenance practices and reverse-engineered replacement parts, this approach becomes more costly and less effective over time. Also, it typically cannot provide key digital technology benefits, such as performance improvements and elimination of single point vulnerabilities.

Just as the aging analog systems are becoming less reliable, expectations for equipment reliability and plant availability are increasing. Analog I&C plants have many single point vulnerabilities that digital technology can eliminate, with corresponding reliability and safety benefits. Power uprates often introduce new conditions and performance requirements (e.g., accuracy, response time) that require digital technology. New builds face unprecedented expectations of operating excellence, even at initial startup.

Negative Experiences with Digital I&C Replacements

Digital upgrades at several plants have incurred significant unanticipated costs due to inadvertent plant trips, extended outages to correct start-up issues, project delays due to protracted regulatory reviews, and even project cancellations. Key factors are inexperience with digital technology, the need for updated methods and tools that address digital-specific technical issues, and a paradigm shift to foster awareness of the issues and adapt utility and vendor processes, organizations and skill sets accordingly.

New Plants will be “All Digital”

New plants will use highly integrated digital systems that push the technical and regulatory concerns beyond the experience of operating plants. Managing digital issues such as cyber security, human factors engineering (HFE), safety-to-non-safety communication, and hazard analysis will require improved analytical methods, guidance and training.

RESULTS IMPLEMENTATION

This project will develop improved methods and guidance that will enable nuclear utilities, their equipment suppliers and system integrators to cost-effectively implement and maintain digital I&C with reduced risk of unanticipated costs and undesired behaviors. EPRI research will develop the technical bases and methods to improve plant processes for I&C modifications and address key issues, such as hazard analysis to find and mitigate vulnerabilities before installation, cyber security, and human factors engineering for digital control room interfaces. EPRI products will include technical reports, guidelines, and companion training materials to enable utilities to apply the research results and update staff on the latest issues and solutions. EPRI will also provide technical input to NRC Research to inform regulatory issues under the existing EPRI/NRC memorandum of understanding.

The EPRI digital I&C research results will play a key role in supporting the Delivering the Nuclear Promise initiative in the U.S., where owner/operators and industry oversight organizations will apply EPRI research results to help ensure that utility engineers maintain competence on digital issues, that utility processes are updated to address specific digital system concerns such as configuration management and common-cause failure, and that the processes are being applied appropriately.
In some cases, EPRI research results may be used to provide a technical basis or resolution of a regulatory concern. Example topics of this type include cyber security, electromagnetic compatibility (EMC), and assessing the likelihood of potential software common-cause failures introduced by digital upgrades in safety and non-safety applications.

EPRI research results will provide the basis for computer-based training (CBT) modules on digital issues that will be made available through normal EPRI channels, and for selected topics, through INPO’s on-line training systems. Utilities will apply EPRI guidance and training materials to maintain proficiency in managing digital I&C from specification to design evaluation, testing, implementation, operation and maintenance. They will require suppliers, integrators and contractors to apply these materials on an as-needed basis. In some cases, operating plants may elect to wait for key issues to be resolved via new plant builds, and then apply the proven solutions to reduce schedule, cost, and regulatory risks.

**PROJECT PLAN**

EPRI will develop improved methods and guidance for addressing digital issues on a topic-by-topic basis and for enhancing design and engineering change processes, including newer approaches like systems engineering techniques. Technical advisory committees (TACs) comprised of knowledgeable utility and industry representatives will guide product development and act as reviewers and contributors to ensure that the products have appropriate scope, detail and practical utility for their intended users. Products will include detailed procedures, worked example problems, industry workshops and training materials. They will be updated on an as-needed basis as new information and operating experience become available and as new issues come to light. Key topic areas of upcoming research include:

*Failure/Hazard Analysis, Including Protecting Against Common-Cause Failure*

It is highly desirable to identify and mitigate potential digital vulnerabilities before the system is operating in the plant. Traditional hardware failure analysis methods are not well-suited for digital technology. Software does not wear out. It can be highly complex, and failures typically result from design errors and unanticipated system interactions. This project has researched existing and emerging approaches and developed guidance for applying selected methods in nuclear plants. It will continue the effort with plant demonstrations, development of tools to streamline steps that are tedious and labor intensive, and improved training and technology transfer methods that will help utilities come up to speed on new and improved hazard analysis methods.

