ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
UNITED STATES ATOMIC ENERGY COMMISSION
WASHINGTON, D.C. 20545

November 8, 1974

L. M. Muntzing
Director of Regulation

SYSTEMS ANALYSIS OF ENGINEERED SAFETY SYSTEMS

With the current effort to standardize the design of certain types of nuclear power plants, the Committee believes that attention to the evaluation of safety systems and associated equipment from a multi-disciplinary point of view to identify potentially undesirable interactions between systems becomes increasingly important. The attached illustrative examples represents an initial and not necessarily complete listing of some problem areas.

The Committee would appreciate the Regulatory Staff reviewing these comments and discussing their ideas with an appropriate Subcommittee. Based on these discussions a mutually beneficial procedure for handling such issues may be developed.

W. R. Stratton
Chairman ACRS

Attachment:
List of Illustrative Examples

cc: P. Bender, SEC
E. Case, DL

Illustrative Examples of Questions to be answered by Systems Analysis and Quality Assurance

The following comments and questions are suggested for consideration as additional guidance in the review of Engineered Safety Systems:

1. Comment: Designers and architect-engineers frequently delegate responsibility for systems analyses to teams with functional engineering specialties such as "civil," "electrical," "mechanical," or "nuclear" with the team effort coordinated by managers responsible for controlling costs and avoiding schedule delays. With the same standard design applied to a number of plants, an intensive systems analysis effort which integrates the functional engineering specialties, is feasible. The scope and approach of the related Quality Control/ Quality Assurance effort should be commensurate with the Project Design effort. Consideration should be given to identifiable multi-disciplinary analyses of safety-related systems and associated systems, as part of Quality Control in design, procurement, construction, operation, and maintenance activities.

   General Question:

   What are the respective roles played by Project Design and Quality Assurance/Quality Control in the multi-discipline analyses of safety systems and associated systems?

2. Comment: As an aid in identification, safety related systems and associated equipment may be categorized as follows:

   a) Those systems or items of equipment which must be de-energized on demand (to a zero energy state) with extremely high reliability to:

      (1) Perform a safety function;

      (2) Prevent fire or other damaging consequence.

   b) Those systems which must be capable of long-term active operation to preserve control over radioactive materials (examples are fuel and environmental cooling and lighting and communications services).

   c) Those systems not directly related to a safety function but whose malfunction could have safety consequences because of secondary effects. It should be noted that such systems may not ordinarily be included in the set for which "conditions of design" are defined.

Question: In the design of such systems, is an interdisciplinary systems analysis performed to assure redundancy and separation appropriate to the category of the system? Does it consider all modes of normal operation, operation following any of the design basis events plus additional incidents such as pipe failures, loss of all active inputs to the system, and operation of part of the active components combined with the failure of others (for example, the operation of a large and critical motor in a space where the ventilation has failed)?

3. Comment: In addition to systems and equipment, space allocation and arrangement are crucial to safety. Both Unit and Station systems must be analyzed to assure adequate independence and separation of all vital functions. The analysis should consider the possibility that adverse "feedback" or other effect from one unit may leave other units without adequate redundancy.

   Such an analysis should help to provide a basis for establishing reliability, redundancy, and separation requirements. It should also provide information concerning the degree of separation necessary to protect against mechanical damage, fire or sabotage.

   Questions:

   a) Are design efforts and systems analyses directed to avoid concentration of vulnerability from various causes in one safety class structure, room, or zone?

   b) Are field located and field run equipment and systems examined to see if localized vulnerability has been created?

   c) Is space allocation a conscious responsibility in design?

   d) Are field inspections of space occupied by safety equipment and systems made by the cognizant design engineer to assure non-encroachment?

   e) Do changes in space allocation or arrangement require special approval?

4. Comments: Control systems may require communication lines, (electrical, pneumatic or hydraulic) that traverse significant distances and pass through several compartments.

   Questions:

   a) Is attention given in system design to physical locations of "field-run" impulse or static lines, including lines that provide information regarding ECCS functions, and other electrical-mechanical-hydraulic-pneumatic control systems which perform

safety functions, to assure that an unacceptable interaction between these and other systems is avoided?

b) Is specific attention given to assuring that field location follows that specified in the design?

5) Comments: Electrical systems and equipment should be analyzed to assure that over-current or other fault protection is sufficiently reliable and redundant to assure appropriate limitation of damage potential to other safety systems.

An example is the electrical power supply to primary system pumps. Failure of the circuit breakers could result in damage to the electrical penetrations and loss of containment under post-LOCA conditions.

