THE 4TH INTERNATIONAL TOPICAL MEETING ON
NUCLEAR THERMAL HYDRAULICS, OPERATIONS AND SAFETY
April 6-8, 1994, Taipei, Taiwan

TRANSIENT AND ACCIDENT ANALYSES TOPICAL DESIGN BASIS DOCUMENTS

Larry Chi
General Electric
Technical Services Company
Tokyo, Japan

Eugene Eckert and Brit Grim
General Electric Nuclear Energy
San Jose, California, USA

INTRODUCTION

The designers and operators of nuclear power plants have extensively documented system functions, licensing performance, and operating procedures for all conditions. This paper presents a complementary, systematic approach for the documentation of all requirements that are based on the analysis of operational transients, abnormal transients, accidents, and other events which are included in the design and licensing basis for the plant. Up to now, application of the approach has focused on required mitigation actions (automatic or manual). All mitigation actions are directly identified with all applicable reactor events, as well as the plant-unique systems that work together to perform each function. The approach is also applicable to all operational functions.

The approach makes extensive use of data base methods, thereby providing effective ways to interrogate the information for the varied users of this information. Examples of use include: evaluations of system design changes and equipment modifications, safety evaluations of any plant change (e.g., USNRC 10CFR50.59 review), plant operations (e.g., manual actions during unplanned events), system interactions, classification of safety-related equipment, environmental qualification of equipment, and mitigation requirements for different reactor operating states. This approach has been applied in customized ways to several boiling water reactor (BWR) units, based on the desires and needs of the specific utility.

BACKGROUND

The current documentation pattern for nuclear power plants includes extensive information for licensing submittals and topical safety analysis reports. The licensing analysis focuses on compliance to regulatory requirements, includes evaluations of postulated events of concern for the plant, and summarizes the primary mitigation steps taken for each case.

A recently renewed effort requires US utilities to update plant system requirements in Design Basis Documents (DBDs). System documentation usually provides a specification of all design functions of the system with particular attention to identifying those functions and parameter values which are important to the basic design decisions for the system. The system documentation also lists industry code or hardware requirements that apply to the system, and it usually includes detailed requirements for interfaces with other systems. The system documentation usually includes operational as well as safety functions.

Operational and emergency procedures have been created for BWRs, identifying the best actions to be taken given the plant symptoms displayed to the reactor operator.

All of this documentation is predominantly prepared separately, and it only links the technical requirements together very indirectly.

The primary functions of most safety-related systems are related quite easily to the most obvious licensing or design basis events in which these functions are required. For example, the suppression pool cooling function is clearly required for the mitigation of a Design Basis Accident (i.e., a postulated pipe break accident inside the primary containment), and system documentation is closely coupled to the licensing documentation. However, current documentation does not usually show all mitigation functions required by each licensing (or operational) event, especially those events considered to be non-limiting, or events identified after the initial plant design. The connection to specific events becomes even more difficult when multiple layers of support provided between systems is considered.

The Design Basis Transient and Accident (DBT&A) documentation approach provides a systematic, complete, and useful connection between each system mitigation function and all the postulated events for which credit is taken for the function. This information ensures that all applications of a system function are considered if plant modifications or design changes are being considered. It strongly supports the effort to establish the safety classification of each function of a plant system (and the components involved). It clearly documents shared mitigation roles - either as support provided (e.g., power supply), or shared single-failure-proof mitigation responsibilities (e.g., the Automatic Depressurization System function provides a shared core cooling function with the applicable high pressure coolant supply system). The approach also provides a means to evaluate the role of systems and components for operating conditions other than high power and to identify the impact of unavailability of a system function on continued plant operation. In many ways, this new approach supplements existing documentation and ties together the functional requirements for the plant.

ORGANIZING THE PROCESS

In order for the DBT&A DBD to provide a detailed link from reactor transient and accident event analyses to all the system functions that are required for mitigation, a consistent, systematic process was developed. Several vital elements of information were defined carefully. For example, the normal operating states of the reactor are usually found in the Safety Analysis Report (SAR) or the Technical Specifications for the unit, but concise definition is needed in the DBT&A DBD.

