ABB

ABB COMBUSTION ENGINEERING

January 31, 1994
LD-94-007

Mr. Douglas Coe
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
7920 Norfolk Avenue
Bethesda, MD 20814

Subject: ABB-CE Responses to ACRS Questions on System 80+™

Dear Sirs:

This letter provides responses to questions (Enclosure) raised by various members of the Advisory Committee on Reactor Safeguards (ACRS) ABB-CE Standard Plant Designs Subcommittee at the meeting held on December 8, 1993. I believe that the attached responses will clarify the issues raised by members of the Subcommittee.

If I can be of further assistance regarding these matters, please do not hesitate to call me, or Mr. Stan Ritterbusch of my staff at (203) 285-5206.

Very truly yours,

COMBUSTION ENGINEERING, INC.

for C. B. Brinkman, Acting Director
Nuclear Systems Licensing

Enclosures: As stated

cc: T. Wambach (NRC)

Enclosure to LD-94-007

ABB Combustion Engineering

System 80+™ Standard Plant Design

Responses to ACRS ABB-CE Standard Plant Designs Subcommittee Questions

(December 8, 1993 meeting)

Responses to ACRS ABB-CE Standard Plant Designs Subcommittee Questions

(December 8, 1993 meeting)

Question 931208-01:

We understand that CRT touch-screens utilizing infrared sensors are used for component actuation control in the main control room, remote shutdown room, and instrumentation and control equipment room. What is the vulnerability of these screens for causing spurious component actuations in a smoke, fire, or high air temperature environment?

Response:

First there are two points of clarification that need to be addressed:

1) The target hardware CRT touch screens do not use infrared sensors but rather use surface acoustic wave technology which relies on finger pressure.

2) The CRT touch screens are not used for component actuation.

The target hardware electroluminescent displays (ELDs) and the associated infrared touch screens located on the desk section of the control panels are used for component actuation. The ELDs have no required qualification for smoke or fire since the geographical separation of systems and associated fire protection boundaries limits the effects of smoke and fire to single channel failures or to one control room, main or remote.

Although there is no specific qualification requirement for smoke or fire, the ELDs do have features that minimize the potential for any adverse effects from these hazards. The ELDs have an operating temperature range of 0 to 55 degrees Centigrade and they have error checking software. The signal received by each infrared sensor must be an AC signal, at a specific frequency thus eliminating errors due to sun/bright light, flame, and high ambient air temperatures. Although there is no evidence that smoke can break the infrared beam, should this occur it is most likely that multiple beams will be broken. The touch sensing software will not respond if multiple beams are broken. In the unlikely event that the beams are broken correctly, the software then looks for the beam to reactivate. This accommodates the normal expected mode of operation which is activate on release (finger removal), not on make. Therefore, for any response, the smoke which remarkably broke only a single beam would then have to clear to cause any screen response.

However, should these two precautions fail and a break event occurs correctly the most likely response is simply a page change on the screen, not a component state change. This is because all component controls are on level 2 and 3 pages; administrative controls will direct the operator to return to the level 1 page (by touching clear) after all control actions are

completed. Should the smoke initiate a change to a control page, the smoke would again have to break and release a single beam for the control action to occur.

In summary, smoke and fire are accommodated through the plant design, not through equipment qualification. In addition, the equipment has robust design features that would require smoke to break and release single infrared beams on two consecutive display screens to cause any adverse control actions.

Question 931208-02:

How well does the System 80+ design incorporate lessons-learned as identified in the INPO operating experience study for advanced plant designs (INPO #93-004/005)? What level of review has ABB-CE given to this document?

Response:

A summary of the approach to incorporation of operating experience into the System 80+ design is provided on the first page of Table 1.2-1 of CESSAR-DC. Basically, we have relied on the experience of the organizations on the System 80+ design team and the experience reflected in the ALWR Utility Requirements Document published by EPRI.

The INPO report referenced in the above question was not drafted until late in the System 80+ design process and, therefore, it was not reviewed in detail during the System 80+ design process. ABB-CE's review of an early draft of the INPO report indicated that all significant experience summarized therein had been addressed.

