ADVANCED SENSORS AND INSTRUMENTATION

Issue 3 • September 2015

Temperature Resistant Spray-on Piezoelectric Transducers for Materials Characterization with Ultrasonic-Guided Waves

Cliff J. Lissenden
Penn State University

Bernhard R. Tittmann
Penn State University

Material Degradation

Many advanced reactor concepts require the materials to resist various stresses in harsh environments over long service durations. Thus, at some point material degradation (e.g., creep, fatigue, embrittlement) will commence, and its progression, if unchecked, could eventually lead to failure. While degradation processes evolve differently based on material, loading, and conditions, they invariably start at the microstructure level and then progress to the macroscale, and ultimately to fracture. Since shutdowns for inspections are extremely costly, it is preferred to implement online condition monitoring to keep the plant operating until maintenance is necessary. The interaction of ultrasonic guided waves with damage make them very useful for condition monitoring, as will be described below. The requirements of the online condition monitoring system investigated herein are (i) resistance to elevated temperature and (ii) ability to detect incipient damage.

Objectives

The Nuclear Energy Enabling Technologies (NEET) program develops crosscutting technologies that directly support the Office of Nuclear Energy's development of advanced reactor concepts and fuel cycle technologies. The Advanced Sensors and Instrumentation (ASI) subprogram develops the scientific basis for sensors and supporting infrastructure technology that address technology gaps relating to measurements at existing and advanced nuclear power plants. One of the five objectives of the ASI subprogram is to "identify and conduct research into monitoring and control technologies, including human factors, to achieve control of new nuclear energy processes, and new methodologies for monitoring to achieve high reliability and availability." This article describes results of a Nuclear Energy University Program (NEUP)-sponsored blue-sky project (11-3046) to investigate spray-on piezoelectric transducers for online condition monitoring in high-temperature environments. The condition monitoring is based on ultrasonic-guided waves.

Materials

Ultrasonic transduction is traditionally achieved using piezoelectric ceramic materials, which convert an alternating voltage into a mechanical disturbance that propagates into and through the material to be monitored or vice versa. Traditional ultrasonic transducers use lead zirconate titanate (commonly known as PZT) as the active material because of its high coupling parameter (d_{33}),

Continued on next page

In this issue...

For more program information, including recent publications, please visit www.energy.gov/ne

U.S. DEPARTMENT OF ENERGY

Continued from previous page

but its Curie temperature (T_c) limits its usage at elevated temperatures. There are piezoceramics that provide better temperature resistance, but typically at a cost of having a lower coupling coefficient. Bismuth titanate ($Bi_4Ti_3O_{12}$, or BT for short) and lithium niobate ($LiNbO_3$, or LN for short) are good examples and their relevant properties are compared with PZT in Table 1. The sol-gel technique makes processing of composites quite straightforward, as described in the subsequent section. In this research PZT/BT and BT/LN composites were investigated for service temperatures up to ~400°C (e.g., for a number of light water reactor components) and ~850°C (e.g., intermediate heat exchanger for the next generation very high temperature reactor), respectively.

Table 1. Properties of some piezoelectric ceramics.

Material	T_c(°C)	d_{33}(pC/N)
PZT	340	125-340
$Bi_4Ti_3O_{12}$	685	5-20
$LiNbO_3$	1200	6

Transducer Processing

The processing of transducers to send and receive ultrasonic-guided waves has multiple steps. The following steps can be used in the laboratory or modified for field implementation.

1. Create a sol-gel solution consisting of the first constituent (e.g., PZT) and dope it with the second constituent (e.g., BT) to form the composite (e.g., PZT/BT). Mix the solution with an ultrasonic horn.
2. Air-spray the mixture at low pressure onto the selected sample. Once dried, a single spray coating is roughly 20 microns thick. Spraying can be done on flat or curved surfaces; a pipe example is shown in Figure 1.
3. Drive out the organic compounds by heating the sample. This pyrolization process reduces the volume so care is taken to minimize microcracking.
4. Repeat the spray and pyrolization steps to achieve the desired coating thickness.
5. Partially densify the multilayer coating with an induction heating system, again taking care to minimize microcracking.
6. Deposit the electrode (e.g., gold or platinum) on the coating. Due to the porosity of the coating and elevated operating temperatures, electrode material selection and the deposition method are critical. Sputter coating and brush application of the same material can have completely different results.
7. Pattern the electrode to enable control of actuation and reception of specific preferred guided wave modes, as described in the ultrasonic-guided wave section below. Figure 2 shows a multi-element comb transducer on a pipe.
8. Attach a lead wire to the electrode to serve as ground as long as it is electrically conductive.
9. Build a dam around the transducer to enable an oil bath to eliminate arcing when a large voltage is applied to the electrode. Pole the transducer by applying a large voltage at elevated temperatures.
10. Deposit a layer of Sauereisen to protect the transducer.

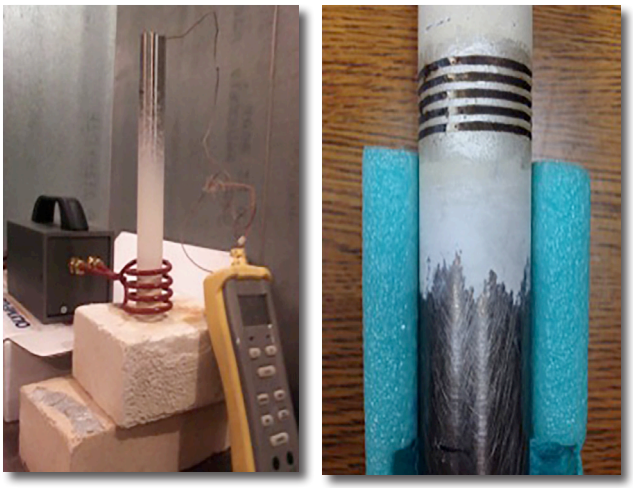


Figure 1. PZT/BT coating sprayed on a stainless steel pipe and ready to densify with an induction heater.

Figure 2. Laser ablated 4-element PZT/BT comb transducer.

Functionality

The temperature-dependence of the signal strength of a PZT/BT transducer sprayed on the end of a roughly 25-mm-long cylindrical rod was tested in a tube furnace. The transducer was pulsed to send a longitudinal wave that reflected off the back wall and was received in pulse-echo mode. The normalized peak-to-peak amplitude is plotted as a function of temperature in Figure 3. Signal degradation starts at 475°C and a detectable signal was received until 690°C. Analogous results are shown in Figure 4 for a BT/LN transducer, for which signal degradation began at 700°C and a detectable signal was received until 1000°C. A limited number of mechanical fatigue tests were conducted, and no coating degradation was observed. Thermal aging tests demonstrated the importance of electrode material selection and deposition method in that electrode atoms can migrate through the porosity of the piezoceramic coating causing short circuit or they can chemically react with elements in the coating nullifying its piezoelectric nature.

Continued on next page

Continued from previous page

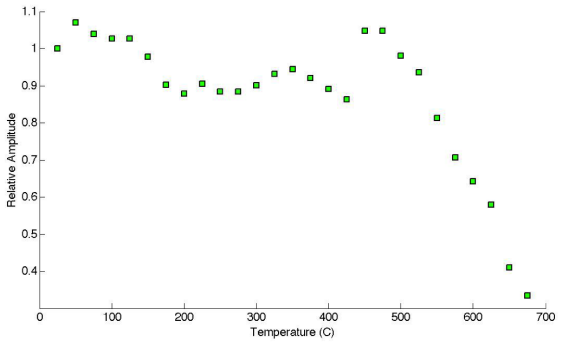


Figure 3. Normalized peak-to-peak amplitude as a function of temperature for PZT/BT transducer.

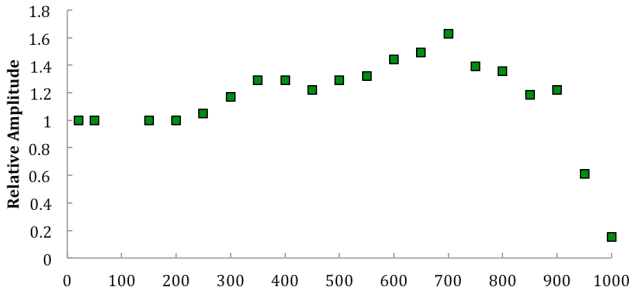


Figure 4. Normalized peak-to-peak amplitude as a function of temperature for BT/LN transducer.

Ultrasonic-Guided Waves

Ultrasonic-guided waves can propagate long distances between transmitter and receiver, provide volumetric coverage of inaccessible material, and offer good sensitivity to damage. Energy loss is small compared to bulk waves because the boundaries of the structure (e.g., a plate or pipe) guide the energy in specific directions. However, the existence of multiple modes at a given frequency and the fact the wave speed depends on the excitation frequency must be taken into account. A comb transducer has multiple elements at a fixed spacing, and because the fixed spacing dictates the preferred wavelength generated, the comb transducer provides a means of wave mode control via the fundamental relationship, $c_p = \lambda f$; where λ is the wavelength, f is the excitation frequency, and c_p is the phase velocity of the preferred mode. By knowing the phase velocity dispersion curves and the desired excitation frequency, the wavelength is computed; hence, the element spacing is known. The dispersion curves for a stainless steel pipe are shown in Figure 5 along with the activation line for a comb transducer having element spacing λ. A comb transducer for a pipe has a sequence of rings with fixed spacing λ.,

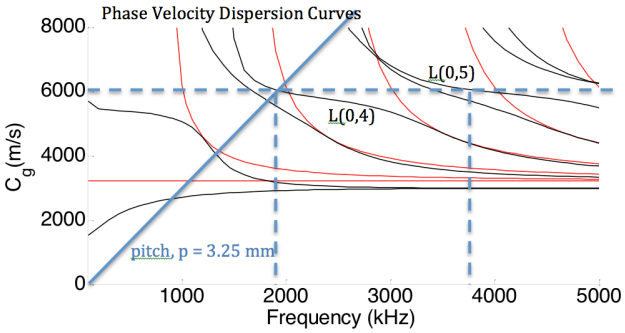


Figure 5. Phase velocity dispersion curves for axisymmetric modes of a stainless steel pipe (25.4-mm diameter, 2.1-mm wall thickness); black lines indicate longitudinal modes and red lines indicate torsional modes. The activation line for a comb transducer is shown for the L(0,4) mode, which generates an L(0,5) second harmonic.

as shown in Figure 2. This PZT/BT comb transducer was processed using the aforementioned 10-step procedure, where the patterning (Step 7) was performed by laser ablation to remove electrode material (i.e., transform a continuous electrode into five rings). The signal in Figure 6 was actuated and received by PZT/BT comb transducers. A comb transducer can also be created by brush painting electrode stripes, although the edges are less uniform.