**Cyber Security**

Nuclear power plants face evolving cyber security threats and regulatory requirements for digital devices, components, and systems. Implementing cyber security design and operational controls for new and existing instrumentation and control (I&C) systems requires cyber security experts, I&C engineers, and procurement organizations to work together with vendors to implement and maintain an effective cyber security posture. Improper or incomplete implementation of controls and methods can result in costly retrofits. This focus area is researching cyber security approaches and developing practical methods for nuclear plant applications in coordination with other EPRI sectors as part of a strategic imperative.

**Human Factors/Advanced Operations via the Control Room**

Human factors engineering (HFE) is important to maintaining safe, reliable and cost-effective operation of the plant. It is also a regulatory requirement. Human error continues to be a significant contributor to events that have occurred at operating plants, and appropriate application of HFE can help reduce the chances for error, increase human performance levels and reduce challenges to the plant. Products will include updated and expanded human factors guidance, including guidance on integrating HFE with other engineering processes, as well as training materials and improved decision-based interface designs.

**Design and Use of New Technologies, Such as Field Programmable Gate Arrays (FPGA) in High Integrity Applications**

Digital technologies are rapidly evolving; this project is investigating promising new devices and approaches for nuclear plant applications. As an example, field-programmable gate arrays (FPGAs) are gaining increased attention worldwide for use in nuclear power plant I&C systems, particularly for safety applications. The use of FPGAs might reduce complexity and the associated burden of gaining regulatory approval and provide better protection against obsolescence compared to conventional microprocessor-based systems. The project is developing guidelines, case studies and design criteria for application of new digital technologies in nuclear plant I&C systems, addressing both safety and non-safety uses. A current demonstration project is developing a low complexity FPGA application to investigate reliability and verification concepts that take advantage of application segmentation and deliberate design simplicity.
RISKS

Successful completion of the research described here will help utilities strengthen programs to update I&C systems. I&C modernization competes for limited utility resources with other issues that may need more immediate attention to maintain plant safety and operability. If utility budgets do not protect long term strategic I&C plans, the transition to digital will be correspondingly delayed, possibly to the end of plant life. Also, if plants experience too many costly problems with digital implementations, they will avoid additional upgrades. The regulatory environment may represent a significant risk if progress is not made in finding practical, cost-effective resolutions to key issues. New builds will likely lead operating plants on some key issues; if their efforts falter, there will be a corresponding adverse impact on operating plant I&C modernization.

RECORD OF REVISION

This record of revision will provide a high level summary of the major changes in the document and identify the Roadmap Owner.

<table>
<thead>
<tr>
<th>REVISION</th>
<th>DESCRIPTION OF CHANGE</th>
</tr>
</thead>
</table>
| 0 | Original Issue: August 2011  
Roadmap Owner: Ray Torok |
| 1 | Revision Issued: December 2011  
Roadmap Owner: Ray Torok  
Changes: Changed title to include new plants, updated implementation group activities and I&C architecture project in flowchart. |
| 2 | Revision Issued: August 2012  
Roadmap Owner: Ray Torok  
Changes: Added milestone completion indicators, updated planned project endpoints where needed within flowchart. |
| 3 | Revision Issued: December 2012  
Roadmap Owner: Ray Torok  
Change: Updated selected schedules and milestones in flowchart. |
| 4 | Revision Issued: August 2013  
Roadmap Owner: Ray Torok  
Changes: Revised write-up and flowchart to focus on selected high-visibility topics rather than high-level discussion of all I&C implementation topics. |
| 5 | Revision Issued: December 2013  
Roadmap Owner: Ray Torok  
Changes: Revised write-up and flowchart to add detail and updates in regard to progress in projects addressing CBT modules, likelihood of digital CCF, hazard analysis, and use of FPGAs in I&C replacements. |
| 6 | Revision Issued: August 2014  
Roadmap Owner: Ray Torok  
Changes: Revised write-up and flowchart to add detail and updates in regard to progress in projects addressing cyber security, human factors engineering, electromagnetic compatibility, and a proposed new project to look at application of systems engineering methods to digital I&C design. |
| 7 | Revision: December 2014  
Roadmap Owner: Ray Torok  
Changes: Updated description of cyber activities. Modified flow chart to reflect latest plan, including new cyber security and systems engineering projects. |
| 8 | Revision: August 2015  
Roadmap Owner: Ray Torok  
Changes: Schedules and funding indicators updated on the flow chart. |
| 9 | Revision: December 2015  
Roadmap Owner: Ray Torok  
Changes: Schedules and funding indicators updated on the flow chart. |
| 10 | Revision: August 2016  
Roadmap Owner: Ray Torok  
Changes: Schedules and funding indicators updated on the flow chart. Added reference to Delivering the Nuclear Promise initiative. |