An extensive operating experience review effort was conducted, independently of the INPO report, for the Nuplex 80+ Advanced Control Complex to resolve past problems. This effort is described in Section 18.4.3 of CESSAR-DC and is documented in full in the Operating Experience Review (OER) for the System 80+ MMI Design. The OER activities included reviewing the INPO Significant Operating Events Review (SOER) data. Selected SOER entries with Man-machine implications related to Nuplex 80+ were specifically addressed.

Question 931208-03:

What is the data storage capability of the I&C system for maintaining a history of operating parameters? Once these operating parameters are stored on optical disk, how long are they retained?

Response:

The Data Processing System (DPS) stores up to 750 analog inputs and 1000 contact inputs at

1) high resolution which stores data every 5 seconds and,

2) low resolution which stores data every 10 minutes.

The data is temporarily stored on magnetic disk for 12 hours and may be transferred to an optical disk for permanent storage in one of two ways:

1) During normal operations the temporarily stored data may be transferred to the optical disk at the option of the operator. The DPS (via an operator aid message), alerts the operator as to when he may initiate the transfer. Normally, the operator will have a 12 hour time interval to request the transfer to optical storage for data which was recorded during the previous 12 hour period.

2) During a plant trip, the data storage software will automatically store to optical disk 2 hours of pre-trip data and 10 hours of post trip data, both at high resolution intervals (5 seconds). Thereafter, data storage to optical disk is again at the option of the operator.

Based on 1993 one gigabyte optical disk technology, the data storage capacity of the I&C system for maintaining a history of operating parameters is 16 days for 2000 points at a 5 second interval and 1920 days for 2000 points at a 10 minute interval. Based on industry information, the projected rate of increase in optical storage capacity, for a given physical size disk, is estimated to double over each 2-3 year period during this decade (1991-2000). This will offer significant increases in permanent data archival capacity in the future to multi-gigabyte levels.

The retention time of the optical disks is a utility function; there is no technical limit

Question 931208-04:

What is the expected ambient temperature effect due to heat loads in rooms where remote multiplexing units are located upon loss of all HVAC to these rooms, and what is the impact of this on multiplexor operation?

Response:

The loss of all HVAC is considered to be highly unlikely as redundant Seismic Category 1 HVAC is provided for essential systems (Refer to CESSAR-DC Section 9.4).

Since the HVAC systems are redundant, there is no requirement for environmental qualification with loss of HVAC.

In the unlikely event of complete failure of redundant HVAC in essential system areas, the ambient temperature may rapidly exceed the qualified temperature of the multiplexor. Under this condition, operability of the multiplexor cannot be assured. However, multiplexor cabinets are equipped with high temperature alarms to annunciate this condition, allowing operators to take the equipment out of service.

Upon restoration of HVAC and return of ambient temperature to the qualified range, the multiplexor can be restored to operation.

Question 931208-05:

Presentation slide SAB:KS2 5/4/93 titled "Nuplex 80+ Software Reliability" lists nine defense-in-depth elements. For each element please provide documentation (or references to documents already provided to ACRS) describing how the element is achieved, including any criteria used.

Response:

Software Design Process Element

The software design process is documented in "Nuplex 80+ Software Program Manual," NPX80-SQP-00101.0, which is referenced in Sections 7.1.2.32 and 7.2.1.1.2.5 of CESSAR-DC. This manual encompasses the entire software life cycle from planning through retirement.

Additional software design process requirements apply to the Core Protection Calculator software design. These requirements are identified in CESSAR-DC Section 7.2.1.1.2.5.

Commercial Dedication Process Element

Requirements for commercial dedication of software and computer hardware are contained in, NPX80-QPS-0401.1, "Requirements for the Supply of Commercial Digital Computer Hardware and Software Components to be Used in Nuplex 80+ Safety Systems". This docketed document is referenced in the Nuplex 80+ Software Program Manual and ABB-CE quality assurance program documents.