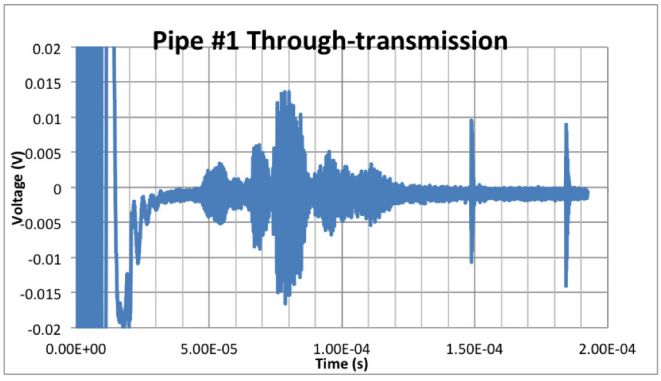


Figure 6. Stainless steel pipe with two PZT/BT comb transducers with four 1.6-mm-wide elements that generates axisymmetric L(0,n) modes when excited at 1.83 MHz

Continued on next page

Continued from previous page

Incipient Damage Characterization

Bulk wave ultrasonics can resolve defects of the order of the wavelength. Guided wave ultrasonics can do significantly better, but the wavelength is larger. On the other hand, nonlinear ultrasonics are sensitive to the effects of microstructural features such as dislocation density, persistent slip bands, precipitates, and voids. This sensitivity is due to the small distortion of the wave caused by the lattice anharmonicity associated with the microstructural defects. The distortion is measurable in terms of higher harmonics in the frequency spectrum, thus the term nonlinear ultrasonics is used because the interrogation signal is at a different frequency than the excitation frequency. Nonlinear ultrasonic-guided waves are more demanding to analyze bulk waves because the higher harmonic must lie on a dispersion curve, it must be phase matched with the primary mode, and there must be power flux transferred to it. If these so-called internal resonance conditions are met, then the higher harmonic will have an amplitude that increases as it propagates, thus it is said to be cumulative. Nonlinear-guided waves combine the advantages of large propagation distances, volumetric coverage, single-sided access, and coverage of inaccessible material with sensitivity to microstructural changes indicative of incipient damage. However, it remains to be shown that spray-on PZT/BT and BT/LN transducers can actuate guided wave modes that generate higher harmonics detectable with PZT/BT and BT/LN receivers. If so, then it should be possible to characterize incipient damage in-situ, thereby enabling condition-based remaining life estimates.

A Risk-informed Supervisory Control System

Sacit M. Cetiner,
Michael D. Muhlheim,
George F. Flanagan, and
Richard T. Wood
Oak Ridge National Laboratory

Highly automated, intelligent control capabilities have not been demonstrated for nuclear power plant operations, and experience is limited in other safety-critical domains. Providing the means for the integration of control, decision-making, and diagnostics to support extensive automation requires that control strategies and methods be developed. These strategies and methods must be part of a flexible, functional architecture to supervise multiunit plants, accommodate shared systems or resources, and enable flexible co-generation operational regimes. The goals for automation include (1) operational management of highly complex plants, (2) dynamic management and control of multiple product streams from a plant, and (3) coordinated management of multiple modules.

In this context, *automation* is the use of computing resources to make decisions and implement a structured decision-making process with limited or no human intervention. The overriding goal of automation is to replace or supplement human *decision makers* with reconfigurable *decision-making* modules that can perform a given set of tasks reliably.

Decision-making is the process of identifying and choosing alternatives based on (1) an agreed-upon set of metrics and (2) the preferences of the decision maker. *Decision-making* presents *alternative options* under consideration, each offering a different approach or *path* to move from a given state or condition to a desired state or condition.

Generation of consistent decisions requires that a structured, coherent process be defined, immediately leading to a *decision-making framework*. The generalized framework for autonomous decision-making can be adopted and tailored to specific requirements for various applications.

The benefits of implementing a supervisory control system with decision-making capabilities into the instrumentation and controls (I&C) architecture include:

- **Reduced plant risk and increased plant availability**, accomplished by reducing the frequency of anticipated operational occurrences that cause plant trips and challenges to plant safety systems by maintaining operating parameters within operational limits. To maintain system operating parameters within operational limits successfully, all combinations of equipment conditions, such as out-of-service for maintenance, failed state, or degraded state should be accounted for to accurately reflect system/component status and operating conditions.
- **Increased life-cycle availability and safety** through the use of a proactive system that uses diagnostics and prognostics as a life-extension tool by probabilistically accounting for changes in component health. This ensures that any decisions to manage the margins to

Continued on next page

Continued from previous page

trip setpoints are based on actual conditions, unlike a reactive system that responds only after a failure occurs.

- **Reduced staffing levels**, achieved by incorporating risk-informed operations that provide the ability to identify potential challenges to plant systems. Current operator staffing levels are based on traditional operational models and limited automation. High staffing levels pose the threat of unsustainable operating and maintenance costs per megawatt for advanced small modular reactors (AdvSMRs). A reliable supervisory control system for AdvSMRs would increase plant automation to reduce operator workload. For plants with multiple nuclear reactors comprising a single power generation system, the predisposition is to staff the plant at levels based on reactor module quantity versus total power output. However, this results in prohibitive operating costs for AdvSMR concepts and does not necessarily improve safety. Therefore, supervisory control research for AdvSMR concepts can offer increased levels of automation with improved reliability and availability and reduced operating costs.
- **Increased operational performance capabilities** for systems that maintain variables, as well as systems affecting the fission process within prescribed operating ranges. This is accomplished by combining the proven benefits of probabilistic risk analysis (PRA) with deterministic design principles in real time. PRAs have been successfully used for design optimization and refinement in safety applications. Expanding their scope to nonsafety-related systems, specifically the nuclear I&C system, can lead to architectures that deliver higher operational performance.

Functional Description

The supervisory control system is implemented as a non-safety-related system. All safety systems, including the reactor protection system and the interlock systems important to safety, are completely independent and isolated from the regular control systems and the supervisory control systems.

Objectives

The main objective of the supervisory control system is to increase the level of automation and to reduce the cognitive load on reactor operators by performing routine operator actions executed primarily during normal operations, and some actions performed during startup and shutdown. In addition to routine operator actions, the supervisory control system will intervene during off-normal conditions such as component failures or unexpected transients. The supervisory control system is not intended to replace the operator as the key decision mode for safety-related actions, nor is it to support or complement protective actions performed by reactor protection or engineered safety features' actuation systems.

System Architecture

The proposed supervisory control system architecture is shown in Figure 1 as a hierarchical structure with three layers of abstraction, progressing from organization to coordination to execution layer, where low-level actions are performed based on the commands or directions from upper layers.

In the supervisory control architecture, the level of decision-making and supervision is greater at the top of the chart shown in Fig. 1. The level of activity and time urgency increases on the lower portion of the chart.

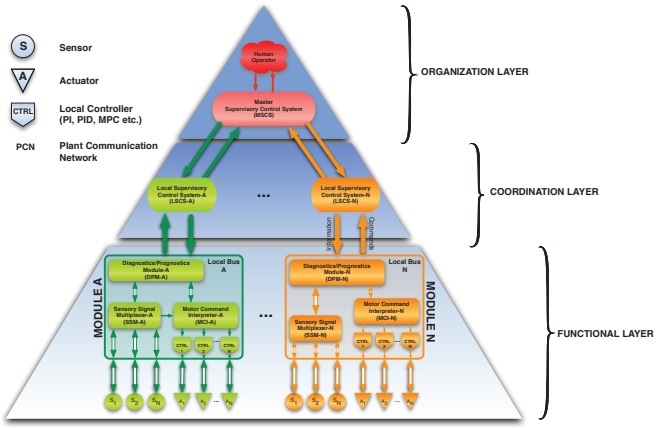


Figure 1. Supervisory control system hierarchical architecture.

The overall functional architecture of the supervisory control system with the proposed autonomous decision-making framework is shown in Figure 2. The decision-making block will be explained further in the next section.

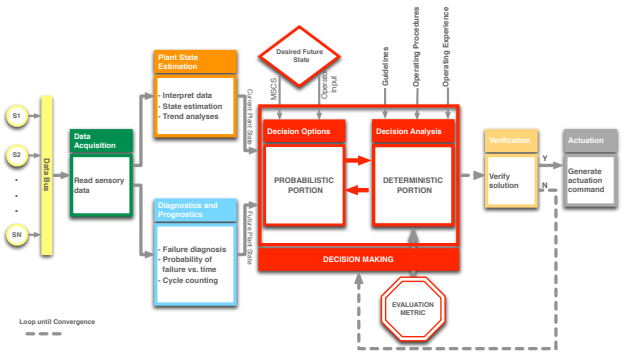


Figure 2. Functional architecture of the supervisory control system.

Continued on next page

Continued from previous page

Autonomous Decision-making

Decision-making involves collection of information, evaluation of alternatives, and selection of the preferred alternative. Every decision-making process results in a final choice, which is developed into an instruction to be executed and implemented.

An *automated process* refers to a predetermined action or set of actions to reach a desired state given a condition or change in condition. Automation is widely used in almost every facet of our lives, but it does not involve decision-making. Automation is merely a convenience that performs certain tasks in the case of a triggering event without human intervention. In an automated process, all input states are assumed to be known. Therefore, uncertainties in monitored processes, unforeseen system states, or deteriorating conditions are not treated directly. However, potential implications of uncertainties can be incorporated into control system design, such as the case in robust control. Automation allows for a limited and relatively small set of actions—typically identified in a decision table or logic table—to be considered given the input states with the highest impacts on output states.