Another basic element is the frequency of occurrence category that applies to each event selected for the DBT&A DBD. A typical set of event groups are:

- Anticipated Operational Occurrences (Moderate frequency events)
- Abnormal Operational Transients (Infrequent events)
- Accidents (Very infrequent events including Design Basis Accidents)
- Other Events (Unique situations such as flood, fire, station blackout, or shutdown from outside the main control room).

The frequency of occurrence categorization is important. Not only are different mitigation performance criteria applied in the analysis depending upon the category of the event, but the results of the DBD can provide important input to the safety classification of the equipment associated with each system function. An example of different performance criteria is the set of criteria in the ASME boiler and vessel code applications associated with different likelihood occurrences (UPSET, EMERGENCY, and FAULTED events). An example of equipment safety classification is the special group of requirements applied to equipment that performs safety functions for the mitigation of a design basis Loss of Coolant Accident (LOCA). The DBT&A DBD can uniquely identify all system mitigation functions for which credit is taken during a LOCA (as well as all other Accident events).

The next element for the creation of a complete set of required mitigation actions is developed by documenting all the safety challenges that may be experienced during the events. It has been useful to define these challenges in terms that are similar to the Safety Analysis Report (SAR) for the plant. For plants in the USA and most other countries, a set of "Unacceptable Results" has been defined for each category of events. Typical Unacceptable Results are:

- Fuel Failure
- Excessive Release of Radioactive Material
- Stresses in Excess of Applicable Criteria

These items are closely linked to the criteria which are used to show acceptable avoidance of each unacceptable result. The criteria are usually associated with regulations that apply to the event category. The DBT&A DBD provides a concise summary of the current regulations and plant commitments related to the mitigation of each transient, accident, or other event that has been postulated during the design and licensing of the plant.

The DBT&A DBD approach identifies all the mitigation actions taken to ensure that each potential Unacceptable Result does not occur. A well defined set of such actions is established. Typical mitigation actions are:

- Initiate scram (trip) of the reactor
- Provide overpressure relief
- Initiate isolation of loss of coolant (e.g., through a pipe break)
- Provide core cooling
- Provide containment cooling
- Provide a controlled environment in the main control room
- Indicate reactor water level outside the control room (for use in shutdown/cooldown from outside)

It should be noted that, as intuitively expected, most of the actions are active mitigation actions, but some will also be passive functions. Many aspects of "boundary" functions (e.g., reactor coolant pressure boundary) are passive, but they are also essential to adequate mitigation of events. Each utility decides to what extent such passive functions are to be included. The output of this process is the set of mitigation actions for all events.

A set of codes is developed for consistent identification of safety action attributes. Some examples of requirements which can be identified are: manual versus automatic actions, active versus passive functions, and need for single failure proof design. The level of detail is a utility option.

APPLICATION OF THE APPROACH

A detailed review of the current analysis for each event is performed to identify the sequence of mitigation actions that were used in providing successful protection for the plant. Each sequence usually involves a sensing function, some logic function, and some final mitigation action. This phase of the approach requires a thorough understanding of the safety analyses and a thorough understanding of the configuration of the plant. It involves strong communication with the analysis groups and with the responsible system engineers. In this way, all related system functions are identified for each mitigation action.

A very effective part of this approach is to develop and tabulate the set of system functions that are associated with each mitigation action. For example, the automatic initiation of the Reactor Core Isolation Cooling (RCIC) System, upon low reactor water level, includes these primary functions:

- Appropriate low water level sensors
- Logic for initiation
- RCIC System automatic startup function
- Water supply systems which are the sources of RCIC flow
- Feedwater System, which provides the piping path for RCIC flow to the reactor.

Supporting system functions have also been included in these sets of related functions. In this example, the support functions include the specific electrical power (and air) supplies for all functions (as needed), the RCIC turbine support systems (e.g., the containment receives RCIC exhaust steam), environmental control for the equipment (e.g., air conditioning), logic to transfer the source of RCIC suction from condensate storage to the suppression pool (if needed), and all systems which have piping boundaries associated with the sensors being used (often on instrument lines common to other equipment), as well as the main flow path boundary. These detailed system interrelationships are constructed by close examination of the plant system design configuration.

Several valuable benefits occur from the development of these sets of related functional groups: (1) They provide a complete set of coupled system functions in a convenient form; (2) The information is necessary for the full understanding of the relationships between plant design, licensing, maintenance, modification, and operation; and (3) The related functional sets also provide a means to consistently enter each function into the DBD data base for all events that need the mitigation action. Consistency is an essential ingredient of this DBD approach.