Diversity Element

Diversity is addressed in CESSAR-DC Sections 7.1.1.9, 7.2.1.1.8, 7.3.1.1.6, 7.5.2.5.2 and is reflected in the CESSAR-DC descriptions of the Discrete Indication and Alarm System (Section 7.7.1.4) and Data Processing System (Section 7.7.1.7). Report ALWR-IC-DCTR-31, transmitted via LD-92-105, provides a comprehensive "Evaluation of Defense-In-Depth and Diversity in the ABB-CE Nuplex 80+ Advanced Control Complex for the System 80+ Standard Design." CESSAR-DC Appendix 7A, which provides a "Common Mode Failure Evaluation for Limiting Fault Events," also provides an overview of the diversity issue.

Simple Deterministic Design Element

This topic is addressed in CESSAR-DC Section 7.3.1.1.6.

Field Proven Executive Software Element

This topic is addressed in CESSAR-DC Sections 7.2.1.1.2.6.2 and 7.3.1.1.6, and in NPX80-QPS-0401.1, "Requirements for Supply of the Commercial Digital Computer Hardware and Software Components Used in Nuplex 80+ Safety Systems."

Segmentation Element

Safety system segmentation is addressed in CESSAR-DC Sections 7.2.1.1.2.6 and 7.3.1.1.6. DIAS segmentation is addressed in Section 7.7.1.4.1.

Sabotage Protection Element

Sabotage protection is addressed in CESSAR-DC Section 7.1.2.16 and Appendix 13A, Section 8. Testing of the Plant Protection System functionality is addressed in Sections 7.1.2.17 and 7.2.1.1.9.

Maintainability Element

Software maintainability requirements are documented in the Nuplex 80+ Software Program Manual, NPX80-SQP-0101.0, particularly with regard to Configuration Management (Section 5.0) and Documentation (Section 7.0). Section 3.4.2.1 requires the development of coding standards. Section 4.9 addresses operation and maintenance V&V. Section 6.0 addresses the software operation and maintenance plan.

Experience Element

ABB-CE experience in designing safety-related software is described in CESSAR-DC Section 7.1.1.7. Section 7.7.1.2 provides a comparison of the Nuplex 80+ and reference plant control systems.

Question 931208-06:

What is meant by "software failure?" Where is it defined?

Response:

The topic of software failures was discussed at the December 8, 1993 subcommittee meeting in the context of common-mode failures.

Software failure is specifically addressed in ABB/CENP's evaluation of the capability of the System 80+ design to cope with a postulated common-mode-failure. In performing the evaluation, all systems using software which is not diverse from the protective system software for which the fault is postulated, are assumed to become unavailable to perform either control or monitoring functions. The assumed result of this fault is defined in Section 1.1 of LD-92-105, "Evaluation of Defense-in-Depth and Diversity in the ABB-CE Nuplex 80+ Advanced Control Complex for the System 80+ Standard Design," as follows:

> The evaluation assumes that a pre-existing common-mode-failure prevents all automatic responses of both the PPS and the ESF-CCS. In addition, subsequent manual operation of the protection system via the ESF-CCS interface is also precluded.
>
> The evaluation also assumes the Discrete Indication and Alarm System Channel N (DIAS-N) could be generating erroneous displays/alarms and, therefore, is not valid for use by the operator in diagnosing and following the event.

The specific safety system actuations which are assumed to fail and specific system functions which remain available are identified in Section 2 of LD-92-105 and Section 2 of Appendix 7A to CESSAR-DC.

Question 931208-07:

Regarding section 4.6.4 of the Software Program Manual, where is "system testing" defined, as applied to integrated hardware/software testing, and to what extent is it performed?"