Generalized Decision-Making Framework

Autonomy is the ability of a system to determine and perform necessary tasks without human involvement. Decision-making is a fundamental element of autonomy. Autonomy refers to the use of computing resources to make decisions and implement a structured decision-making process with limited or no human intervention. The overriding goal of autonomy is to replace or supplement human decision-makers with reconfigurable decision-making modules that can perform a given set of tasks reliably.

The decision-making process must consider uncertainties, evaluate options, and then assess potential consequences of a particular decision. Hence, evaluation and assessment steps may require consideration of multiple attributes of a system, components or elements of a system, or their future states, especially for large-scale complex systems such as a nuclear power plant.

While there are minor differences in the literature about the necessary and sufficient steps for decision-making (Baker et al.), the decision-making process for the supervisory control system is based on three fundamental elements:

1. Identification: identify decision alternatives
2. Evaluation: evaluate alternative decisions
3. Resolution: generate a single solution or a single trajectory.

Autonomous Decision-Making Framework for Supervisory Control

The fundamental assumption that goes into the design of the supervisory control system is that, if the supervisory control system fails to act during a transient, the safety system will eventually and independently initiate protective actions and bring the plant to a safe shutdown state.

The elements and the process of the proposed decision-making framework are illustrated in Figure 3. In the first block, decision alternatives are created based on the probabilistic model that captures component-, subsystem-, or system-level faults, incorporating the diagnostics and prognostics assessments. The function of this block is to create a list of alternative actions that can take the system from a degraded state to a nominal or acceptable state through a reliable pathway. The alternatives identified by the probabilistic portion are then evaluated by the deterministic portion, depicted in the second block, to generate a single solution, or the resolution of the decision-making process.

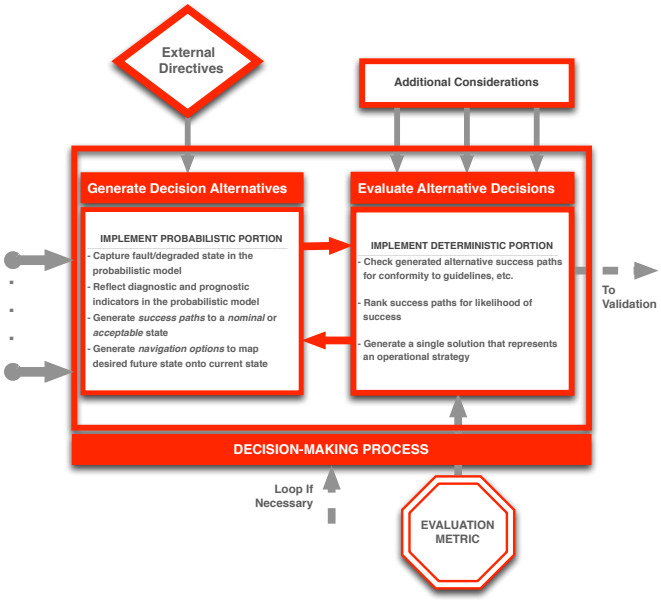


Figure 3. The decision-making framework for the supervisory control system.

Probabilistic Portion

There are many different methods and tools that can be used to perform probabilistic assessments; however, choosing the appropriate method is key for consistency. The first step is to identify the functional requirements of the probabilistic method. After the requirements are identified, the analytical method and tools can be selected and the necessary automation tools developed. The

Continued on next page

Continued from previous page

completion of this stage signifies the transition from a theoretical problem to an application of the technology developed.

To meet the objectives for the supervisory control system, the following requirements of the probabilistic tools will allow narrowing the selection of probabilistic techniques to be considered. Specifically, the probabilistic techniques must be able to:

- Recognize component states (i.e., failed, out of service, degraded, operating)
- Recognize changes in status for one or more components simultaneously
- Reflect changes in component status on a real-time basis (e.g., working to failed)
- Recognize changes in probability of failure
- Calculate different metrics of interest.

Deterministic Portion

Plant operating procedures (OPs) are rule-based modules executed by human operators. A rule-based model

- Identifies the system state
- Associates the state with a task
- Accesses stored rules to perform the task.

Operational limits and conditions (OLCs) are developed to ensure that the plant is operated in accordance with plant design assumptions and intent. OLCs also include actions to be taken and limitations to be observed by operating personnel, or in this case, the supervisory control system. OPs are developed for normal operation to ensure that the plant is operated within the OLCs and to provide instructions for the safe conduct of all modes of normal operation, such as starting up, power production, shutting down, shutdown, load changes, and fuel handling. Any action taken by the supervisory control system must not diverge from the established OPs and cannot compromise established OLCs.

Advantages of Risk-informed Supervisory Control System

An important function of the control system is to maintain a sufficient margin between plant operating parameters and reactor protection parameters to prevent unnecessary trips and challenges to plant safety systems. The supervisory control system monitors plant and equipment status in real-time and maintains specific knowledge of the reactor protection system trip setpoints under all operating regimes.

Any plant could benefit from using a control system that incorporates probabilistic assessments into the decision-making process. The probabilistic portion of a risk-informed supervisory control system optimizes plant safety and availability through the detection and mitigation of plant events that explicitly account for the plant configuration and power level. The deterministic portion of the risk-informed decision-making systems ensures that any action taken by the supervisory control system does not diverge from the established OPs and cannot compromise established OLCs.

At this stage of the research, Oak Ridge National Laboratory has successfully demonstrated that PRAs—constructed in a distinct way as illustrated in this article—can be used to automatically identify available decision options and to generate a state trajectory (i.e., a set of corrective actions to move the system from a troubled state to an acceptable state). A comprehensive demonstration through simulation of the extended decision capabilities for supervisory control is planned for subsequent work.

REFERENCES

Baker, D., Bridges, D., Hunter, R., Johnson, G., Krupa, J., Murphy, J., and Sorenson, K. *Guidebook to Decision-Making Methods*, DOE WSRC-IM-2002-00002, 2001.

Involving Industry in Outage Control Center Research in the Light Water Reactor Sustainability Program

Shawn W. St. Germain
Idaho National Laboratory

LWRS Program Advanced Instrumentation, Information, and Control Systems Technologies Pathway

One of the key characteristics of the Advanced Instrumentation, Information, and Control Systems Technology Pathway within the Light Water Reactor Sustainability (LWRS) Program (www.inl.gov/lwrs) is that the nuclear power industry is continuously engaged, ensuring that ongoing research is relevant and meets the needs of industry. This focus on industry involvement strongly promotes the overall goal of the LWRS Program to support the long-term operation of the nation's fleet of nuclear power plants. The Advanced Outage Control Center (AOCC) is a pilot project in the Advanced Instrumentation, Information, and Control LWRS Program pathway that seeks to improve nuclear power plant efficiency by developing technology-based process improvements to support refueling outage coordination and performance. In addition to power uprates, reducing the duration of refueling outages represents an option to improve nuclear power plant capacity factors.

LWRS Program researchers initially began working with Arizona Public Service's Palo Verde Nuclear Generating Station to develop, implement, and evaluate new technology applications that can improve safety and efficiency during refueling outages. Researchers developed a baseline for outage performance by observing outage activities at Palo Verde Nuclear Generating Station during their spring 2013 refueling outage. During this observation period, data were collected to support a function and task analysis of outage activities and to assess human factor aspects of their existing physical outage control center (OCC) layout. Based on direct observation of outage activities and interviews with Palo Verde Nuclear Generating Station staff, several areas were identified where the use of technology would benefit outage coordination activities.

The first area identified for technology development was a collaboration tool used by the Issues Response Team (IRT). The IRT is a team of individuals assembled to understand and facilitate the needed recovery actions for resolving issues discovered during a refueling outage. The project team developed a standard issues package using collaboration technology to manage information for emergent issues. The standard issues package is a template using collaboration software to consistently collect, organize, and share information. IRT templates that included the necessary procedural forms were developed to support IRT issue tracking and resolution. A standardized file structure and instructions were developed for issue documentation. Training was held with IRT managers and staff prior to the start of the refueling outage to familiarize personnel with the new collaboration tools. Palo Verde Nuclear Generating Station implemented the technology upgrades and modified the IRT process to take advantage of the new collaboration tools during the fall 2013 refueling outage. Because the standard issues package was network accessible and updateable by numerous users simultaneously, the value of the collaboration tool was quickly recognized by Palo Verde Nuclear Generating Station management. The improved technology and modified IRT process was successfully used for all emergent issues during the refueling outage. As a result of these process improvements, the Nuclear Energy Institute awarded a Top Industry Practice Award Process Award to Arizona Public Service Company for leveraging technology to improve outage coordination and performance.

LWRS Program staff worked with Palo Verde Nuclear Generating Station to update their OCC with technology to improve outage communication and collaboration for the entire outage organization. Figure 1 shows training being conducted in Palo Verde's upgraded OCC. The use of new technology in the OCC allows staff to access and update all the information displayed in the OCC from any computer on the business network. This level of access to information greatly reduced the number of phone calls and distractions to the OCC, allowing OCC staff to maintain focus on managing the outage.

Use of the new OCC technology during Palo Verde's spring 2014 refueling outage was well received, and Palo Verde Nuclear Generating Station achieved a new station record for outage duration.

Benchmarking at other utilities has been performed to verify that the methods and approaches that yielded the results observed at Palo Verde are applicable to other utilities, ensuring that the overall results and technologies are generalizable and usable by others. Initial benchmarking visits confirmed that most plants have been managing refueling outages in a manner similar to Palo Verde and encountering similar issues. There was increasing interest in the success of Palo Verde's process improvements. Consequently, LWRS Program staff began

Continued on next page

Continued from previous page

Figure 1. Palo Verde Unit 2 OCC video wall.

to explore options for sharing experience and lessons learned to best leverage the results of research with the broader nuclear power industry. Typically, research results have been shared by the publication of reports documenting the process improvements and lessons learned. For the AOCC pilot project, a different approach is being taken to augment the publication of research reports. LWRS Program staff are conducting outreach with utilities interested in applying the technology and process improvements developed within the pilot project. This also permits collection of additional observations of AOCC adoption and lessons learned at other plants and a growing knowledge base of expertise in power plants with the pilot project technologies.

