SAN97-2766C
CONF-971172--

Cost-Effective Instrumentation and Control Upgrades for Commercial Nuclear Power Plants Using Surety Principles Developed at Sandia National Laboratories*

Gary E. Rochau, Nuclear Reactor Safety Department
Larry J. Dalton, Command and Control Software Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0742
USA

Abstract

Many nuclear power plants use instrument and control systems based on analog electronics. The state of the art in process control and instrumentation has advanced to use digital electronics and incorporate advanced technology. This technology includes distributed microprocessors, fiber optics, intelligent systems (neural networks), and advanced displays. The technology is used to optimize processes and enhance the man-machine interface while maintaining control and safety of the processes. Nuclear power plant operators have been hesitant to install this technology because of the cost and uncertainty in the regulatory process. This technology can be directly applied in an operating nuclear power plant provided a surety principle-based "administrator" hardware system is included in parallel with the upgrade. Sandia National Laboratories has developed a rigorous approach to High Consequence System Surety (HCSS). This approach addresses the key issues of safety, security, and control while satisfying requirements for reliability and quality. HCSS principles can be applied to nuclear power plants in a manner that allows the off-the-shelf use of process control instrumentation while maintaining a high level of safety and enhancing the plant performance. We propose that an HCSS administrator be constructed as a standardized approach to address regulatory issues. Such an administrator would allow a plant control system to be constructed with commercially available, state-of-the-art equipment and be customized to the needs of the individual plant operator.

1. INTRODUCTION

Most of the instrumentation and control equipment currently installed at U.S. nuclear power plants is based on analog electronics. While this equipment is safe and operable, it is now commercially obsolete, difficult and expensive to maintain, and inefficient[1]. The state of the art in process control and instrumentation has advanced to use digital electronics and incorporate technology such as distributed microprocessors, fiber optics, intelligent systems (neural networks). Furthermore, advanced displays optimize processes and enhance the man-machine interface while maintaining control and safety of the processes. These advances have not been captured by U.S. nuclear power plants due to lack of favorable cost/benefit analysis of such technologies combined with the uncertainty of obtaining regulatory approval of the new technology.

---

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

[1] J. Naser, "Integrated Instrumentation and Control Digital Upgrades for Cost Reduction," Proceedings: Distributed Digital Systems, Plant Process Computers, and Networks, EPRI TR-104913, March 1995.

DISCLAIMER

2. STATUS OF I&C SYSTEMS IN THE UNITED STATES

Instrumentation and Control (I&C) technology is key to nuclear plant safety, reliability, and availability. A majority of the I&C systems used in U.S. nuclear power plants use analog circuits for the plant safety system. These systems must be tested frequently, adding to the possibility of human error, causing a plant trip. An inadvertent signal can take a nuclear power plant off-line in an instant. Consequently, the cost of an I&C failure resulting in a plant trip is substantial when compared to the cost of new systems provided the new system significantly reduces the probability of a trip.

High-reliability instrumentation and control systems are needed for the cost-effective operation of the nuclear power plant. A stable and mature technology is needed to obtain the regulatory approvals. However, I&C digital technology is a developing field of technology, and I&C suppliers are rapidly moving away from supporting the safety systems of nuclear power plants. Manufacturers have discontinued product lines without replacements, failed to maintain an adequate spare parts inventory, and decreased service support.[2] To counteract this trend, nuclear power plants must begin to transition to the commercially available digital instrumentation currently used by the process control industry.

Industry-wide, I&C systems currently have highly customized Process Control Systems "tuned" to meet the operating characteristics for the individual plant and standardized Plant Protection Systems supplied by a single vendor to meet regulatory requirements. Thus, as the equipment becomes obsolete, a nuclear power plant operator is faced with a dilemma: should the existing technology be maintained in some fashion, or should the technology be upgraded to state-of-the-art and necessary regulatory acceptance obtained? This dilemma is being considered under existing economic conditions, increasing competition from other power producers, and uncertain regulatory issues. The majority of the industry has chosen to maintain I&C systems and upgrade them, on a subsystem basis, when plant performance is impacted. Consequently, there is no common vision for the "Control Room of the Future."