Response:

The Software Program Manual deals with integrated hardware/software testing throughout section 4, Software Verification & Validation Plan. Section 4.1.2 states that validation *"provides the overall assurance that the capabilities specified in the requirements are implemented in the hardware and software, and that the system is properly integrated."*

Section 4.8 provides general requirements for system validation testing for which, as section 4.8.1 states, *"the fully integrated system with the actual system hardware and software is required."* Requirements include:

- Black box testing of functional operation, performance, and interfaces;
- Testing of abnormal conditions consistent with design requirements;
- Transient condition testing
- Testing of system tolerance to failure
- Testing of built-in testing capabilities
- Simulator testing

In addition to system validation testing, Section 4.4.4 and 4.4.4.1 provide requirements for verifying that the specification of the integrated hardware and software meets system requirements, including evaluations of:

- Design feasibility, testability, maintainability;
- Adequacy of functional features for meeting system objectives;
- Adequacy of system operation conformance with performance requirements;
- Adequacy of interfaces with, software, internal hardware, external hardware, user.

The detailed requirements for integrated hardware/software testing vary for different Nuplex 80+ systems. Therefore, these requirements are to be described in system specific test plans, which will be developed for each system starting in the requirements phase. Section 3.2.2.2 identifies information to be included in the system specific test plan. These plans define the tests required to meet the Software Program Manual requirements.

The simulation of process noise was also questioned at the December 8, 1993 meeting. According to section 4.6.4(9), simulator testing with input signal noise is not performed during system testing. Other sections of the Software Program Manual did not clearly identify when testing for input signal noise would be performed.

The Software Program Manual was intended to state:

> *Testing for the effects of input signal noise is performed during the phase of testing most likely to detect related defects. The system specific test plan will identify when this type of testing is to be performed. The scope of test for the effects of input signal noise depends on the design of the specific system and is also documented in the test plan. For example, some systems have no time dependent behavior, and the equivalent of noise testing can be accomplished by simulating inputs over their normal and abnormal ranges. For some other systems where noise testing is determined to be necessary, the preparer of the test plan must consider the various ways this can be accomplished, and the characteristics required for the noise. This determination would depend on the design of the system and its susceptibility to input signal noise.*

Since the concept in the above paragraph is not clearly stated in the Software Program Manual, the above paragraph will be added to the end of section 4.6.4(10). Section 4.6.4(9) will be clarified as follows:

> *The input signals used for the system validation test are simulated. If the system specific test plan requires system testing with input signal noise, the validation tests shall be run with and without input signal noise, since noise may obscure some defects that may be identified with simulator testing.*

Question 931208-08:

To what extent does the PRA treat the possibility of a seismic event causing spurious actuation of fire protection water spray equipment in both divisions (with an assumed loss of the CTG due to the seismic event)?

Response:

The spurious actuation of fire protection system water spray equipment in both divisions was not explicitly modeled in the System 80+ Seismic Margins Assessment (SMA) in section 19.7.5 of CESSAR-DC.

Based on the preliminary deterministic Fire Hazards Assessment for System 80+, automatic water spray systems will be provided in each Diesel Generator (DG) room and each turbine driven Emergency Feedwater (EFW) pump room. As the detailed Fire Hazards Assessment evolves, automatic sprinkler systems may be added to other rooms.

These automatic sprinkler systems are dry header systems with preaction valves. Upon detecting a fire, the fire detection system in the appropriate room would send a signal to the preaction valve to open to fill the sprinkler header. The sprinkler heads have heat sensitive elements, such as a frangible link, that would open when the temperature in the room reaches the appropriate point. When the heat sensitive element opens, the sprinkler head would begin spraying down the surrounding area. The preaction valves are solenoid operated valves that fail as is on loss of power. The seismic category 1 portion of the automatic sprinkler system consists of the standpipe from the water supply to the seismic category 1 isolation valves just upstream of the preaction valves, an 18,000 gallon fire water tank inside the nuclear annex, and a seismic category 1 fire pump that can deliver 150 gpm to the standpipe downstream of the seismic category 1 check valves. The dry portion of the system is not seismic category 1 but welded pipe is used through out and is considered to be seismically rugged. The preaction valve are not seismic category 1. The fire detectors are not seismic category 1.

