Instrumentation and Controls Division

QUALIFICATION ISSUES FOR ADVANCED LIGHT-WATER REACTOR PROTECTION SYSTEMS*

Kofi Korsah, Robert L. Clark
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6010

Christina Antonescu
NRC Office of Nuclear Regulatory Research
Rockville, MD 20852

Submitted for presentation at the
American Nuclear Society Topical Meeting
Garden Plaza Hotel, Oak Ridge, Tennessee

April 18-21, 1993

*Research sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission under Interagency Agreement number 1886-8179-8L and performed at Oak Ridge National Laboratory, managed by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under contract DE-AC05-84OR21400.

QUALIFICATION ISSUES FOR ADVANCED LIGHT-WATER REACTOR PROTECTION SYSTEMS*

Kofi Korsah, Robert L. Clark
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, Tennessee 37831-6010
(615) 576-6064

Christina Antonescu
U.S. Nuclear Regulatory Commission
Rockville, Maryland 20852
(301) 492-3824

ABSTRACT

The instrumentation and control (I&C) system in advanced reactors will make extensive use of digital controls, microprocessors, multiplexing, and fiber optic transmission. Elements of these advances in I&C have been implemented on some current operating plants. However, the widespread use of the above technologies, as well as the use of artificial intelligence with minimum reliance on human operator control of reactors, highlights the need to develop standards for qualifying the I&C used in the next generation of nuclear power plants.

As a first step in this direction, the protection system I&C for present-day plants was compared to that proposed for advanced light-water reactors (ALWRs). An evaluation template was developed by assembling a configuration of a safety channel instrument string for a generic ALWR, then comparing the impact of environmental stressors on that string to their effect on an equivalent instrument string from an existing light-water reactor. The template was then used to suggest a methodology for the qualification of microprocessor-based protection systems. The methodology identifies standards/regulatory guides (or lack thereof) for the qualification of microprocessor-based safety I&C systems. This approach addresses in part issues raised in NRC policy document SECY-91-292, which recognizes that advanced I&C systems for the nuclear industry are "being developed without consensus standards, as the technology available for design is ahead of the technology that is well understood through experience and supported by application standards."

I. INTRODUCTION

In 1991 the NRC initiated the *Qualification of Advanced Instrumentation and Control Systems Program* at ORNL to develop an understanding of the technical issues involved in evaluating long-term properties and performance of "advanced" digital I&C systems proposed for use in ALWRs. The objective is to support the development of standards that will help ensure the

*Research sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission under Interagency Agreement number 1886-8179-8L and performed at Oak Ridge National Laboratory, managed by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under contract DE-AC05-84OR21400.

operability and qualification of such I&C systems in a nuclear power plant environment.

Initial studies under this program have focused on protection systems and the I&C portions of engineered safety feature actuation systems. Some of the hardware issues identified for the proposed systems that were studied are reported in this paper, and others can be found in references 1 and 2.

The forthcoming change from completely analog systems to fully digital-computer-based I&C systems can lead to significant benefits. These benefits include reduced stress on I&C components from frequent maintenance and testing cycles due to the self-testing/diagnostic capabilities of microprocessor-based systems, and the potential reduction in system costs and cabling due to sharing of data transmission lines via multiplexing equipment. However, the introduction of digital technology in safety-related systems of nuclear power plants also raises key issues relating to the systems' *environmental* qualification and *functional* reliability. For example, does the new hardware introduce new degradation mechanisms that could adversely impact the safety of the plant? To what extent can present qualification standards and acceptance criteria be extended to protection system I&C proposed for ALWRs?

To answer these questions an evaluation template was developed by assembling a configuration of a protection system for a generic ALWR, then comparing the impact of environmental stressors on system components to their effect on an equivalent channel from an existing light-water reactor. Hardware issues considered in the template include typical I&C components and materials, and methods of protection against the environment. Functional issues considered include independence, communication methods, and capability for test and calibration. The template is then used to suggest a methodology for the functional and environmental qualification of microprocessor-based protection systems. The methodology identifies standards/regulatory guides (or lack thereof) for the qualification of microprocessor-based safety I&C systems.

II. ENVIRONMENTAL, FUNCTIONAL, AND AGING DATA TEMPLATES FOR PROTECTION SYSTEMS

We addressed functional and environmental qualification issues for ALWR protection system I&C by developing an environmental, functional, and aging data template for the protection channel of each current ALWR design. Using information provided by manufacturers, we identified environmental conditions and stressors to which I&C equipment in reactor protection channels may be subjected. The resulting data were then compared to a similar template for an instrument string typically found in an analog protection channel of a present-day nuclear power plant.