3. BENEFITS OF USING DIGITAL TECHNOLOGY

Using digital technology as the basis for nuclear power plant I&C upgrades allows the nuclear market to tap the rapidly developing digital I&C market for industrial process control. Accessing this technology, the nuclear power plant operator can be assured not only of efficient and reliable I&C operation, but also of a much larger supply of replacement parts and future replacement systems, thereby reducing plant operations and maintenance costs. In addition to availability of hardware, digital technology provides a new infrastructure that allows the plant operator to enhance the efficiency of plant operation, to increase the plant capacity factor, and possibly to reduce the cost of generated electricity.

The use of digital technology is estimated to reduce I&C-related operations and maintenance costs by 10% and increase plant power output by 5%. Industry-wide, the total U.S. nuclear generation costs would be reduced by $1 billion per year and power produced would increase by 30 million MWh.

---

[2] W. G. MacFarland, "A Utility Perspective," Proceedings: Joint DOE/EPRI International Conference on Cost-Effective Instrumentation and Control Technology Upgrades for Nuclear Power Plants, EPRI TR-105148, August 1995.

Replacement of this generating capacity would require the construction of five 1000 MWe fossil plants costing $5-10 billion[3].

4. REGULATORY ISSUES ASSOCIATED WITH DIGITAL I&C SYSTEMS

The successful integration of digital technology into I&C systems at U.S. nuclear power plants faces five significant challenges[4]:

1) Technical uncertainty inherent in the introduction of new technology;
2) Shift of existing technology base from analog experience;
3) Technical problems identified from applications of digital I&C in other nuclear power plants;
4) Difficult, time-consuming, and customized licensing approach; and
5) Lack of consensus on issues underlying evaluation and adoption of I&C technology and the means to obtain a satisfactory resolution.

The key regulatory issues can be summarized as six technical issues and two strategic issues[5]:

Technical Issues:

1) Systems aspects of digital I&C technology - How do all the systems interact?
2) Software quality assurance - How do we know that the software will always perform according to the requirements?
3) Common-mode software failure potential - How do we avoid having bad tools in the software toolbox which cause redundant systems to fail?
4) Safety and reliability assessment methods - How do we derive a probability of failure for a digital system?
5) Human factors and human-machine interfaces - How does digital technology change the operator interface with the plant?
6) Dedication of commercial off-the-shelf hardware and software - How digital technology from the process control industry be used?

Strategic Issues:

1) Case-by-case licensing process - What assurance does the licensing of one digital system give for approval the next system?
2) Adequacy of technical infrastructure - What changes do regulatory authorities need to make to support digital I&C regulation?

These issues are roadblocks for implementing digital I&C technology at nuclear power plants. Since specific regulations are not in effect, the cost uncertainty associated with regulatory acceptance is unacceptable to many plant operators.

---

[3] N. Fletcher, etal., "Joint Nuclear Power Industry/DOE Instrumentation and Control Upgrade Program," Proceedings: Joint DOE/EPRI International Conference on Cost-Effective Instrumentation and Control Technology Upgrades for Nuclear Power Plants," EPRI TR-105148, August 1995.

[4] National Research Council, Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operation and Safety, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Final Report," National Academy Press, Washington D.C., 1997, p. 1.

[5] Ibid., pp. 4-11.

5. HIGH CONSEQUENCE SYSTEMS SURETY APPROACHES USED AT SANDIA NATIONAL LABORATORIES

Sandia National Laboratories, as steward of the U.S. nuclear weapon stockpile, has developed a rigorous approach to High Consequence System Surety (HCSS). Developed to provide for the safety and security of nuclear weapons, HCSS principles can provide significant support in the design of new digital I&C systems. This approach addresses the key issues of safety, security, and control while satisfying requirements for reliability and quality. HCSS is achieved by using four major principles: isolation, inoperability, incompatibility, and independence. Isolation allows a system to be insensitive to external events. Inoperability makes the system safe before the isolation of the system is overwhelmed by an event. Incompatibility makes the system unresponsive to any signals except those which are uniquely identified. Independence is achieved by design to eliminate commonality between safety subsystems. These four principles are maintained in parallel with a system design. Using "state machines" (digital electromechanical devices), the system behavioral model is captured in a system of interlocks and mechanical analogs. These machines model the system with quantifiable integrity, using discriminating devices which are robustly designed to respond to a unique signal. Thus, through the use of state machines, the behavior of a system is monitored, not the specific system controller functions. These concepts have been demonstrated for robotic systems used for remote handling of plutonium parts from nuclear weapons[6].