One outreach activity was conducted with Southern Company's Plant Farley. LWRS Program staff assisted Plant Farley staff in setting up outage communication and collaboration process improvements. Plant Farley implemented these process improvements for their fall 2014 refueling outage. LWRS Program staff visited Plant Farley during their refueling outage to evaluate the implementation and results. Valuable lessons related to change management and knowledge transfer were learned from the process. The process improvements proved valuable to Plant Farley, and Southern Company has expanded their use to Plant Hatch and Plant Vogtle. Additionally, they are using some of these tools and concepts for on-line project related communication.

Another outreach activity was conducted with Tennessee Valley Authority's (TVA's) Sequoyah Nuclear Plant. LWRS Program staff worked with Sequoyah staff in setting up outage communication and collaboration process improvements. Sequoyah staff provided several additional enhancements that have been shared with other participating utilities. Sequoyah implemented these process improvements for their spring 2015 refueling outage, and LWRS Program staff evaluated the results. With each implementation and observation, additional best practices are being documented and shared. Figure 2 shows the Sequoyah OCC staff using the new communication process. Results have been positive and TVA intends to expand its use to Watts Bar this fall and Browns Ferry next spring. TVA has also adopted the tools to manage online emergent issues.

In the spring of 2015, LWRS staff created an AOCC Pilot Project working group to facilitate sharing best practices related to outage technology implementation. Bi-monthly

Continued on next page

Continued from previous page

Figure 2. Sequoyah OCC using collaboration software to manage outage information.

teleconferences are held to share recent lessons learned and best practices. Additionally, an external SharePoint site was established to support sharing information within the group. Utilities that have already implemented process improvements, such as Palo Verde and Sequoyah, share lessons they learned during implementation with those just starting out with the AOCC technologies being developed by the pilot project. Currently, there are participants in the working group from Arizona Public Service Company, Southern Company, Duke Energy, TVA, and Xcel Energy. Collectively, this group of utilities represents nearly 30% of the nuclear generation in the U.S. Additional outreach and observations are planned with Brunswick and Prairie Island.

In conjunction with sharing early research results with industry, additional research is ongoing to identify new applications of technology and process improvements. Palo Verde continues to support LWRS Program research. During Palo Verde's spring 2015 refueling outage, a new study was conducted to demonstrate automatic work status updates from electronic work packages. An electronic work package was used in the field to perform work on large feedwater check valves. The procedure was rendered to a tablet connected via a wireless network, a detailed work status was available to the work supervisor, and an overview display was provided to the OCC. This provided a form of distributed task information for real time work management and execution in an operational setting, shared simultaneously with multiple locations on plant site. There was a positive response from all groups involved in the work and additional research will be conducted to determine the best application of this capability. Figure 3 shows field workers using an electronic work package for field work.

In summary, the level of industry involvement in the AOCC Pilot Project has increased significantly since the project started. The increased participation by industry greatly increases the speed by which ideas can be developed, rendered into technologies that are suited to nuclear application, verified, and tested in controlled work environments. Then feedback is obtained, and processes and technologies are ultimately improved. Continuous participation by industry through all phases of the pilot project ensures that the research will be applicable and valued by industry. The voice of the end user is represented on the front end of research, and operators provide needed information to assure the quality and safety of the resulting prototype technology. This process also provides a template for technology development

Continued on next page

Continued from previous page

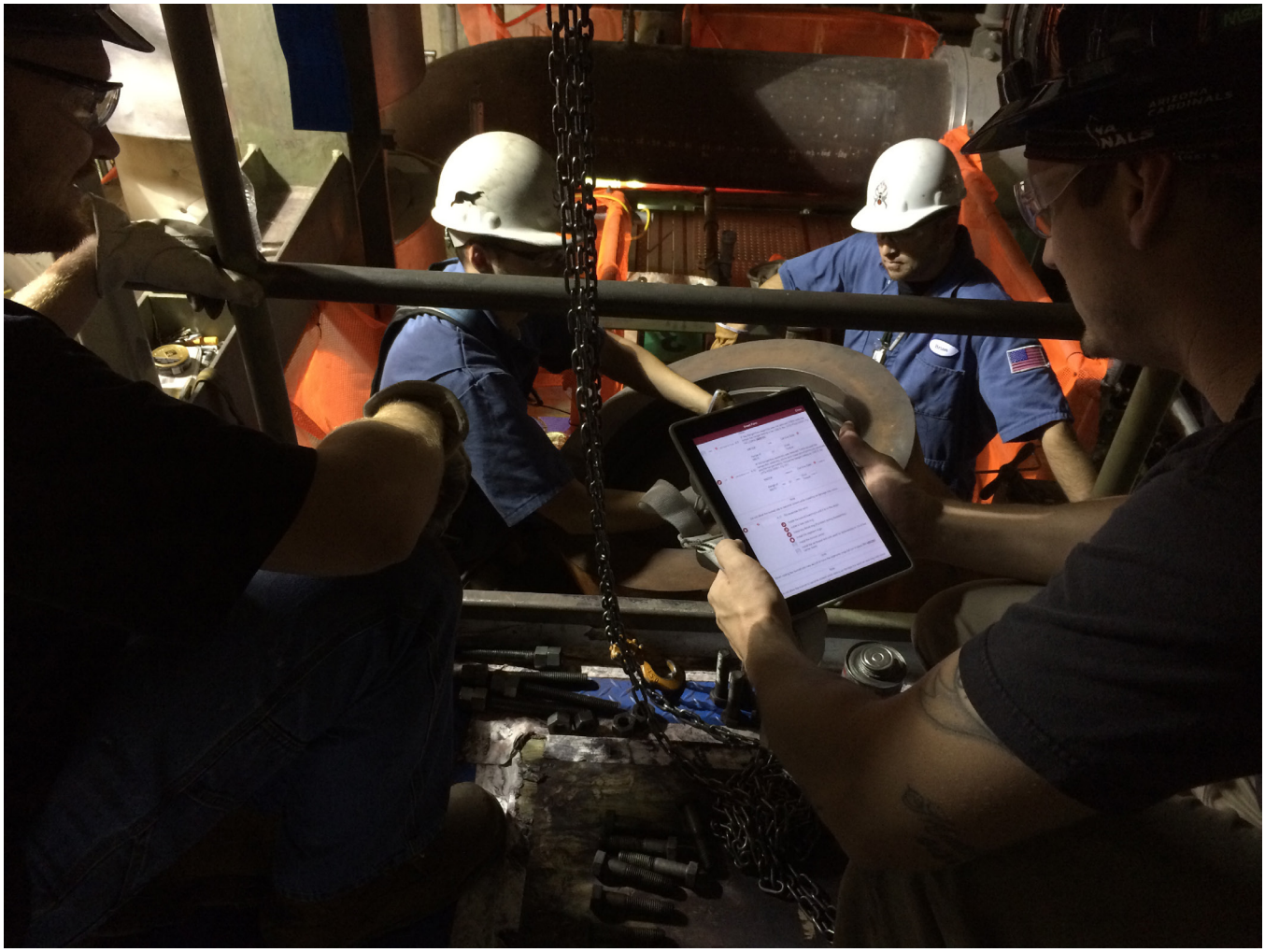


Figure 3. Field workers using an electronic work package at Palo Verde.

and commercialization by vendors who are interested in providing technology delivery and services to the nuclear power market and provides needed assurance that the resulting technologies conform to the nuclear safety culture so important to the continued safety record of the industry. Participation by multiple utilities ensures that new concepts are shared and can be generalized to the broader nuclear industry and are not just a unique solution for one utility. There is growing interest in this research, and we anticipate additional utilities will soon join the working group.

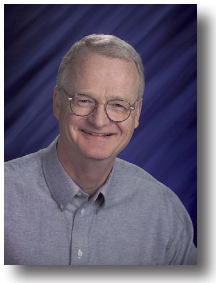
REFERENCES

1. Shawn St. Germain, Ronald Farris, April Whaley, Heather Medema, David Gertman, *Guidelines for Implementation of an Advanced Outage Control Center to Improve Outage Coordination, Problem Resolution, and Outage Risk Management*, INL/EXT-14-33182, Rev. 0, September 2014.

Advances in Online Monitoring for Measurement within Nuclear Fuel Reprocessing Streams

Samuel A. Bryan and Amanda J. Casella

Pacific Northwest National Laboratory



There is a renewed interest worldwide in promoting the use of nuclear power and closing the nuclear fuel cycle. The long-term successful use of nuclear power is critically dependent upon adequate and safe processing and disposition of the used nuclear fuel. Liquid-liquid extraction is a separation technique commonly employed for the processing of the dissolved used nuclear fuel. The instrumentation used to monitor these processes must be robust, require little or no maintenance, and be able to withstand harsh environments such as high radiation fields and aggressive chemical matrices.

Scientists at Pacific Northwest National Laboratory (PNNL) have been designing spectroscopic methods for the robust measurement of nuclear fuel reprocessing solutions (Bryan et al. 2011a). The PNNL research team has experimentally assessed the potential of Raman and ultraviolet-visible-near infrared (UV-vis-NIR) spectroscopic techniques for online real-time monitoring of metals, including uranium, plutonium, and neptunium (Bryan et al. 2011b) as well as total acid (Casella et al. 2013c) and pH (Casella et al. 2015) in solutions relevant to used-fuel reprocessing. These optical techniques demonstrate robust performance in repetitive batch measurements of each analyte conducted in a wide concentration range using simulant and commercial dissolved-used–fuel solutions. In commonly used solvent extraction schemes, the acid strength and pH are of critical importance for process quality and control, as they affect speciation of the target analytes and thus their extraction efficiencies and selectivities. In a nuclear fuel reprocessing facility, classic potentiometric pH measurements are not suitable for obtaining real-time continuous data because they require frequent calibration and maintenance and have poor long-term stability in aggressive chemical and radiation environments. By contrast, online spectroscopic monitoring has proven a viable technique for determining the pH compatible with real-time monitoring of dynamic separation processes in nuclear fuel reprocessing streams.