A typical instrument string (e.g., reactor coolant flow) is shown in Fig. 1. The figure, adapted with modification from reference 3, shows environmental conditions typically found at the location of major components in the string, materials in the system components that contribute to system aging, and the stressors that contribute to component degradation. Note that the diagram in Fig. 1 refers to identifiable analog components in the "path" of a (flow) process variable monitored for a protection system function. In a microprocessor-based protection system however, this identification of individual components through trip bistable circuitry is not meaningful following the multiplexer(s), since a single microprocessor may perform multiple functions under software

control. Thus, Fig. 2 shows an environmental, functional, and aging data template for a protection channel of a generic ALWR. Because of space considerations, only an abridged version is presented in this paper. The following discussion refers to Figs. 1 and 2.

A. Transmitters and Cables

Although there are several similarities in the approach taken by ALWR manufacturers in the implementation of protection system I&C, there are also some differences. For example, in some cases the transmitters performing protection system functions will be hardwired to the protection cabinets, whereas in others the signal from containment will be processed by multiplexing equipment strategically located throughout the plant outside containment. In all cases studied, indications are that conventional analog transmitters will be used and that environmental conditions in containment (e.g., temperature, humidity, and radiation) are not likely to be significantly different from those in existing nuclear plants. This observation may also apply to EMI/RFI sources to which instrumentation within containment will be subjected. Under normal plant operating conditions, transmitters are subjected to aging stressors from temperature, moisture, radiation, and vibration, with elevated temperature being the dominant stressor in most cases.[3,4] However, transmitters may also be subjected to aging stressors from testing and maintenance practices, the monitored process, and power supply variations. Humidity levels under normal plant conditions should not pose a problem for nuclear-qualified transmitters, since such transmitters are sealed for design basis accidents (DBA) such as main steam line breaks.

Presently, most transmitters for use within containment have a qualified life of 10 to 40 y, depending on type, materials of construction, and other factors. For example, a strain gauge transmitter typically has a qualified life of 40 y, while a differential capacitance transmitter may be qualified for only 10 y. Seals and gaskets for transmitters may have a much shorter qualified life (e.g., 4 y).[3] It is reasonable to assume that the performance and lifetime of transmitters will be the same for ALWRs as for conventional reactors.

Although conventional analog transmitters are most likely to be used, I&C systems for the next generation of nuclear power plants are still evolving, and it is possible that some form of "smart" transmitter technology could be used in future plants. Work is progressing on the development of several technologies with low-power capabilities, such as CMOS silicon-on-insulator, that can withstand a total radiation dose of several tens of megarads (Si)[5]. This will enable the advantages of smart transmitters to be exploited for the nuclear power plant containment environment. These advantages include (1) capability for remote calibration resulting in reduced personnel exposure, (2) capability for remote verification of calibration, (3) capability for remote range changes, (4) automatic diagnostics, and (5) little cost difference between smart and conventional transmitters.

Apart from improvements in transmitter electronics, new pressure sensing technologies are also being evaluated to improve pressure sensor performance[6]. Present-day pressure transmitters are subject to certain failure modes that are unacceptable, especially in safety-related systems of nuclear power plants. An example is the loss of oil from oil-filled transmitters[7]. This type of failure significantly increases the transmitter's response time and may also limit its dynamic range. These effects, however, are not observable during steady-state operation. Technologies that are currently being investigated for the development of improved pressure sensor performance include fiber optic and mechanical tuning fork resonance frequency[6].

As with transmitters, cable types and connections within ALWR containments are not likely to be different from those used in present-day reactors. Stressors that are known to enhance cable degradation include temperature, radiation, and moisture. Cable materials experience ambient temperature and radiation for long periods of time. Under accident conditions, however, they may be subjected to much higher radiation and temperature transients, and this is taken into consideration in their design and qualification. Electrical cables are normally qualified for 40 y, and their performance and lifetime will be substantially the same for ALWRs as for conventional reactors.

As far as the protection channels of ALWRs are concerned, optical fiber data links will be used for interchannel communication and, in some cases, between subsystems within a channel. Fiber optic cables also will be heavily employed in the (distributed) control system and in the interface between the trip system and the engineered safety features systems (ESFs). Several environmental stressors, or their synergistic effects, can result in aging and increased failure rates for certain fiber optic cables. These stressors include high humidity and high temperatures,[8] coupled with choice of fiber coatings.[9] However, protection system cabinets are typically located in an area having a lower radiation level than exists in containment. Temperature and humidity levels are also less harsh. Typically, the set of protection system cabinets for *each* protection channel of an ALWR will be placed in a geographically separate Class 1E room. Ambient temperatures at such locations have been estimated to be between 65 and 75°F, and humidity levels are likely to be similar to present-day control-room environments. Aging tests have shown that, with suitable coatings, present-day fibers can withstand at least 20 y exposure to an extreme outside plant climate.[10] This longevity suggests that the proposed application of optical fibers in the control systems and in the interface between the protection system and the ESFs in nuclear power plants could be encouraged. (The environment of such cabinets and systems is generally less harsh than in containment.) This conclusion appears to be supported by a study of the performance of fiber optic cables from several vendors[11]. The study, which was conducted to determine the radiation sensitivity of commercially available radiation-hardened fiber optic cables, concluded that fiber optic cables are currently available which perform reliably in nuclear reactor environments. While some fibers fluoresce enough under radiation to obscure low-strength (nanowatt) signals, others (such as pure silica core fibers) exhibit no significant performance change with doses as high as 3800 Gy. In fact, any conventional transmitter will couple about 10^6 times as much light into fibers as flourescence does.