There is no equipment in the turbine drive EFW pump room that would be directly affected by the spray from the fire water sprinklers. If, however, the room is flooded by the spray, the turbine-driven EFW pump could fail. It is assumed that, consistent with common practice, the turbine driven pumps are mounted on six inch high pads. Thus, the rooms would have to be flooded to a depth greater than six inches to affect the pumps.

Likewise for the DG rooms, the electrical and electronic equipment in the rooms are drip proof and/or protected from the spray such that the actuation of the spray would not directly result in failure of the equipment. If, however, the electrical or electronic equipment is submerged, it would fail. The base elevation in the DG rooms is elevation 50. All of the electrical and electronic equipment in the DG rooms are on grating platforms at elevation 70. The DG support equipment is on an elevated platform at elevation 54. The DGs are assumed to be mounted on platforms at least six inches high, consistent with common practice. It is

also assumed that the DGs would have to be submerged to some reasonable depth before they would fail.

A scenario can be postulated in which a seismic event occurs and the non-seismic fire detectors fail such that an actuation signal is generated and causes a spurious actuation of the automatic fire sprinkler systems. (Under the "One Fail - All Fail" assumption, all automatic sprinkler systems are assumed to be spuriously actuated if one is spuriously actuated.) This spurious actuation signal would open the preaction valves so that the sprinkler system headers will be filled with water. However, the sprinklers would not begin sprinkling the rooms unless they also failed due to the seismic event. As previously stated, the sprinkler headers use welded piping throughout and are considered to be seismically rugged. Historically welded piping systems have performed very well during seismic events and have failed only as the result of the failure of multiple supports. Thus, the sprinkler header piping is not expected to fail except at high accelerations. The sprinkler heads are also considered to be seismically robust and should not fail as long as they are laterally restrained so that they will not impact solid objects or structures to their sides during the seismic event. These sprinkler heads are tested per UL199. UL199 specifies that the sprinkler heads are tested at frequencies from 18 to 35 hertz with an amplitude of 0.4 inches for 120 hours. The test frequencies and amplitudes result in test acceleration of up to about 13g. Thus, even with a spurious actuation signal, no complete spurious actuation of the automatic sprinkler systems is expected.

If the seismic event is postulated to cause a failure of the sprinkler heads such that they fail open, the rooms protected by the sprinkler systems will be sprayed down. As stated above, the total fire water inventory in the seismic category 1 tank is 18,000 gallons. This is 2400 ft^3. The DG rooms are approximately 40 feet by 120 feet and the turbine driven EFW pump rooms are approximately 20 feet by 40 feet. Thus, the total floor area in the four rooms covered by the automatic sprinkler systems is 11,200 ft^2. If it is conservatively assumed that half of the floor space is occupied by equipment, the available inventory in the seismic category 1 fire water tank would flood the remaining 5600 ft^2 of floor space to a depth of only 5.2 inches. (NOTE: Operation of the floor drains in the DG rooms was not credited.) Thus, even if the sprays were fully actuated by the seismic event, the equipment in the rooms covered by the automatic sprinkler systems would not be affected.

Question 931208-09:

Which busses have overvoltage protection devices and what actions does each device initiate? Do each of the two switchyards have primary and secondary breakers, or is there one set of breakers for both switchyards?

Response:

Overvoltage protection on the Main Power System Bus is provided as follows:

1. Generator volts/hertz - Device 24

This relay protects against voltage regulator malfunction by detecting an excessive ratio of generator voltage to frequency, where frequency is 60 hertz and voltage 120V from the secondary of voltage transformers.

ACTION: Actuate lockout to trip generator circuit breaker and exciter.

2. Volts/hertz relay in regulator protection package

This relay operates in the same manner as Device 24 described above.

3. Regulator volts/hertz limiter

Each of the two switchyards has one power circuit breaker which connects the station with its respective transmission line. Primary and secondary relaying is provided to protect each line. Sensing for the primary and secondary relays is from independent current transformers. Each circuit breaker has two trip coils which are powered by separate DC power sources.

Question 931208-10:

What is the basis for the test requirement specified in ITAAC test #9.(b) on Table 2.6.1-1?