This article summarizes some of the current technologies being developed and discusses the logic for their use within the Fuel Cycle Research and Development Program.

Methodology

The scheme depicted in Figure 1 shows the flow and use of information needed for process monitor development. In this scheme, static spectroscopic measurements are taken as training set data—the basis of chemometric models that are then used for predictive, online, process monitoring.

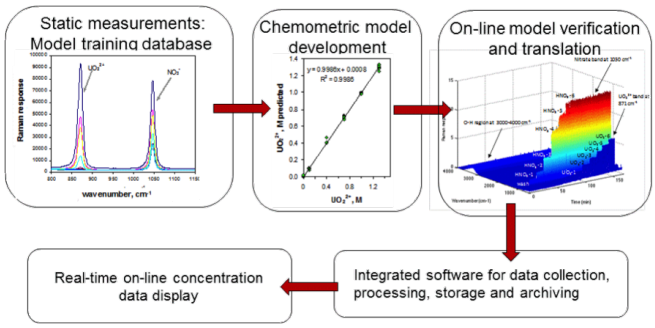


Figure 1. Methodology for online process monitor development.

A bank of centrifugal contactors, used for continuous, counter-current solvent extraction experiments in shielded glovebox containment, has been commissioned for used-fuel experimental testing at PNNL. Figure 2 contains a photograph of the bank of contactors, which are utilized for online process monitoring demonstration tests. For purposes of demonstrating online process monitoring, this bank of contactors has been instrumented with optical process monitoring probes.

Figure 2. Photograph showing a bank of centrifugal contactors inside a shielded glovebox.

Continued on next page

Continued from previous page

Online Process Monitoring of $UO_2(NO_3)_2$ and nitric acid.

As a demonstration of monitoring a uranyl nitrate/nitric acid process stream of varying concentration, a series of solutions, sequentially increasing in nitric acid and $UO_2(NO_3)_2$, were introduced into the shielded centrifugal contactor flow loop system. Raman spectra were collected concurrently with the additions of HNO_3 and $UO_2(NO_3)_2$ into the feed. The concentrations were built up incrementally, starting with the addition of nitric acid (0 to 6 M), followed by uranyl nitrate ($UO_2(NO_3)_2$) added from 0.1 to 0.6 M (Bryan et al. 2011a).

The feed solution was well mixed during and after each addition of nitric acid, and uranium nitrate, allowing for the homogenization of the feed solution prior to adding the next analyte. During the additions, Raman measurements were taken at the online monitoring point designated at the exit of the raffinate stream. Figure 3A shows the accumulated Raman spectra taken over the time frame during which the nitric acid and uranium are added. Significant spectral features apparent within this figure are the water region at 3000 to 4000 cm^{-1}; the nitrate band at 1050 cm^{-1}; and the UO_2^{2+} band at 871 cm^{-1}. By using a chemometric analysis, the concentrations of UO_2^{2+}, nitric acid, and total nitrate are determined for each Raman measurement.

Figure 3B contains the predicted concentrations of UO_2^{2+}, nitric acid, and nitrate species as a function of time for the Raman online measurements. The light blue lines are the expected concentration of analyte in solution; the red, green, and dark blue lines are the predicted concentration of HNO_3, total nitrate, and $UO_2(NO_3)_2$ respectively. It is worth noting that the model is capable of not only predicting the UO_2^{2+} and nitrate concentrations but also of differentiating between total nitrate and nitric acid.

Spectroscopic Analysis Applied to Used Fuel Measurements

The efficacy of using Raman and UV-vis-NIR spectroscopy for analytical measurements has been demonstrated using used nuclear fuel samples. Uranium, plutonium, and neptunium were measured spectroscopically and compared to inductively coupled plasma mass spectrometry (ICP-MS) analysis, with comparisons being within 1–2% using used commercial ATM-109 fuel.

Table 1 contains the concentrations for U, Pu, Np, and Nd for the ATM-109 feed as determined by spectroscopic analysis. This table also contains the comparison with the standard ICP-MS analysis for these species. The ratio of the spectroscopic/ICP method shown (ratio = 1.0 is an ideal match) indicates good agreement between spectroscopic and ICP method. UV-vis-NIR was used for Pu, Np, and Nd analysis, and Raman spectroscopy was used to determine U concentrations.

Table 1. Concentrations of U, Pu, Np, and Nd for ATM-109 fuel feed as determined by spectroscopic analysis and comparison with ICP-MS analysis. Data from (Bryan et al. 2011b). Concentrations are in Molar units.

ATM-109	U	PU	Np
Spectroscopy	0.719	8.90E-03	4.7E-04
ICP-MS	0.721	8.99E-03	4.7E-04
Spectroscopic/ICP ratio	1.0	0.99	1.0

Real-Time Diversion Detection

Connecting spectroscopic monitoring probes to a bank of cross-current centrifugal contactors demonstrated the ability to quantify the total inventory of metal content being extracted within a mock diversion. For this, $Nd(NO_3)_3$

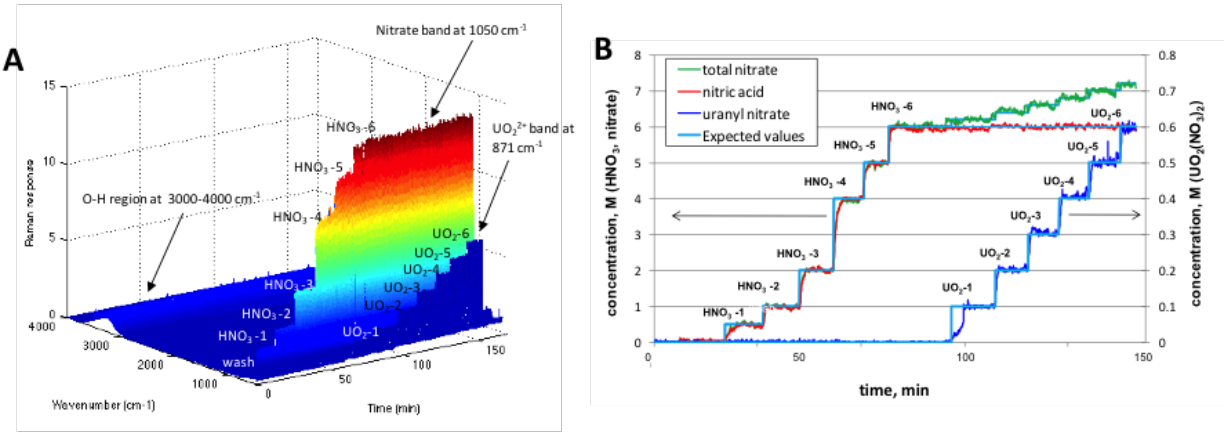


Figure 3. (A) Real-time Raman monitoring of the fuel simulant extraction solution. (B) Measured and predicted Raman online measurements showing excellent agreement between values.

Continued on next page

Continued from previous page

was used as a non-radioactive surrogate for $Pu(NO_3)_4$ with a PUREX-type extraction system. The spectroscopic instrumentation was connected to the influent and effluent lines of the bank of centrifugal contactors. Figure 4 contains a schematic representation of the bank of contactors used, with the locations of feed, raffinate, organic inlet, and loaded organic product streams. The vis-NIR and Raman monitoring probes were positioned on each inlet and outlet stream, with the real-time spectral measurements shown in Figure 5. The analysis of the spectral data shows cumulative Nd^{3+} in the feed and in the combined organic and raffinate streams. The difference between the feed (inlet) and organic product and raffinate (outlet) is shown in Figure 6.

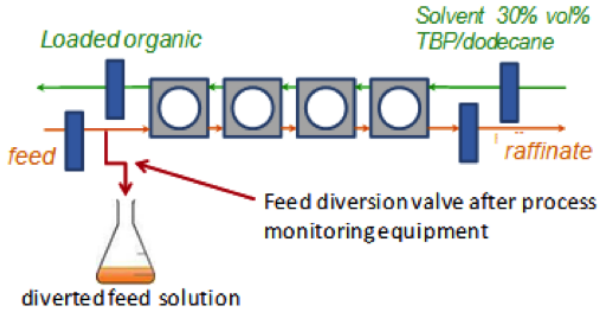


Figure 4. Schematic representation of the bank of contactors used in our study; the feed, raffinate, and loaded organic product streams are instrumented with vis-NIR and Raman probes as well as flow meters.

The difference between the two measurements, labeled "delta from in-process" in Figure 6A, is the variance in millimoles between the two curves ("feed" and "organic + raffinate"). After the start of diversion at 87 minutes, the "organic + raffinate" curve in Figure 6A further deviates from the "feed" curve; during the diversion period (between 87 minutes and 134 minutes) the two curves

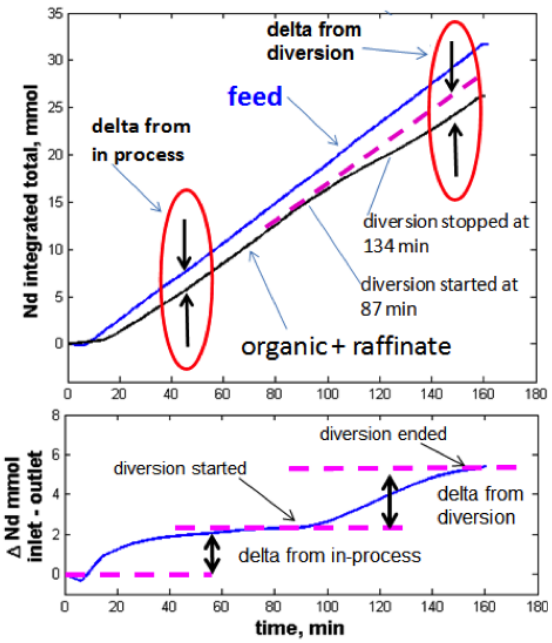


Figure 6. Nd^{3+} extracted and measured in feed, raffinate, and organic product streams showing (A) detection of Nd from contactor Feed and Product stream concentration profile as a function of time; and (B) difference of integrated total amount of Nd between Feed and Product streams as a function of time.

are no longer parallel. After diversion is stopped (at 134 minutes) the "organic + raffinate" curve then returns to being parallel with the "feed" curve. Extrapolating a line from the "organic + raffinate" curve prior to diversion enables us to measure the amount of Nd^{3+} material diverted by subtracting the extrapolated value (prior to diversion) from the measured value after diversion. The "delta from diversion," also shown in Figure 6B, shows that 3×10^{-3} mol Nd^{3+} was diverted, based on the graphical analysis of the data (Figure 6). This value is in excellent agreement with that obtained based on mass balance values from Table 1 (2.9×10^{-3} mol Nd^{3+}).