B. Stressors

The same stressors that contribute to I&C system age degradation in present-day reactors will also affect ALWRs. Examples are elevated temperature, smoke, chemical spray, vibration, radiation, moisture, environmental cycling, and EMI/RFI.

EMI/RFI is an important stressor because of increased use of microprocessor-based technology in ALWR safety-critical I&C systems. A study of the *licensee event report* database over a 10-y period (1982-1991) shows that the fraction of EMI/RFI-related protection system events is significant compared to traditionally recognized environmental stressors such as elevated temperature. Although digital systems typically have higher noise margins than analog systems, their failure modes are often quite different and much less predictable. Also, trends toward the use of higher clock frequencies, lower logic voltage levels, and ever denser packages lead to increasing probability of upsets. The increasing levels of integration tend to decrease the noise

immunity of the digital devices. While on-chip protection methods help somewhat to protect the devices against interference-induced damage, the record shows that they have not eliminated upset problems. Studies show that even fault-tolerant systems generally do not achieve reliable system performance in some high-EMI environments.[12] Ongoing research under the I&C qualification program is geared towards improving our understanding of microprocessor behavior in EMI/RFI fields.

Smoke is another important stressor because it may cause electronic systems relatively far removed from a fire to degrade and malfunction over time. Fire-produced particulates that settle on electronic boards and other equipment contain chlorides and sulfides. In the presence of moisture and air (oxygen), the particulates form electrolytes which can eat away the metal interconnections on electronic boards or other metal contact surfaces, thereby causing degradation and system faults long after the occurrence of a fire.

We investigated the precautions taken by ALWR manufacturers to protect safety systems against smoke. In general, smoke/particulates are not monitored inside the protection system cabinets. Rather, the entire plant protection system will be designed and qualified for the worst-case operating conditions that can be expected during plant life, and each of the Class 1E equipment rooms will have smoke and temperature sensing as part of the fire protection system.

III. QUALIFICATION OF MICROPROCESSOR-BASED SAFETY SYSTEMS

In this section, we summarize our study by addressing reliability issues for microprocessor-based safety systems from a *systems* (integrated hardware/software) approach, and identifying standards or (lack thereof) for such systems. Where standards are available, areas that may need modification in view of the introduction of advanced I&C in the safety systems of nuclear power plants are discussed. This approach addresses, in part, issues raised in NRC document SECY-91-292, which recognizes that advanced I&C for the nuclear industry "is being developed without consensus standards, as the technology available for design is ahead of the technology that is well understood through experience and supported by application standards."

Fig. 3 depicts the qualification process for a generalized (analog) safety system in a present-day nuclear power plant. It also identifies the most significant standards related to the particular qualification activity. Fig. 4 attempts to identify some areas in the qualification process that could be (or are being) strengthened for application to microprocessor-based safety systems. As illustrated in the figures, the goal of qualification is to achieve a high degree of *reliability* through the maintenance of quality at various levels of design, implementation, and operation of the safety system.

Requirements for functional reliability of safety systems is embodied in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," and IEEE Std 603-1980, "Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE Std 279-1971 is endorsed by Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." The requirements in IEEE Std 603 are independent of the specific equipment used and thus apply to both analog and microprocessor-based safety systems. In fact, Regulatory Guide 1.153 encourages the application of advanced technology such as programmable digital computers in the operation of nuclear power plants if such technology serves to enhance safety. However, the nature of computers/microprocessors poses new challenges to both the functional

and environmental requirements (e.g., independence, separation, diversity, common mode failure, EMI/RFI effects, etc.) for safety system I&C. These issues have been discussed elsewhere,[2] and reflect the minimum set of issues that need to be considered to maintain the reliability of microprocessor-based protection systems at the levels achievable with current analog systems. (It is reasonable to compare reliability measures, acceptance criteria, and standards with those used for analog systems because considerable experience with the latter has been accumulated over the years.) Reliability involves maintaining a high level of confidence in the *design* of the system hardware and software. System verification and validation (V&V) methods are currently the best means of achieving this. It is recognized that ANSI/IEEE 7-4.3.2-1982 is inadequate in addressing acceptance criteria for microprocessor-based safety I&C, and these issues are being addressed in the standard's next revision.[13]

As depicted in Figs. 3 and 4, reliability of safety system I&C also includes ensuring a high level of confidence that the system will perform adequately in its *environment* under normal, design-basis, and post design-basis event conditions. Qualification ensures that Class 1E equipment can perform its safety function(s) with no failure mechanism that could lead to common-cause failures under postulated accident conditions. As illustrated in the figures, equipment qualification is generally handled under environmental, seismic, and fire protection criteria and standards.