Using the processes described above, each event is evaluated using the available documentation:

- A basic description of the event is written, including any differences in the sequence of the event if it should occur at different initial power conditions. The emphasis here is to be certain to identify all the different paths of mitigation that may be required.
- All the safety challenges (applicable unacceptable results) to the plant are identified for the event. Is there a threat to the fuel, to the reactor vessel, to the containment, or to cause release of radioactive material?
- All the mitigation actions which are utilized in the plant safety analysis to avoid each potential unacceptable result are listed. If the same mitigation action helps avoid more than one unacceptable result, it is usually listed for the safety concern that occurs first. For example, in many events, Trip (Scram) of the reactor provides benefit to many aspects of the case. Its role in fuel protection is usually the most prompt need, so it is usually entered in that role. However, if a different Scram (Trip) sensing path is essential to another potential unacceptable result, it would also be entered there. Special attention is paid to the first Scram (Trip) path for each reactor operating condition (since some protection actions are only active at high power). Each mitigation action is keyed to the operating conditions to which it applies (e.g., some only apply at high power, others only apply during refueling).
- For each mitigation actions, all the system functions that contribute to that function are entered for that event - still keyed to the applicable operating conditions. The sets of related system functions described above are used extensively in this step of the DBD.
- Event unique mitigation functions are included as necessary. In addition, special constraints are entered depending upon the unique use of the mitigation action in the event. For example, a particular mitigation action may only be required if some other aspect of the event occurs (e.g., only if main condenser low vacuum develops). In other cases, certain actions may occur that are not necessary for the mitigation of the event (e.g., the turbine steam bypass valves are opened for a turbine or generator trip transient event, but this function is not usually required in these cases because most BWRs also show that acceptable protection is provided for these cases even with bypass failure).
- Characteristics of each system function are specifically tabulated. Some examples are automatic or manual initiation, and single failure proof design by itself or with an associated system function.
- Numerical values for setpoints, flow rates, response times, etc. are also included for the application of each analytical mitigation parameter. Technical Specifications and surveillance procedures can utilize this information as upper (or lower) analytical boundaries for acceptable equipment performance monitoring.

The DBD includes a section for each evaluated event. It provides descriptions of how the source documents were used to create the system functions that are assigned as required mitigation steps for that event. It also includes in tabular form, a listing of all these system functions for the event. Table 1 shows a portion of such an event table constructed for a Turbine Trip event for a typical BWR plant.

This process is continued for all events to be included in the DBD. A completed document would include all the events for which plant analyses have been submitted to the licensing authority. In this way, any mitigation action for which credit has been taken would be clearly included in the data base.

When all the event information has been added to the data base, it is possible to sort the information for other uses. A typical DBT&A DBD also includes listings of the information in the following areas of interest:

(1) All functional requirements for a given system are listed together. All instances of the same function are grouped together (e.g., all events that use the low water level signal for initiation of RCIC are grouped together in the list for system that provides the sensed low water level signal). All other functions provided by that system are similarly listed. This table becomes a direct input to each system design basis document. It lists all functions for which credit has been taken, gives unique information associated with any of those instances, and provides exactly which events take credit for the functions. Table 2 provides a portion of such a system requirement listing for the Reactor Protection System.

(2) All manual actions are also listed separately. The specificactions, the systems involved, the indicators used by the operators to decide to perform the actions, and the safety concern (unacceptable result) are included in this listing in addition to each event that requires the actions. This provides clear input to operational and abnormal event procedures. It also relates directly to the sections of the SAR that discuss operator actions during each event. An example of manual action that

Table 1 - Mitigation Functions for Turbine Trip Transient Event (Typical BWR)

SAFETY ACTION DESCRIPTION: Scram

React Oper State	Unacceptable Results Title	System Name	Description of the System Function
F	Fuel Failure	MAIN STEAM	Provide main turbine stop valve <90% open trip signal to RPS.
F	Fuel Failure	MAIN STEAM	Provide >30% turbine first stage pressure interlock signal to RPS (fail-safe logic).
F	Fuel Failure	FEEDWATER	Provide high reactor vessel pressure trip signal to RPS (fail-safe logic).
F	Fuel Failure	CRD	Scram signal from RPS will activate the control rod drive system to insert rods (scram) and close the scram discharge volume vent and drain valves.
F	Fuel Failure	REACTOR PROTECTION	Provide scram signal to CRD system on signals from main steam system indicating main turbine stop valves <90% open and turbine first stage pressure >30%.