Response:

The basis for the test requirement specified in ITAAC test #9.b is contained in Appendix A to Regulatory Guide 1.68, "Initial Test Programs for Water-Cooled Nuclear Power Plants", Rev 2 (8/78), which requires that emergency loads be tested to demonstrate the capability to start and operate with the maximum and minimum design voltage available. Regulatory Guide 1.68 also states in the same passage for clarification: "To the extent practical, the testing of emergency or vital loads should be conducted for a sufficient period of time to provide assurance that equilibrium conditions are attained." For the System 80+ design, testing as described above will be performed for the Class 1E busses by adjusting the voltage levels of the Emergency Diesel Generators to the test levels described in test #9.b (+/- 10% bus nominal voltage). Performance of this pre-operational test will also involve temporary adjustments of undervoltage relay setpoints to defeat automatic actions by the EDGs and electrical power distribution system. Once test voltage levels are established, equipment powered from the safety busses will be operated to verify acceptable operation for degraded and overvoltage conditions.

Question 931208-11:

For those plant components identified in the SSAR or Design Description which are not expected to be replaced during a 60 year design life, how will it be assured that such components will be designed to last 60 years? Will ABB-CE provide any design guidance for when to replace components that are not expected to last 60 years?

For NRC STAFF: What is the staff's position on the degree to which ABB-CE needs to specify design guidance in both of the above cases?

Response:

The 60-year plant design life for System 80+ as been accomplished through a combination of design, material selection, design analysis, procurement requirements, pre-/inservice inspection, maintenance, and replacement activities for individual components and systems. These issues are addressed on CESSAR-DC. Major NSSS component design life (e.g., the reactor vessel) is confirmed through analysis and monitored throughout the station life as described in CESSAR-DC. For example, CESSAR-DC Section 3.9.1.1 describes the approach to fatigue analysis of the NSSS based on the transients expected through a 60-year plant life. For the reactor vessel, improved material specifications are stated in Section 5.2.3.2 and the neutron irradiation analysis for 60 years is documented in Section 5.3.2.1. Major Nuclear Steam Supply System (NSSS) and turbine generator (T-G) components are not expected to be replaced during the 60-year design life of the System 80+ plant. The design and inspection requirements for the turbine are reviewed in CESSAR-DC Sections 10.2.3 and 10.2.5.

For components that may be replaced during the 60-year design life, the design life is determined during the actual design and procurement process where the objective is to obtain the longest design life obtainable for a given component, consistent with life-cycle cost considerations. For those components where 60-year life is not obtained, replacement criteria will be included in the plant's equipment manuals and, as part of maintenance and surveillance programs as described in Section 3.11.2.1 and summarized in Section 3.9.6 and 6.6.

Question 931208-12:

What role does the Alternate AC Source (Combustion Turbine) have in meeting the requirements of the Station Blackout Rule? Is this described in the Design Requirements?

Response:

The Alternate AC Source (Combustion Turbine) is the "Alternate AC Source" described in the Station Blackout Rule, Regulatory Guide 1.155. The AAC provides a source of AC power which is diverse from other sources of AC power (e.g., offsite power, Class 1E diesel generators) which are assumed to be unavailable for blackout coping capability. This diverse source of AC power meets all requirements of RG 1.155. CESSAR-DC contains sufficient description of the design bases and capabilities of the AAC, as well as its regulatory compliance with RG 1.155. The role of the AAC is described in the ITAAC Tier 1 Design Description.

Question 931208-13:

Provide a drawing(s) depicting location of major I&C equipment outside the MCR/RSP.

Response:

Drawings showing the location of all major I&C and electrical equipment are provided in CESSAR-DC. The Nuclear Island general arrangement drawings provided in Figures 1.2-2 through 1.2-12 show locations of all major I&C and electrical equipment. The plan views identify I&C and electrical equipment with a unique number. The name associated with each number is given in the upper right of each plan view drawing under the heading "ELECTRICAL EQUIPMENT".