Environmental qualification methods are embodied in IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," which is endorsed by Regulatory Guide 1.89, "Qualification of Class 1E Equipment for Nuclear Power Plants." IEEE Std 323-1983 provides further clarification of these environmental qualification procedures. Although the NRC has not specifically endorsed the 1983 version, it has commented that IEEE 323-1983 neither alters the industry guidance provided nor does it alter the NRC's endorsement of acceptable qualification methods. Type testing is the most frequently used method of equipment qualification, and involves subjecting the equipment to the environments and operating conditions for which it was designed. It also includes the concept of aging, in which the equipment is put in a condition which simulates its expected end-of-qualified-life. In this study, we identified environmental conditions and aging stressors to which major components in ALWR protection channels will be subjected, and compared them to environmental conditions and stressors in present-day nuclear power plants. We concluded that many of the environmental stressors are likely to be similar. However, EMI/RFI may be of particular interest as an environmental stressor for microprocessor-based I&C systems. Irrespective of whether a microprocessor-based system is likely to be more or less susceptible to EMI/RFI than its analog counterpart, the fundamental problem which remains is the unpredictable behavior of a software-based digital system to EMI/RFI upsets. Thus, qualification criteria should include EMI/RFI tests with the intent of demonstrating that the protection system will *fail safe* for the worst case EMI/RFI conditions to which the system is likely to be exposed. At present, EMI/RFI susceptibility tests are generally not included in the environmental qualification process. Rather, EMI/RFI is addressed on an individual equipment basis as necessary, such as to demonstrate physical independence of Class 1E and non-Class 1E circuitry in a microprocessor-based protection system.

Seismic qualification criteria are embodied in IEEE 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations." This is endorsed by Regulatory Guide 1.100, "Seismic Qualification of Electrical Equipment for Nuclear

Power Plants." Seismic testing is typically performed as part of an overall qualification program, and is designed to demonstrate an equipment's ability to perform its safety function during and after the time it is subjected to the forces resulting from a defined safe shutdown earthquake. The requirements for seismic qualification of microprocessor-based I&C equipment appear to be no different than for analog I&C equipment, and so continued endorsement of the standard seems appropriate.

The basic design requirements for protection against fire is stipulated in General Design Criterion 3 of Appendix A of 10CFR50 and IEEE-384 "Independence of Class 1E Equipment and Circuits." General Design Criterion 3 requires that structures, systems, and components important to safety be located to minimize the probability and effects fires and explosions. IEEE-384 requires that an electrically-generated fire in a Class 1E division shall not result in the loss of function in the redundant Class 1E division. In addition to these requirements, Appendix R of 10CFR50 requires a defense-in-depth approach to be taken to: (1)prevent fires from starting, (2)detect rapidly, control, and extinguish promptly those fires that do occur, and (3)provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent safe shutdown of the plant. A fire protection system must be able to detect, contain, and suppress a fire. In addition, it must be able to isolate redundant safety channels from the detrimental effects of smoke, heat, and the potential generation of toxic gases. In general, physical separation and fire protection requirements, rather than environmental qualification of the Class 1E equipment, should be relied upon to mitigate the consequences of a fire.

IV. CONCLUSION

This paper has addressed qualification issues for safety system I&C for the next generation of nuclear power plants. It appears from comparing templates for present-day analog protection systems with their ALWR counterparts, as well as standards used for their qualification, that a combination of good engineering design, excellent V&V and qualification procedures, and diversity can result in reliable microprocessor-based safety I&C systems. To achieve this goal, however, adequate standards need to be established. Currently, the standard that establishes criteria for the use of computers in safety systems is ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems of Nuclear Power Generating Stations." This standard is endorsed by Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants." However, ANSI/IEEE-ANS-7-4.3.2-1982 does not adequately reflect the rapid developments in computer technology. A rewrite of the standard is therefore needed and is currently in progress,[13] and is likely to include an expanded software section and an amplification of the IEEE-603 requirements to reflect advances in computer technology.

With the increased application of microprocessor technology to reactor safety systems, EMI/RFI emission and susceptibility criteria need to be established for the nuclear power plant environment.