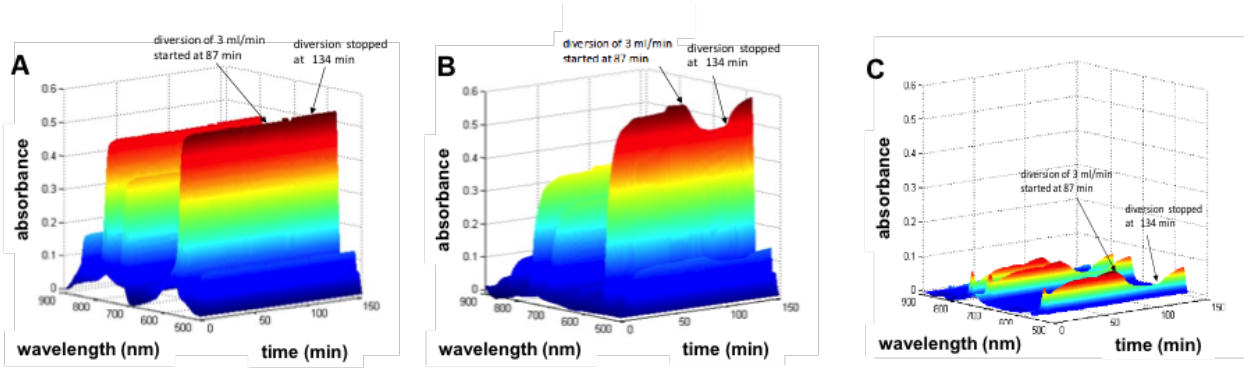


Figure 5. Visible spectra showing Nd^{3+} in feed (A), organic product (B), and raffinate (C) as a function of time during centrifugal contactor experiment.

Continued on next page

Continued from previous page

On-line pH measurement of Process Streams

Solvent extraction reprocessing schemes currently being developed contain various steps, each tailored to the separation of specific radionuclides. In these systems, acid strength/pH is essential to process quality and control, as explained above (Casella et al. 2015; Casella et al. 2013b; Casella et al. 2013a).

The effect of pH on the Raman signature of the carboxylate fingerprint region from pH 0.20 to 6.09 is illustrated in Figure 7. The large changes in the Raman spectra, which are due to the proportioning between the protonated and anion forms of the buffer molecule used, correlate directly to the pH of the solution and provide the basis for this method of pH measurement (Casella et al. 2015).

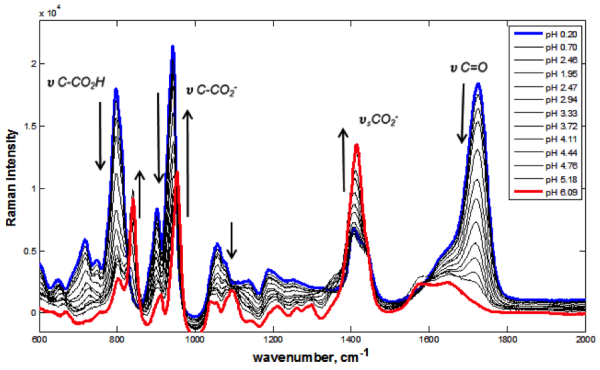


Figure 7. Raman signatures 1.5 M citrate with pH between 0.20 and 6.09. Direction of arrow indicates trend with increasing pH.

The real-time Raman spectroscopic results collected during dynamic flow testing are illustrated in Figure 8A. This graph clearly shows the results from changing solution pH. The developed chemometric model was applied to the spectra and evaluated for both variability and accuracy in determination. The two methods varied in their determinations by only ± 0.1 pH units over the entire applicable range.

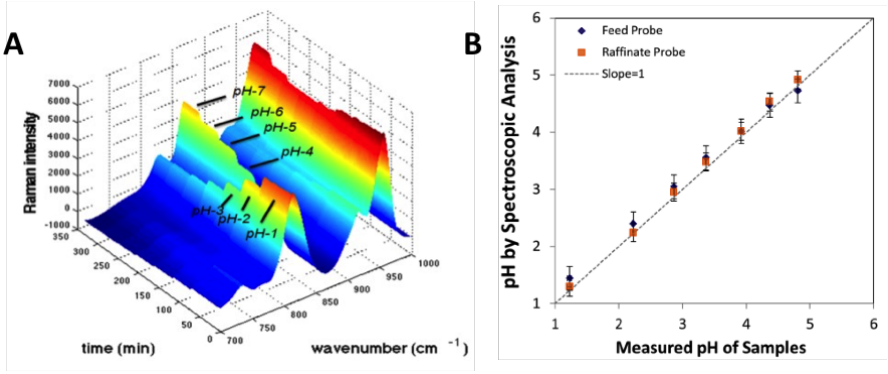


Figure 8. (A) Raman signatures of 1 M citric acid/0.125 M HEDTA with a pH range of 1.2 to 5.0. (B) pH determined by chemometric analysis compared to the analytically measured value.

Summary

Under Fuel Cycle Research and Development Program funding, PNNL has developed an array of methods for spectroscopic online determination of multiple metal analytes and other constituents within used nuclear fuel streams. These methods enable us to identify material intentionally diverted from a liquid-liquid solvent extraction contactor system in real time. This work also demonstrated the applicability of using Raman spectroscopy as a robust method to measure pH in a used nuclear fuel reprocessing separation system. The next steps for this technology involve testing at a larger scale chemical separations facility, such as H Canyon at the Savannah River Site.

REFERENCES

Bryan S. A., T. G. Levitskaia, A. J. Casella, J. M. Peterson, A. M. Johnsen, A. M. Lines, E. M. Thomas, and C. Orton, 2011a. "Spectroscopic On-Line Monitoring for Process Control and Safeguarding of Radiochemical Streams." In *Advanced Separation Techniques for Nuclear Fuel Reprocessing and Radioactive Waste Treatment*, eds. K. L. Nash and G. J. Lumetta, Cornwall, UK, Woodhead Publishing Ltd; CRC Press LLC.

Bryan S. A., T. G. Levitskaia, A. M. Johnsen, C. R. Orton, and J. M. Peterson, 2011b. "Spectroscopic Monitoring of Spent Nuclear Fuel Reprocessing Streams: An Evaluation of Spent Fuel Solutions Via Raman, Visible, and near-Infrared Spectroscopy." *Radiochimica Acta*, Vol. 99, No. 9, pp. 563–71, <Go to ISI>://000294789600005. DOI 10.1524/ract.2011.1865.

Casella, A., L. Hylden, E. Valerio, J. Peterson, G. Lumetta, T. Levitskaia, and S. Bryan, 2013a, "Advances in On-Line Spectroscopic Monitoring for Weak Acid Based Nuclear Fuel Reprocessing Schemes," *Transactions of the American Nuclear Society,* Vol. 109, No. 1, pp. 387–8.

Casella, A. J., L. R. H. Ahlers, E. L. Campbell, T. G. Levitskaia, J. M. Peterson, F. N. Smith, and S. A. Bryan, 2015, "Development of Online Spectroscopic pH Monitoring for Nuclear Fuel Reprocessing Plants: Weak Acid Schemes," *Analytical Chemistry,* Vol. 87, No. 10, pp. 5139–47, http://dx.doi.org/10.1021/ac504578t. 10.1021/ac504578t.

Casella, A. J., L. R. Hylden, E. L. Valerio, J. M. Peterson, G. J. Lumetta, T. G. Levitskaia, and S. A. Bryan. 2013b. *Advances in On-Line Monitoring for Weak Acid Based Nuclear Fuel Reprocessing Schemes. Presented at American Nuclear Society, Winter Meeting, Washington, D.C., ANS, La Grange Park, Illinois*, 2013.

Casella, A. J., T. G. Levitskaia, J. M. Peterson, and S. A. Bryan, 2013c, "Water O-H Stretching Raman Signature for Strong Acid Monitoring Via Multivariate Analysis," *Analytical Chemistry*, Vol. 85, No. 8, pp. 4120–8, http://www.ncbi.nlm.nih.gov/pubmed/23472939. 10.1021/ac4001628.

Radiation Hardened Circuitry Using Mask-Programmable Analog Arrays

Charles L. Britton, Jacob H. Shelton, M. Nance Ericson, Miljko Bobrek, Dwight A. Clayton

Oakridge National Laboratory

One of the pressing needs in research for reactor-accident instrumentation involves reliable radiation- and heat-tolerant electronics for sensing and control. While some measurements are suitably made using tethered instrumentation placed well away from radiation zones, others require that electronics are placed in close proximity to sensors, which can often be located in harsh radiation and temperature environments. Close measurement access is often achieved using agile and mobile telerobotic platforms that allow flexible placement in a variety of areas, which may or may not require long-term functioning measurement systems. However, this ability to place sensors and electronics in critical areas brings the associated problem of radiation damage to the measurement system and associated electrical components.