State machines incorporate hardware programmed Application Specific Integrated Circuits (ASICs) and discriminating devices (mechanical systems) which must be moved into proper position for actions to proceed. In the last few years, the state-of-the-art for such systems has advanced to use micromechanical actuators which are so small that they can be mounted on a digital circuit chip. The mechanisms, shown in Figure 1, have the capability of operating at up to 300,000 revolutions/minute and operate for over 8×10^8 revolutions[7].

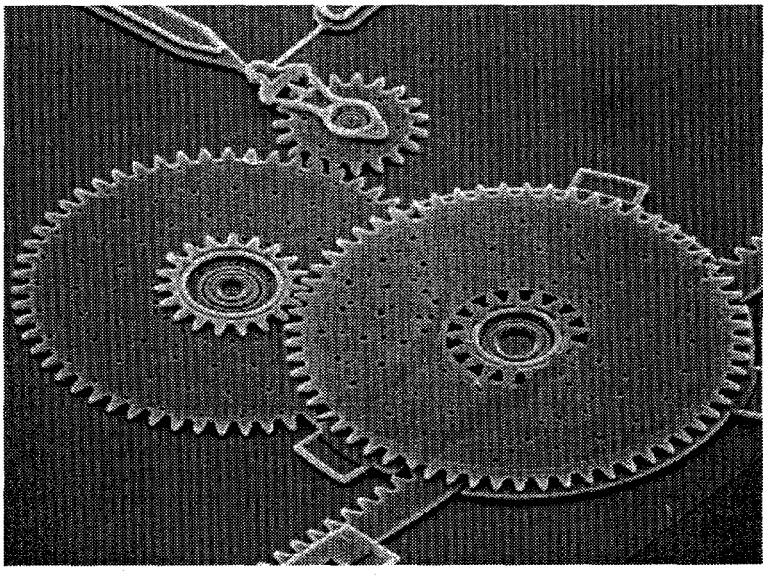

Figure 1. Micromotor with gear train transmission.
(Approx. scale 260 microns, ref.: human hair is about 80 microns)

---

[6] J. Smith, "Micromachined Sensor and Actuator Research at Sandia's Microelectronics Development Laboratory," Proc. Sensors Expo Philadelphia '96, pp. 143-148, Oct. 1996.

[7] Sandia National Laboratories, "High Consequence System Surety," version 3, video tape, 8 minutes, March 31, 1995.

6. APPLICATION OF HCSS TO NUCLEAR POWER PLANT I&C SYSTEMS

We believe that HCSS principles can be applied to nuclear power plants in a manner that allows the off-the-shelf use of process control instrumentation while maintaining a high level of safety and enhancing the plant performance. The Control Room of the Future can incorporate digital I&C technology directly from the process control industry and can also incorporate a surety system to implement regulatory controls and safeguards. A plant control system can be constructed with commercially available, state-of-the-art equipment that can be customized to the needs of the individual plant operator and phased into the plant as economic conditions dictate. A standardized HCSS system would be constructed for a specific Nuclear Steam Supply System (NSSS), which would contain the model for safe operation of the system. The HCSS "administrator" is the state machine for the NSSS and needs to be manipulated into the proper configuration by the I&C system. As long as the proper configuration of the HCSS administrator is maintained, the I&C system would function at any enhanced level or with direct operator control. Failure to maintain the administrator would be the equivalent of a plant trip in some instances or prohibition of an operator action in others.

In theory, the HCSS administrator functions as a digital, electromechanical analog computer modeling the reactor system. The administrator responds to and generates digital signals, but uses mechanical analogs and interlocks to model the system operational space.

Three advantages of an HCSS administrator are:

1) Utilizes state-of-the-art I&C technology from the process control industry,
2) Allows regulatory issues to be addressed through a standardized surety principle-based administrator, and
3) Minimizes concern for safety-related I&C software design, quality assurance, and maintenance.