Questions:

a) Are the circuit breakers for electrical power circuits that pass through containment penetrations set to trip in the event of arcing faults within the penetration?

b) Are such circuits designed with ground fault trips to protect the penetrations?

c) Are ground fault trips provided on all power circuits within the physical safety complex to reduce the fire hazard?

d) Are emergency lighting systems and internal communication systems safety grade?

e) Are control and power cables of widely differing voltages and currents intermixed in cabletrays, raceways, or conduits?

f) Are magnetic forces and molten copper considered in specifying the separation required between cables?

g) Are differences between laboratory test conditions for flame resistant cable insulation, and conditions that could exist in a cable way under faulted conditions, considered in defining separation requirements?

h) In determining the adequacy of separation, is consideration given to "foreign" sources of damage such as vehicle impact, use of welding equipment, explosive gas accumulation, or acts of sabotage?

i) Is fireproof, rather than fire "retardant" insulation required in vital areas? Is potential damage from radiation exposure from nearby components, such as air filters and charcoal adsorption beds, taken into account?

j) Is the timing of loss of offsite power considered in the prediction of the consequences of an accident? (For example, the most disadvantageous time may be just as motor operated valves are about to open or large pumps are almost up to operating speed).

6. Comments: Some ventilation systems may not be given attention as engineered safety features, however, situations may arise in which they can have important effects on safety.

Questions:

a) Are auxiliary systems such as containment or reactor building air cooling systems analyzed to see if their failure can lead to the failure of safety systems?

b) Are dynamic as well as static differential pressures on containment ventilation ducts and isolation dampers considered?

c) Are local effects of flow pressure gradients resulting from pipe ruptures analyzed for phenomena such as the collapsing of ventilation ducts, which could result in closing vent areas?

d) In evaluating the adequacy of the protection provided to operators in the control room following a LOCA, is consideration given to the possibility that a ventilation (or large electrical) penetration of the containment has failed and is leaking the containment atmosphere into the adjacent space?

7. Comments: Experience has indicated that fluid systems deserve special attention in both static and dynamic situations. Particular attention should be given to stresses resulting from valve action, pump starts, and water slugs, including backflow and check valve action, as well as flow action under severe accident conditions or fault modes.

Questions:

a) Is consideration given to the effect of fluid system dynamics on mechanical stresses in components and equipment?

b) Are the consequences of the failure of check valves to close properly in various fluid systems examined for normal and faulted conditions?

c) Is evaluation made of the possibility and effects of crushing and/or rupturing one group of control rod drive hydraulic lines during a LOCA? Are combinations of ruptured and crushed lines also considered?

d) In PWRs, are the consequences of multiple steam generator blowdown considered?

e) In the evaluation of a system's ability to perform its required service is consideration given to potential flooding effects resulting from roof drain obstruction (potential roof collapse), rupture of non-Class I tankage, continued operation of a leaking system, or reverse flow through normal or ruptured pipe that could be siphoning liquid from some storage source?

f) What controls are placed on the use of "plaster" or glass wool type thermal insulation within containment, that could foul or possibly cause failure of ECC systems?

g) Is an analysis performed to determine when pool boiling would occur, if during refueling (with the reactor vessel head removed) both of the two canal cooling systems become disabled?

What would be its consequences? How long would the operators have to restore cooling?

8. Comments: Fires may have unusual consequences in reactor systems and deserve special attention.

Questions:

a) How are fires analyzed for potential effects on safety?

b) Are the storage of flammable materials in vital spaces and the passage of flammable gases or liquids through vital spaces prohibited?

c) Are safety enclosures, including doors, for diesel generators designed to withstand a diesel runaway, fire, or combined fire-explosion?

d) Does analysis of electrically generated fires consider the following for each power circuit:

1) The change of a circuit short or overload in a circuit within a safety class structure?

2) The chance of a branch overload or short circuit followed by failure to clear the fault?

3) The chance of fire from circuit overheating at or below normal current load?

4) The possibility that fire will propagate to:

a) Disable one vital electrical division if the circuit is not already in a vital division?

b) Disable two or more vital divisions in a local area where minimum allowable separation is employed?

5) The potential consequences of combustion of fumes from fire in confined spaces?

9. Comments: After careful analysis and design it is essential that operation or tests in the field follow the resulting specifications.

Questions:

a) Does environmental qualification allow for or test for the possible lack of discipline in field installation which may result in a field installation that is significantly different from the qualification test setup? Do the qualification tests represent a condition of long term (multi-year) normal operation followed by short term, very severe environmental conditions?

b) Are special instructions for operation and maintenance identified after being developed by a disciplined systems analysis? Examples of such instructions are "use no flame", "no traffic area", "do not operate if ...," "no welding without prior approval of fire protection personnel", "do not use mercury-containing instruments", "do not overtorque", "no substitutes for this material".