SAFETY ACTION DESCRIPTION: Pressure Relief

React Oper State	Unacceptable Results Title	System Name	Description of the System Function
F	Fuel Failure	MAIN STEAM	Main turbine bypass valves open on turbine control system turbine trip signal. (This action may occur, but is not required by this event.)
F	Syst Stress	MAIN STEAM	SRVs open on high reactor pressure.
F	Syst Stress	PRIMARY CONTAIN	Accept SRVs steam blowdown to suppression pool.

Table 2 - Mitigation Actions for the Reactor Protection System (Typical BWR)

REACTOR PROTECTION SYSTEM - MODE DESCRIPTION:
Provide auto scram signal and SDV vent/drain valve isolation signal to CRD system.

Event Title	Safety Action Title	React Oper State	Unacceptable Results Title	Func Code	Description of the System's Function
01C PresReg Fail-Close	Scram	F	Fuel Failure	SF	Provide scram signal to CRD system on neutron monitoring system APRM neutron flux trip signal.
02 Turbine Trip	Scram	F	Fuel Failure	SF	Provide scram signal to CRD system on signals from main steam system indicating main turbine stop valves <90% open and turbine first stage pressure >30%.
03 Main Steam Isolation	Scram	D	Fuel Failure	SF	Provide scram signal to CRD system on neutron monitoring system IRM neutron flux trip signal.
03 Main Steam Isolation	Scram	F	Fuel Failure	SF	Provide scram signal to CRD system on main steam system MSIVs <90% open trip signal (if in RUN mode).

(more events as required)

REACTOR PROTECTION SYSTEM - MODE DESCRIPTION:
Provide signals to primary containment isolation system logic.

Event Title	Safety Action Title	React Oper State	Unacceptable Results Title	Func Code	Description of the System's Function
24 Rod Drop Accident	Pri Cont Iso	DF	Rad Release	SF	Provide low water level (L3) signal from feedwater system to PCIS for initiaiton of L3 isolations.
25A Large Break Inside	Pri Cont Iso	CDEF	Rad Release	SF	Provide low water level (L3) signal from feedwater system to PCIS for initiation of L3 isolations.

(more events as required)

appears frequently in the DBT&A DBD is the manual initiation of suppression pool cooling mode of the Residual Heat Removal System.

(3) All system functions associated with Design Basis Accidents are listed separately or identified uniquely to support the safety-related classification of system functions and the equipment and structures that perform the functions.

(4) All system functions associated with a particular mitigation action are listed separately. For example, all items associated with reactor Trip (Scram) are listed, then all items associated with core cooling, etc.

(5) All system functions required by postulated events during a specific reactor operating state are listed separately (e.g., during refueling).

(6) Other specific listings of information as required by the individual utility or licensing authority.

ALTERNATIVE SCOPE OF APPLICATIONS

The process is flexible. In some cases, it has been done for only a selected set of events. For example, the most limiting events (from the viewpoint of reactor operating limits) are chosen to provide the limiting event mitigation requirements upon the systems. Many mitigation actions are derived with this approach, but some system requirements are not listed since their source event has not been included. The unlisted system requirements must be covered using current documentation, or until a more complete events DBD document is produced. For example, the Refueling Zone high radiation protection functions are not included in the DBT&A DBD until events like the Refueling Accident or Loss of Fuel Pool Cooling are included in the DBD. The full value of the DBD is achieved when the complete set of events and thereby the complete set of mitigation actions are included. Then this approach becomes a complete source for all system design basis documentation, for safety evaluations of design changes and modifications, and for input to operating procedures for abnormal events.

The application has been extended different amounts along the path of support systems related to primary mitigation functions. The methodology works in all cases; however, the amount of effort and the size of the DBD are strongly affected by these choices. A variation which has been used for the documentation of the network of system interactions is to utilize a second, system interface DBD to include this level of detail without overwhelming the base document.