In present-day plants, physical separation and fire protection requirements, rather than environmental qualification of the Class 1E equipment, are generally relied upon to mitigate the consequences of a fire. This also seems to be a reasonable approach for the next generation of nuclear power plants.

V. REFERENCES

1. KOFI KORSAH *et al.*, "Environmental Qualification and Functional Issues for Microprocessor-Based Reactor Protection Systems," *20th Water Reactor Safety Information Meeting*, Bethesda, MD, October 21-22, 1992.

2. KOFI KORSAH and CHRISTINA ANTONESCU, "A Survey of Issues Associated with Microprocessor-Based Reactor Protection Systems," accepted for presentation at the *Second Intl. Conf. on Nuclear Engr.*, San Francisco, March 21-24, 1993.

3. L. MEYER, *Nuclear Plant Aging Research on Reactor Protection Systems, NUREG/CR-4740,* Idaho National Engineering Laboratory, January 1988.

4. A. C. GEHL and E. W. HAGEN, *Aging Assessment of Reactor Instrumentation and Protection System Components, NUREG/CR-5700,* Oak Ridge National Laboratory, July 1992.

5. J. L. LERAY et al., "CMOS/SOI Hardening at 100 Mrad(SiO_2)," *IEEE Trans. Nucl. Sci., NS-37, No. 6,* 2013 (1990).

6. J. M. WEISS and R. L. SHEPARD, "Evaluation of Advanced Pressure Sensor Technology," *Proceedings of the 8th Power Plant Dynamics, Control & Testing Symposium, May 27-29, 1992, Vol. 1,* 2.01-2.09.

7. *Oil Loss Syndrome in Rosemount Pressure Transmitters*, Compiled by Analysis and Measurements Corporation, AMS 9111 Cross Park Drive, Knoxville, TN 37923, August 1991.

8. M. J. MATTHEWSON and C. R. KURKJIAN, "Environmental Effects on the Static Fatigue of Silica Optical Fiber," *J. Am. Ceram. Soc. 71(3),* 177-83 (1988).

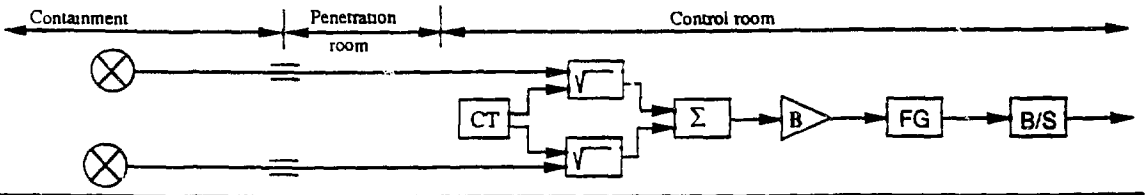
9. K. M. DOTY and K. J. LONG, "Prediction of Shipboard Fiber Optic Cable Service Life," *Proc. Internat. Society Optical Eng. (SPIE), 1174,* 205-18 (1989).

10. *Lightguide Digest, Issue No. 1, 1992,* AT&T Network Systems, P.O. Box 1278, NJ 07962-9905.

11. *Optical Fibers in Radiation Environments*, Electric Power Research Institute, Publication No. TR-100367, 1992.

12. R. J. HANSON, "Interference Effects on Microprocessor and Subsystem Performance," *Eval. Engr.,* 155 (May).

13. J. R. MATRAS, "Technical Note: Rewriting the Standard on the Functional requirements for Computers Used in Safety Systems of Nuclear Power Plants," *Nucl. Safety, Vol. 32,3,* 375-79 (1991).