Since the end of the Cold War, the primary military need for radiation-hardened semiconductor processes has all but vanished. Through the late 1980s, the driver was the expectation of nuclear exchanges that could totally and instantaneously destroy military components in exposed aircraft or ground-based systems. At the end of the Cold War, the demand for terrestrial and airborne radiation-resistant electronics waned as the need continued in space-based applications (such as satellite systems). The requirements for the extra-terrestrial environment are quite different as the total dose received by space-borne devices occurs at a much lower rate but over a much longer time period; therefore, other types of radiation events such as single-event effects (SEE; of much lower magnitude than anticipated in nuclear exchanges) become more important from a hardening perspective. The radiation damage issues to be considered in building electronic systems for robotics that will potentially be used for post-accident inspection and monitoring in nuclear power plants lie somewhere between the Cold War instantaneous dose effects and the present day satellite continuous dose combined with the SEE.

The reduced availability of truly radiation-hardened semiconductor processes has resulted in development of a variety of techniques to mitigate some of these effects while using standard, readily available commercial processes. Collectively, these techniques are referred to as radiation-hardened-by-design or RHBD. These techniques extend from actual transistor layouts that reduce device damage to special circuit architecture designs ensuring that damaged devices will not be allowed to override the operation of undamaged devices.

Over the last several years, radiation-hardened digital circuitry has become available, primarily in the form of nominally rad-hard field-programmable gate arrays (FPGAs). Several companies such as Atmel and MicroSemi offer space-qualified digital circuitry in the form of FPGAs and sea-of-gates. Honeywell offers these plus individually packaged analog functions such as ADCs of various types. Recently Xilinx introduced the Virtex-5QV, which is a rad-hard version of its popular Virtex-5 device that is hardened to greater than 1 MRad. Consequently, there are a number of viable commercial solutions for moderately hardened digital circuits.

On the other hand, there is not a significant variety of rad-hard circuitry for analog functions, particularly functions with programmable interconnects. Certainly, an analog circuit similar to the FPGA would be an excellent addition to the designer's toolkit for rad-hard robotics design. Recently UT-Knoxville participated in an unrelated project to design and test an early radiation-hard version of Triad Semiconductor's Via-Configured Array (VCA). This new product offering by Triad Semiconductor (www.triadsemi.com) is pre-configured as an array of analog tiles—such as operational amplifiers, voltage references, and analog-digital converters (ADCs). These analog tiles are designed and fabricated in a standard semiconductor process, and are left mostly complete, except for the last two levels of interconnect metal which are subjected to a semi-automated design process. Software developed and provided by Triad can be used to design and simulate the customer's desired system by interconnecting and therefore configuring the connectivity of the on-chip analog blocks in these last two levels. After the desired system has been designed, the software is used to generate the description of the final two levels of metallization, which are then applied to complete the fabricated system chip. The completed silicon wafers are subsequently diced, the dies are packaged, and the chips are ready for integration into the target rad-tolerant electronic system. As part of the previous STTR, Triad Semiconductor personnel, along with UT-Knoxville students and faculty, jointly developed a rad-hard VCA that contains ADCs, digital-to-analog converters (DACs), switched-capacitor filters, op-amps, and voltage references. The rad-hard VCA has been tested against a similar non-rad-hard version and found to be functional to >300 kRad total dose.

Continued on next page

Continued from previous page

The high-level block diagram, shown in Figure 1, illustrates the electrical signal-processing paths for three distinct types of sensors. Each sensor will require some level of input gain and filtering and an ADC to convert the signals to a digital format. The sensor and electronics signal flow will be presented in the following sections. The three channels of signal conditioning/signal processing will be implemented using the circuitry present on the Triad VCA. Each VCA application-specific integrated circuit (ASIC) contains multiple single-ended operational amplifiers, biquad filters designed as input anti-aliasing filters for the sigma-delta modulators, which are also on the ASIC, and a bandgap voltage reference.

ASICs are very important to electronic systems for multiple reasons. First, integrated circuits (ICs) have the inherent capability to perform numerous electrical functions and operations within one area with efficient space. Not only do ICs optimize circuit density, but they also offer improved matching behavior performance (i.e., consistency from IC to IC) when compared to using individual functional blocks to accomplish the same operation. This is because the IC fabrication process, although precise, is not perfect, and silicon substrate variations from chip to chip are inevitable. Combining multiple functions into one IC effectively reduces matching errors and provides minimal variation from expected results.

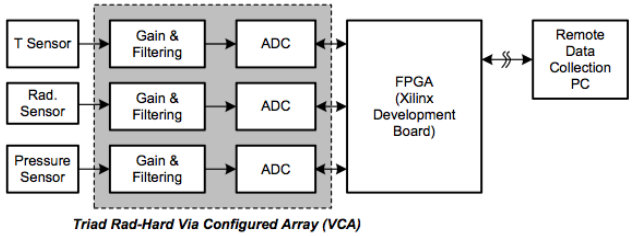


Figure 1. Data acquisition system based on commercial and near-commercial rad-hard circuits.

Secondly, as their name implies, ASICs are application specific, which means they can be designed to perform precisely to the requirements of an application. On the other hand, general ICs must be designed to satisfy a wide variety of applications, and nothing comes for free with circuit design. Tradeoffs must be made; thus, certain performance characteristics of the IC will diminish relative to an ASIC. This advantage over general ICs makes ASICs almost necessary, especially when stringent conditions such as extreme environment operation is required.

The overall project was divided into four tasks, each of which provided clear objectives and associated metrics for performance evaluation. These are summarized below:

Task 1. Electronics design and hardware selection. Developed a detailed functional block diagram of the proposed data acquisition system.

Task 2. Detailed system design and fabrication. Using the analog blocks available in our currently pre-configured VCA, performed a detailed schematic design of our system to include the signal-processing blocks for temperature, radiation, and pressure.

Task 3. System testing and validation (pre- and post-irradiation and temperature). The system's performance for both pre- and post-irradiation as well as operation at elevated temperature was evaluated.

Task 4. Data analysis and presentation. Data taken from the pre- and post-radiation/temperature evaluation was analyzed to quantify variations.

Testing was performed at the Arizona State University Gammacell (^{60}Co) facility. The test setup is shown in Figure 2. For the purposes of radiation testing, three complete systems (Systems 1, 4, and 5) underwent radiation exposure within the Gammacell 220. This is enough of a sample size to effectively analyze the radiation tolerance of the system while also preserving two systems (Systems 2 and 3) for any future preradiation uses. System 5 was irradiated to a total dose of 200 kRad, and the other two systems, System 1 and 4, were irradiated to a total dose of 300 kRad. The project proposal stated a requirement of only 200 kRad total dose exposure for each system, but typical radiation "tolerant" qualification for circuitry is at the threshold of 300 kRad total dose, which is useful for making claims about the system in conference or journal report submissions. Figure 3 shows an image of the rad-hard board inside the containment chamber before the chamber is closed and lowered into the gamma radiation pool to commence the test.

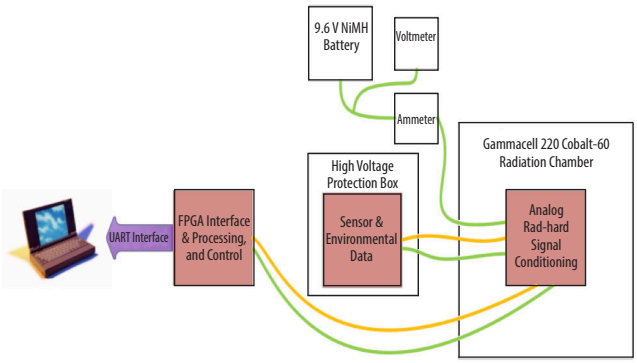


Figure 2. Radiation-hardened test setup.

Continued on next page

Continued from previous page

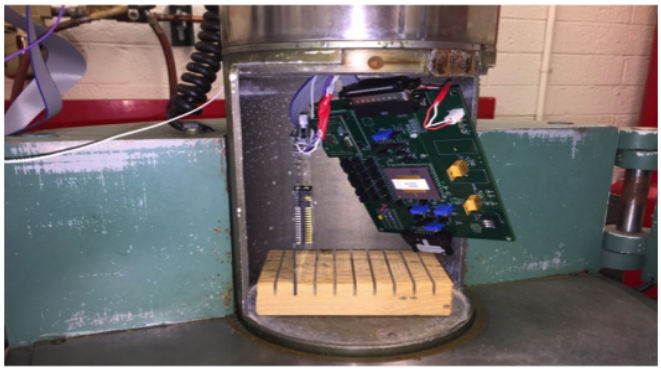


Figure 3. Actual test board being loaded into the Gammacell irradiator.

Performance characteristics measured during the test runs included supply current, temperature, barometric pressure, and gamma event rate. All data were taken during irradiation and were as expected except for some temperature drift. The reason for this is not completely clear since the pressure data showed no drift after being processed by an ADC on the same board. We presently expect some difference was exhibited between the room temperature monitor and the system temperature sensor.

Summary

We have presented the results of the NEET 2 project "Radiation Hardened Circuitry Using Mask-Programmable Analog Arrays." The testing and validation task was divided into two main phases: system calibration and radiation testing. The calibration phase was completed solely at Oak Ridge National Laboratory using onsite environmental temperature chambers, finely tunable pressure generators, and high-voltage equipment for the G-M tube output pulse. The radiation testing, using a ^{60}Co gamma source, took place at Arizona State University in a laboratory under the direction of Dr. Keith Holbert.

Quantifying Software Dependability of Safety Critical Instrumentation and Control Systems in Nuclear Power Plants

Carol Smidts,
Fuqun Huang,
Xiang Li

Ohio State University

"To measure is to know."
—Lord Kelvin

" 'Tis evident that all reasonings concerning matter of fact are founded on the relation of cause and effect, and that we can never infer the existence of one object from another, unless they be connected together, either mediately or immediately."
— David Hume

Goal

The current transition from analog to digital instrumentation and control systems is leading to a significant increase in the number and variety of software-based systems to be found in nuclear power plants. It is a widely accepted fact that hardware systems are inherently different from software systems. Their failure modes and failure mechanisms differ drastically. Unlike hardware, software does not wear and is highly non-linear. Software systems now count millions of lines of code and software complexity is escalating at an unprecedented pace. As such, the challenges faced in software design, development, and testing are distinct from those encountered for hardware systems. One such distinct challenge includes the trust one can place in software-based systems once they have been developed, the ability to analyze and assess this level of trust, and the ability to control the software development process to generate software-based systems at a given level of trust. The trust placed in software is typically termed software dependability. The lack of systematic science-based methods for quantifying software dependability in software-based instrumentation and control systems, particularly in safety critical applications, has shown itself to be a significant inhibitor to the expanded use of modern digital technology in the nuclear industry. This issue is rendered significant by the fact that analog technology is aging and becoming obsolete (i.e., replacement parts are difficult or impossible to find), that the new generation of nuclear power plant engineers is now more familiar with digital technology than it is with analog technology, and that the benefits that digital technology offers cannot be tapped into. These benefits include enhanced features, greater diagnostics, prognostics, and online monitoring capabilities and added flexibility.