In some instances, the DBD has been designed to provide significant information about the regulatory requirements that apply to the plant and/or the analytical methods that have been used in the analysis of each event. This information is dependent upon the source of the analysis, and has been documented in separate sections of the DBD (since most analytical methods apply to more than one event).

When operational functions are included in a similar systematic documentation approach, a complete set of functional inputs to the system documents is provided, not just to those associated with event safety mitigation. One of the primary benefits of this alternative is to highlight those system functions that are important for avoidance of unit Trip (Scram) or other unnecessary actions (e.g., unnecessary isolations). In this way, evaluations of system modifications and design changes would have specific inputs to ensure that important operational functions as well as design safety features are not jeopardized.

SUMMARY

An effective, systematic approach has been developed to correlate all specific system requirements to all (or a selected portion of) plant accidents, transients, and special events. Figure 1 summarizes the process that has been developed. This approach provides a comprehensive foundation for the set of System Design Basis Documents being created and maintained by most utilities for use in evaluation of reactor system modifications, design changes, and effective plant operation.

AUTHORS

Larry Chi is currently the manager of Japan Core Engineering. Mr. Chi has worked in various capacities

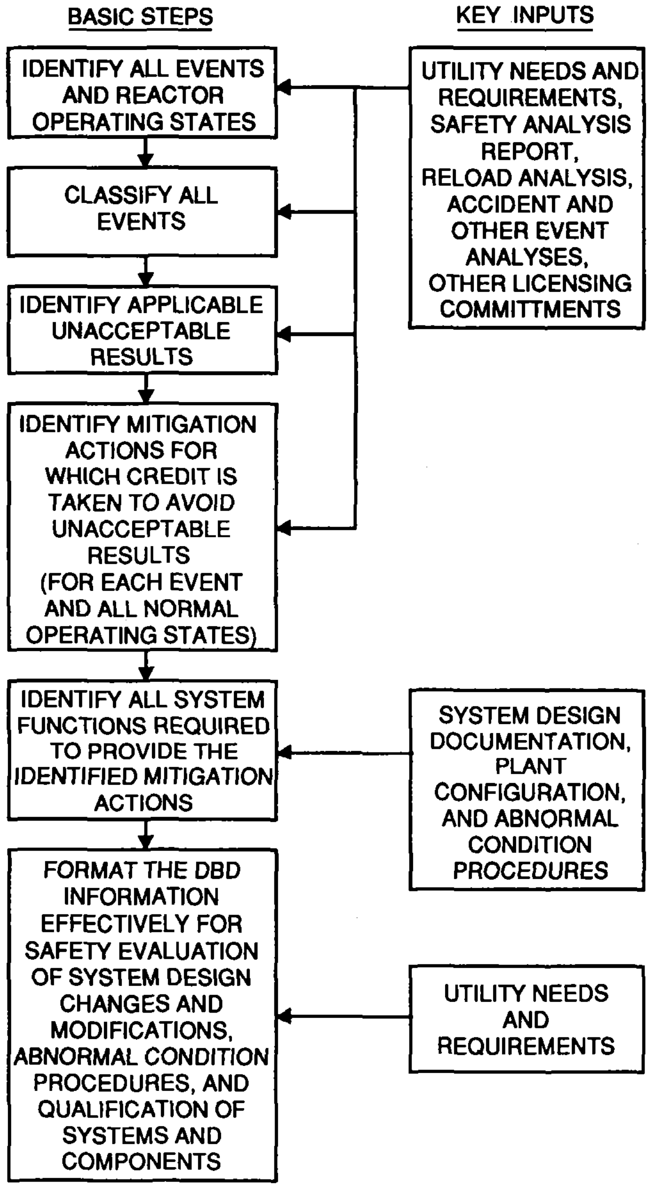

Figure 1 - Process Diagram for the Establishment of Mitigation Requirements

in the nuclear industry for 17 years. Mr. Chi holds engineering degrees from the University of California at Berkeley.

Eugene Eckert is currently serving as a principle engineer in BWR Engineering Services in San Jose, California. Mr. Eckert has worked in the design of BWRs for over 30 years. Mr. Eckert holds engineering degrees from Valparaiso (Indiana) University and Stanford (California) University.

Brit Grim is currently manager of Water Level Instrumentation Project. Mr. Grim has worked in the nuclear industry for 25 years. Mr. Grim holds engineering degrees from California Polytechnic State University and San Jose (California) State University.