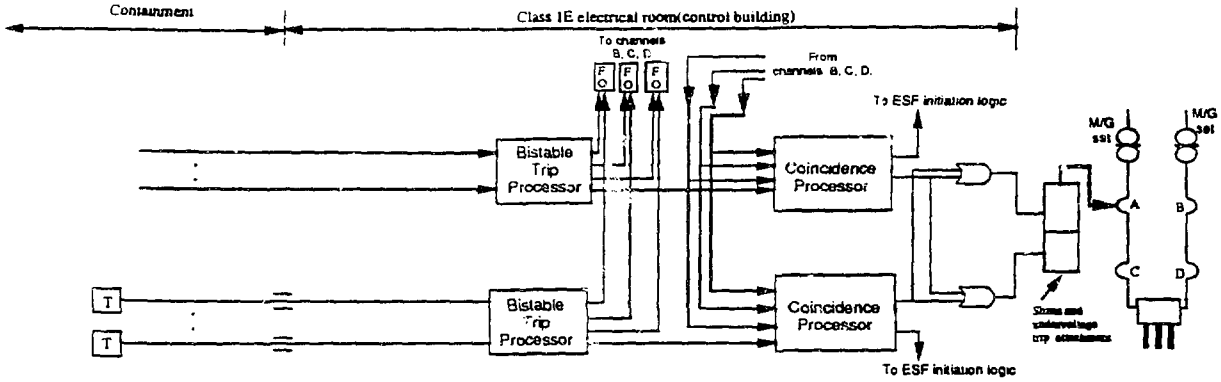


	Flow transmitter	Reactor building cable	Reactor building penetration	Penetration room cable	Calibration/ test module	Square root extractor	Summing circuit	Buffer amplifier	Function generator	Power/flow comparator bistable
Functions performed in software	None									
Radiation	~ 4 x 10^4 rad over 20 years				<4 x 10^2 rad over 40 year plant life					
Ambient temperature	Average temperature in containment:~120 deg.F. Average transmitter operating limits: -40° to 240° F		60° to 130° F		- 60°- 80° F in control room.					
EMI/RFI	Nuclear qualified transmitters typically operate normally around sources of radio frequency from ~30 MHz to 500MHz and field intensity of 20 V/m.				EMI/RFI susceptibility tests are generally addressed on an individual equipment basis as necessary, such as demonstrating physical independence of Class 1E and non-Class 1E circuitry.					
Interfaces	Reactor coolant piping, junction boxes, seals, 110 Vac and 120 Vdc power supplies, inverters, interlocks, and bypass modules.									
Signal type	Pressure to current transduction (4 - 20mA current loop.				±10 Vdc					
Stressors	Temperature, radiation, moisture, maintenance & installation handling, environmental cycles.				Maintenance/testing cycles, elevated temperatures inside cabinet housing the electronic modules/components, electromagnetic interference.					
Materials	CABLE MATERIALS: *Reactor building instruments:* **Conductor:** 16 AWG copper conductor **Insulation:** Cross linked polyethylene* **Sheath:** Neoprene* **Outer Jacket:** Galvanized steel				Several types of transmitters are used. The following is representative: MATERIALS IN CAPACITANCE TYPE PRESSURE TRANSDUCERS:[a] **Housing:** Aluminum with epoxy polyester paint or 316 stainless steel. **Fill fluid:** Silicon oil. **Isolation diaphragm:** 316 stainless steel. **Housing seal:** Ethylene propylene.* **Electronic components:** Seals and insulating materials used on electronic components.* **Circuit boards:** Epoxy glass laminate.*			Seals and insulating materials used on electronic components, encapsulating materials for electronic components, and solder joints, are all subject to aging degradation.		

[a]Materials subject to aging degradation are representative of other transmitter types.

*Materials subject to aging degradation.

Fig. 1. Environmental and aging data template for coolant flow string in an analog protection channel (after ref. 3).