Continued on next page

Continued from previous page

The current licensing methods and acceptance criteria for I&C systems in U.S. nuclear plants (new and current fleet) are based on NUREG-0800 Standard Review Plan, Chapter 7,: "Instrumentation and Control," and the associated Branch Technical Positions BTP-7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," and BTP-7-19, "Diversity and Defense-in-Depth." The current regulatory review process described in BTP-7-14 does not use a quantitative basis and instead depends on the qualitative assessment of the reviewer. During recent reviews of BTP-7-19 by the NRC Advisory Committee on Reactor Safeguards (ACRS), it was reaffirmed that no credit would be given for digital system reliability in the context of Digital Common Cause Failure (DCCF) review and approval because the industry data were not sufficient to provide the NRC with a viable justification for accepting dependability -based analysis for digital system software.

To address the need for quantification and to give a more objective basis to the review process and reduce regulatory uncertainty, *measures and methods are needed to assess dependability early and throughout the life-cycle process of software development*. The results of these assessments can be used in two different ways: (1) to guide development and (2) to build a dependability case. Development guidance will enhance dependability of the final software product thereby reducing the regulatory uncertainty. This will support the current NRC licensing regime and in particular support the application of Independent Verification and Validation (IV&V) techniques, which are required for new reactor or existing reactor upgrades in accordance with USNRC Regulatory Guide 1.168 and the associated IEEE-1012 (1986).

Dependability is commonly considered as a general concept that encompasses different attributes (i.e., reliability, safety, security, availability and maintainability). One [1]–[4] or two [5][6] software dependability attributes can already be quantified using existing models, but an integrated framework for quantifying all of the attributes is ultimately desired.

This project aims to develop an integrated method for quantifying software dependability. This approach should enable practitioners to assess various software dependability attributes at different stages of the software lifecycle.

Current Status

Our research emphasizes identification of the cause-effect mechanisms that lead to failing to meet the dependability requirements and the needs of the system. Subsequently, quantification is nothing else but an assessment of these cause and effect relationships. Our focus on causality comes from an attempt to steer away from the softer (and therefore lesser actionable) relations typically used to assess dependability attributes such as those found in typical correlation models.

Expert opinion elicitation [7] has been used to extract the knowledge of software dependability experts as it pertains to the causal mechanisms and their dependencies. Three panels of experts have been held consecutively to progressively enrich and refine these domain models. Expert Panel A focused on dependencies between software dependability attributes, and the causal mechanisms involved in failing to meet one of the dependability attributes. These causal mechanisms are expressed using causal graphs. Expert Panel B focuses on a verification of the main causal mechanism graphs, on the refinement and enrichment of the graphs and on the identification of measures, measurement approaches, and measurement tools for the concepts contained in the graphs. Expert Panel C is focused on the elicitation of additional experts that will help identify missing measures. We contacted over 100 experts; 47 of these experts agreed to participate in the panels. We received 14, 24, and 7 responses for Panels A, B, and C, respectively.

Questionnaires were designed for each panel and the experts provided textual responses to the questions. The causal knowledge embedded in the natural language texts was extracted and represented using a new notation system (with a sample notations shown in Table 1), called Causal Mechanism Graph (CMG) [8]. This notation system was found to be sufficiently powerful to express most aspects of causality found in the texts.

Each expert response was converted to an individual CMG. These CMGs were then merged to obtain consensus knowledge and sliced to extract knowledge pertinent to given questions of interest. For example, focusing on the high-level dependencies between various dependability attributes, we developed Figure 1. The main causal mechanisms for software reliability, safety, security, availability, and maintainability were also obtained [9].

Questionnaires related to measurement of the concepts in the main causal mechanism graphs were yielded a total of 50 entities (e.g., software security failures), 124 related properties (e.g., *impact*), and 265 measures for these properties (e.g., degree of loss of confidentiality for a security failure). We are now awaiting additional inputs from Expert Panel C for the remaining measures. These measures integrated with the main CMG form a comprehensive cause-effect network that can be later used to construct quantification models.

Continued on next page

Continued from previous page

Table 1. A sample of the notations used in Causal Mechanism Graphs.

Symbol	Name	Description
$a_1 \rightarrow a_2$	Imply	Directed correlation, involving a broad class of dependency. When one variable implies another variable, it means dependency exists between the two variables (say a1 implies a2). Such dependency allows one to make inference about one variable according to another variable. "Imply" is not direct causality, but variables involved in this relation may share some common causal factors.
<arg1, arg2, arg3 >	Constraint	Describes the *scenario* for which a relation is present. Arg1 represents the scenario, while arg2 represents the type of the relation. There are three types of relations: positive relation represented by "+", negative relation represented by "-", and undefined or neutral relation left as blank. Arg3 describes the strength of the relation by a number.

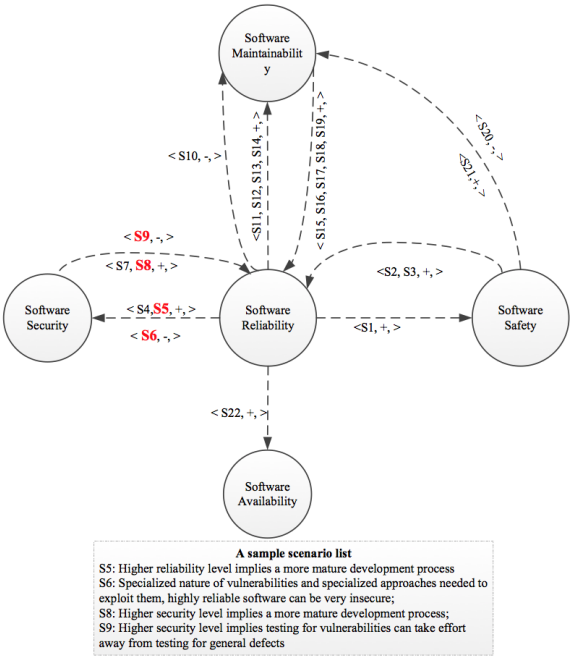


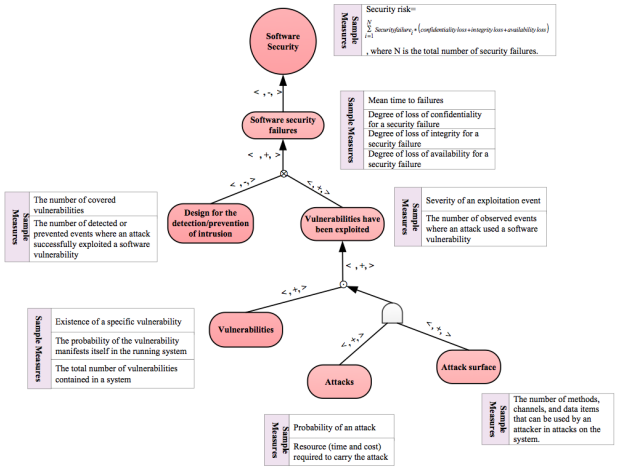
Figure 1. The dependencies between software dependability attributes.

Impact

This project has contributed to the software dependability domain in the following aspects:

1. Proposed an integrated framework to quantify software dependability attributes
2. Designed a series of questionnaires to elicit experts' knowledge on dependencies, causal mechanisms, and measurement in the software dependability domain
3. Designed a new notation system to represent, model, merge, and analyze experts' mental knowledge
4. Extracted the most important entities that influence various software dependability attributes
5. Extracted measures for these entities.

These achievements provide a solid foundation for constructing systematic quantification models that can incorporate evidence at different stages of the software lifecycle. Such quantification models can be further used to improve software dependability design and manage dependability risks.



REFERENCES

[1] M. Lyu, *Handbook of software reliability engineering*. Los Alamitos, Calif.: IEEE Computer Society Press, 1996.

[2] O. Alhazmi, Y. Malaiya and I. Ray, "Measuring, analyzing and predicting security vulnerabilities in software systems," *Computers & Security*, Vol. 26, No. 3, pp. 219–228, 2007.

[3] K. Trivedi, G. Ciardo, B. Dasarathy and M. Grottke, A. Rindos, B. Varshaw, "*Achieving and assuring high availability,*" Service Availability. Springer Berlin Heidelberg, pp. 20–25, 2008

[4] M. Riaz, E. Mendes and E. Tempero, "A systematic review of software maintainability prediction and metrics," In *Proc. ACM-ESEM*, Oct. 2009, pp. 367, 377.

[5] A. B. Brown, "Towards availability and maintainability benchmarks: a case study of software raid systems," University of California at Berkeley, Berkeley, CA, Technical Report, 2001.

[6] V. Sharma and K. Trivedi, "Quantifying software performance, reliability and security: An architecture-based approach," *Journal of Systems and Software*, Vol. 80, No. 4, pp. 493–509, 2007.

[7] C. Smidts, F. Huang, X. Li and C. Mutha, "A Method for Quantifying the Dependability Attributes of Software-Based Safety Critical Instrumentation and Control Systems in Nuclear Power Plants," In *Proc. NPIC-HMIT*, February 2015.

[8] F. Huang and C. Smidts, "Eliciting and Modeling Causal Mechanisms," unpublished, submitted to MIS Quarterly.

[9] Fuqun Huang, Xiang Li, Boyuan Li, Chetan Mutha, Ted Quinn, Carol Smidts, "Software Dependability: from Causal Mechanisms to Dependencies," submitted to ISSRE 2015.