In practice, the HCSS administrator would be placed in parallel with the plant process control system (Figure 2). The administrator would have specific requirements for proper alignment and have exclusive control of plant safety-related components. The plant process control system must meet the input requirements of the HCSS administrator in order to maintain control. Should this condition not be maintained, the administrator would take control of the reactor to place it in a safe condition. Under operator control, the administrator would allow any action permitted under the system model and prohibit operator actions that would violate the system model. This configuration scheme may eliminate the need for extensive software testing and quality control. We believe that rather than examining all possible failure scenarios, the surety of the system is maintained by monitoring the system parameters to be within the operational space of the system and preventing those parameters from leaving that space.

In application, the HCSS administrator would be installed in the plant first, eventually replacing the plant protection system. The administrator would be subject to intense regulatory review, but this review would be based on the system model, not on unresolvable issues. The plant operator would then be allowed to make I&C system equipment changes as need dictates and economics allow. These I&C changes should be accomplished with a minimum of regulatory review.

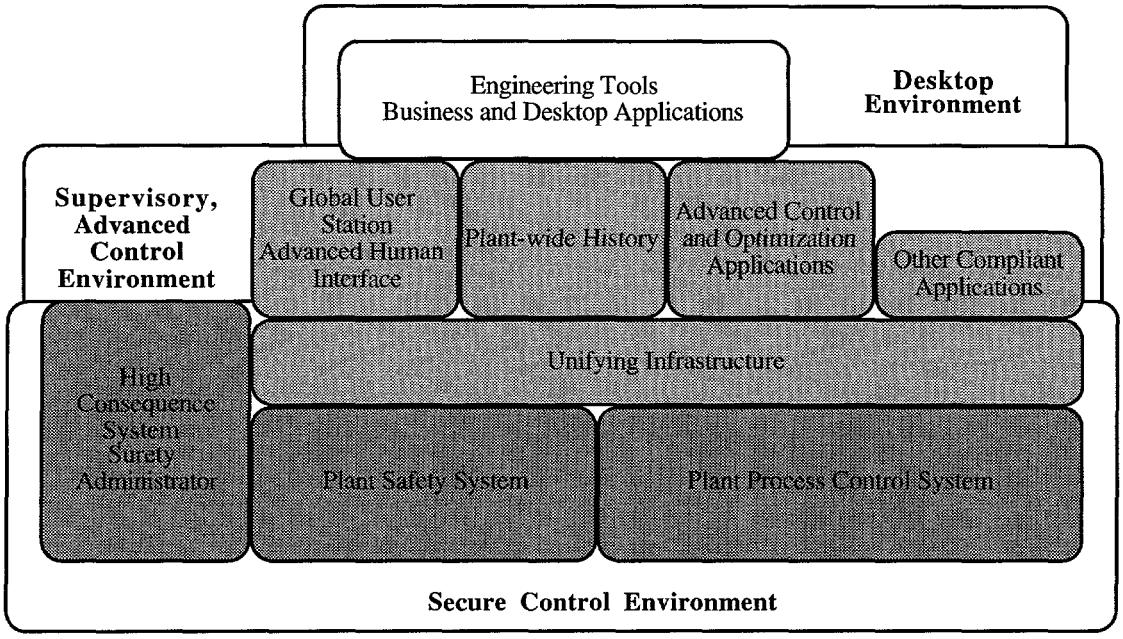

Figure 2. High Consequence System Surety (HCSS) administrator applied to a state-of-the-art process control system.[8]

7. CONCLUSION

Cost-effective instrumentation and control upgrades for nuclear power plants are possible using standardized digital technology if a standardized approach can be found to resolving regulatory issues. A system "administrator" developed for standardized nuclear reactor types which employ High Consequence System Surety (HCSS) principles developed at Sandia National Laboratories meets this need. An HCSS administrator would allow the nuclear power industry to utilize the state-of-the-art digital I&C technology from the process control industry while maintaining the same level of system safety required by nuclear safety regulators.

[8] Process Control System is the TotalPlant® Solution System schematic, courtesy of Honeywell Corporation.