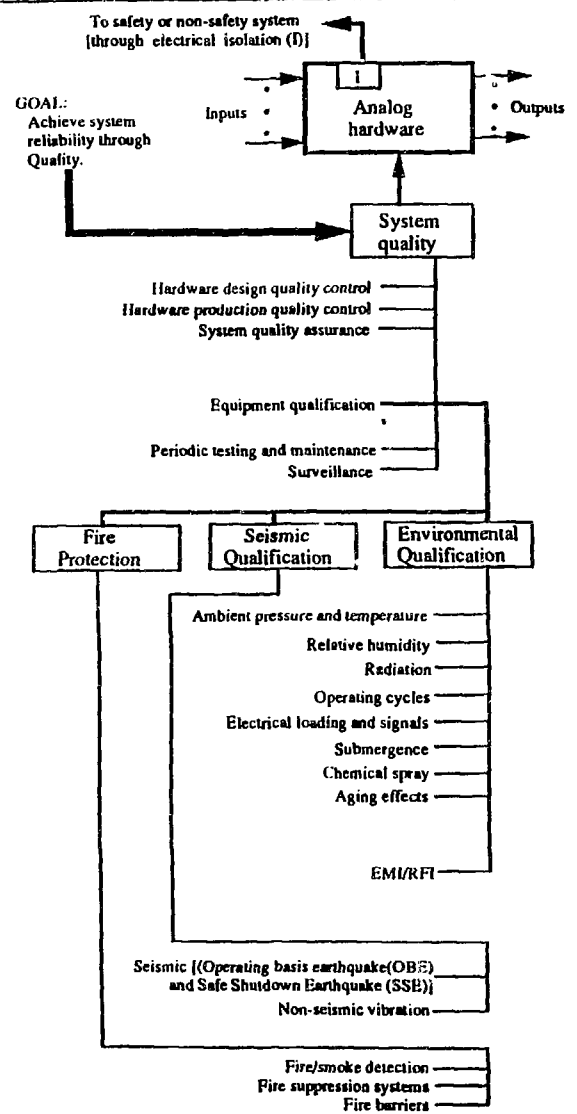
	Transmitters	Penetration room and cables. (Transmitters are hardwired to plant protection system cabinet).	Bistable trip processors generate trips based on the digitized input value exceeding a digitized setpoint	Processors evaluate the local coincidence logic based on the state of the four *like* trip signals and respective bypasses.	Switchgear
Functions performed in software	None		Multiplexer scanning, sample-and-hold functions, digital data acquisition. Channel trip calculations. Process signals provided to the BTP through conventional (analog) signal conditioning equipment.		None
Radiation	< 3 x 10^6 rads gamma (60 yr total dose).	Total integrated dose over 60 yr: <= 10^3 rads gamma.			
Ambient temperature	60° - 110° F Average transmitter operating limits: -40° to 240° F	~77° F ambient in battery room. Design limits for instrumentation: (Not Available)			
EMI/RFI	Operate normally around sources of radio frequency from ~30 MHz to 500 MHz and field intensity of 20 V/m	Mil Standard 462 is used for EMI testing. Particular tests used are CS01, CS02, CS06, RS03, and RS04.			
Interfaces	Reactor coolant piping, junction boxes, seals, 110 Vac and 120 Vdc power supplies, inverters, interlocks, and bypass modules.				
Stressors	Temperature, radiation, moisture, vibration, maintenance & installation handling, environmental cycles	Maintenance/testing cycles, elevated temperatures inside cabinet, electromagnetic interference. Smoke can adversely affect electronic equipment far removed from the source of the smoke or fire.			
Channel independence	[a]Where control and protection systems have identical sensor input requirements, redundant Class 1E sensors that are used independently by each channel of the protection system may in some cases also be used by the control system. In such cases fiber optic (or conventional electrical isolation devices) are used to ensure electrical independence. Separate processors are used for performing trip functions and communication functions.				Switchgear breakers are located in the electrical equipment rooms which are geographically separated from each other.
Materials	Transmitters will be identical to those found in present-day power plants. MATERIALS IN CAPACITANCE TYPE PRESSURE TRANSDUCERS[a]: **Housing:** Aluminum with epoxy polyester paint or 316 stainless steel. **Fill fluid:** Silicon oil. **Isolation diaphragm:** 316 stainless steel. **Housing seal:** Ethylene propylene.[b] **Electronic components:** Seals and insulating materials used on electronic components.[b] Circuit boards: Epoxy glass laminate.[b]		Optical fibers will be used for interchannel communication. The following specifications are typical of type(s) to be used: FIBER MATERIAL: Silicon dioxide (pure and doped). SECONDARY BUFFER: polyamide or acrylic. STRENGTH MEMBER: Aramid yarn or kevlar. OUTER JACKET: Flame retardant chlorinated polyethylene. FLAMMABILITY: Tested to IEEE 383-1974 OPERATING LIMITS: -20° C to 80° C (operating) 0 to 100% (relative humidity).		
	MATERIALS SUBJECT TO AGING DEGRADATION IN CABLES: Insulation (cross linked polyethylene). Sheath (Neoprene). Outer jacket (Galvanized steel).		Seals and insulating materials used on electronic components, encapsulating materials for electronic components, and solder joints, are all subject to aging degradation.		

[a]Materials subject to aging degradation are representative of other transmitter types.

[b]Materials subject to aging degradation.

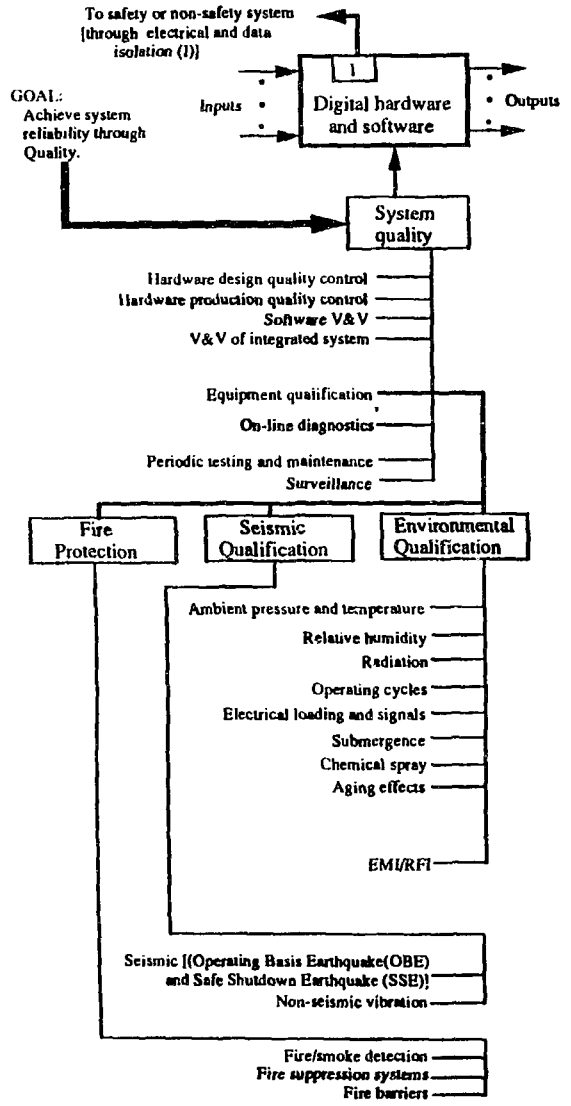
F.O.: Isolation via optical fiber.
RPS: Reactor protection system.
NA: Not available

Fig. 2. Environmental and aging data template for the protection channel of a generic ALWR.



CODES AND STANDARDS	COMMENTS
	Diagram represents generalized safety I&C system consisting of analog and electromechanical components. Interfaces to other safety systems or non-safety systems typically employ electrical isolation.
ASME NQA-1-1989, "Quality Assurance Program Requirements for Nuclear Facilities." IEEE Std 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems."	
IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."	
IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety System Equipment Used In Nuclear Power Generating Stations." IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.89, "Environmental Qualification of certain Electric Equipment Important to Safety for Nuclear Power Plants."	EMI testing is typically addressed on an individual equipment basis, as necessary.
IEEE Std 1050-1989, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations." MIL-STD 461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of EMI." MIL-STD-462, "Measurement of Electromagnetic Interference Characteristics."	Other standards such as SAMA PMG 33.1, ANSI/IEEE C62.43, and IEEE Std 472, are used.
IEEE Std 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.100, "Seismic Qualification of Electrical Equipment for Nuclear Power Plants."	
10CFR50, App. A; 10CFR50.48; 10CFR50, App. R. IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." Regulatory Guide 1.75, "Physical Independence of Electric Systems."	General Design Criterion 3 of 10CFR50, Appendix A, requires systems important to safety to be designed to minimize the probability and effects of fires and explosions. The specific requirements for fire protection is given in Appendix R.

Fig. 3. Qualification procedure for present-day (analog) safety system .



CODES AND STANDARDS	COMMENTS
	Diagram represents generalized, microprocessor-based safety I&C system. Interfaces to other safety systems or non-safety systems are typically by fiber optic links. In a microprocessor-based safety system, the concept of data isolation should also be considered in addition to electrical isolation. That is, there should be *data isolation between the safety software* and the communication software. Failure of the communication software should have no effect on the protection system's ability to perform its safety function.
ASME NQA-1-1989, "Quality Assurance Program Requirements for Nuclear Facilities." IEEE Std 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." ANSI/IEEE-ANS 7-4.3.2-1982, "Application Criteria for Digital Computers in Safety Systems of Nuclear Power Facilities." Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Regulatory Guide 1.152, "Criteria for Programmable Digital Computer Software *in Safety-Related Systems* of Nuclear Power Plants."	ANS/IEEE-7-4.3.2 - 1982 is inadequate in addressing issues relating to microprocessor-based I&C. These issues are being addressed *in the next revision* of IEEE 7-4.3.2.
IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."	On-line diagnostics methods can reduce stress on (digital) safety system I&C by *reducing the number* of periodic maintenance schedules required. This advantage could be reflected in current periodic maintenance requirements.
IEEE Std 627-1980, "IEEE Standard for Design Qualification of Safety System Equipment Used In Nuclear Power Generating Stations." IEEE Std 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.89, "Environmental Qualification of certain Electric Equipment Important to Safety for Nuclear Power Plants." Regulatory Guide 1.100, "Seismic Qualification of Electrical Equipment for Nuclear Power Plants."	EMI testing is typically not *included in the* environmental qualification process. It is addressed on an individual equipment basis, as necessary. However, the unpredictable failure modes of *microprocessor-based* systems require all (digital) safety I&C to be *environmentally* qualified against EMI/RFI.
IEEE Std 1050-1989, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations." MIL-STD 461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of EMI." MIL-STD-462, "Measurement of Electromagnetic Interference Characteristics."	Other standards such as SAMA PMG 33.1, ANSI/IEEE C62.43, and IEEE Std 472, are used. However, specific criteria for EMI/RFI qualification for the nuclear power industry is lacking.
IEEE Std 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations." Regulatory Guide 1.100, "Seismic Qualification of Electrical Equipment for Nuclear Power Plants."	
10CFR50, App. A; 10CFR50.48 IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." Regulatory Guide 1.75, "Physical Independence of Electric Systems."	Fire and its effects (smoke, heat, ignition explosions, toxic gases) on safety-related equipment is a fire protection concern and not necessarily an environmental qualification issue.

Fig. 4. Proposed methodology for qualification of digital safety system .