

EDO Principal Correspondence Control

FROM: DUE: 12/20/07

EDO CONTROL: G20070846
DOC DT: 11/26/07
FINAL REPLY:

J. K. August
CORE

TO:

P. Madden, NRO

FOR SIGNATURE OF :

** GRN **

CRC NO: 07-0787

Borchardt, NRO

DESC:

Relational Design Framework Communication
(EDATS: SECY-2007-0541)

ROUTING:

Reyes
Virgilio
Mallett
Ash
Ordaz
Cyr/Burns
Dyer, NRR
Sheron, RES

DATE: 11/28/07

ASSIGNED TO:

CONTACT:

NRO

Borchardt

SPECIAL INSTRUCTIONS OR REMARKS:

EDATS

Electronic Document and Action Tracking System

EDATS Number: SECY-2007-0541

Source: SECY

General Information

Assigned To: NRO

OEDO Due Date: 12/20/2007 5:00 PM

Other Assignees:

SECY Due Date: 12/20/2007 5:00 PM

Subject: Relational Design Framework Communication

Description:

CC Routing: NRR; RES

ADAMS Accession Numbers - Incoming: NONE

Response/Package: NONE

Other Information

Cross Reference Number: G20070846, LTR-07-0787

Staff Initiated: NO

Related Task:

Recurring Item: NO

File Routing: EDATS

Agency Lesson Learned: NO

Roadmap Item: NO

Process Information

Action Type: Letter

Priority: Medium

Signature Level: NRO

Sensitivity: None

Urgency: NO

OEDO Concurrence: NO

OCM Concurrence: NO

OCA Concurrence: NO

Special Instructions:

Document Information

Originator Name: J. K. August

Date of Incoming: 11/26/2007

Originating Organization: CORE

Document Received by SECY Date: 11/28/2007

Addressee: P. Madden, NRO

Date Response Requested by Originator: NONE

Incoming Task Received: Letter

OFFICE OF THE SECRETARY
CORRESPONDENCE CONTROL TICKET

Date Printed: Nov 27, 2007 15:34

PAPER NUMBER: LTR-07-0787 **LOGGING DATE:** 11/27/2007
ACTION OFFICE: EDO

AUTHOR: J. August
AFFILIATION: AFF UNK
ADDRESSEE: Peter Lyons, Commissioner
SUBJECT: Relational design framework communication followup-status

ACTION: Direct Reply
DISTRIBUTION: RF

LETTER DATE: 11/25/2007
ACKNOWLEDGED: No
SPECIAL HANDLING: Made publicly available in ADAMS via EDO/DPC
NOTES:
FILE LOCATION: ADAMS
DATE DUE: 12/20/2007 **DATE SIGNED:**

EDO --G20070846



November 26, 2007

Patrick Madden
Deputy Director, Infrastructure Policy
U.S. NRC TWFN
11555 Rockville Pike, MS O-12E13
Rockville, MD 20852

Relational Design Framework

Dear Mr. Madden:

New NRC Information Technology infrastructure improves regulatory communications, effectiveness and new plant licensing, ultimately benefiting the nuclear industry. On a more fundamental level, information technology remains neglected. Logically extending 1950's era text-based 10 CFR Part 50 Appendices and B licensing framework remains a great unrealized nuclear industry opportunity. New methods that improve standard design license information accuracy, quality and accessibility would complement NRC efforts in many ways.

Recapturing our capacity to learn would help the nuclear industry resume new plant construction and improve operations. Standardization, modular construction, modern designs, integrated digital control systems, and integrating design basis information are all new. Although 10 CFR 52 approves four (4) Combined Operating License (COL) standard plant designs, none have been built; it remains to fully-exercise the COL process. (A COL allows an operating company – like NRG/South Texas Project – to construct a standard plant design (with a rule and design control documents) on an approved site, guaranteeing an operating license upon completion.)

In the first wave of nuclear construction (1969-1995), of 220 plants ordered; 117 were cancelled, with losses estimated at \$20 billion upward, depending on cost accounting used. For political reasons, Long Island Lighting Company's completed Shoreham plant was decommissioned as a write-off loss of over \$4 billion, without ever generating a megawatt. (Ten years operations were paid by ratepayers and shareholders.) With this background, NRC remains confident that financial losses attributable to regulatory delays will be avoided by reinvigorating thirty-year old licensing processes. To address regulatory delay costs from that era, Congress has approved up to \$2 billion in loan guarantees for the first six units ordered. Meanwhile, that Part 52 COL licensing allows plant construction startup on a schedule remains to be proven. Until demonstrated, that goal remains problematic:

- Plants have not been built in thirty years
- Rules have changed substantially, becoming more complex
- Many NRC inspectors are new; many designers' staff engineers are new
- Outstanding design issues like digital controls and design basis integration remain unresolved
- Three Mile Island (TMI) accident rule changes 1979-1986 confused requirements, contributing to delays at plants that did not have their operating license before TMI. Construction delays damaged public confidence and raised nuclear project costs, benefiting interveners, hurting investors, and setting the industry back.
- Amid 117 plant cancellations from 1979 to 1995, at least twenty billion dollars were written off, not including deregulation, restructuring and other charged write-downs.
- Due-diligence burden of proof that plants were ready to license fell upon licensees. Long license approval delays were the norm. Licensing submittal reviews for the Evolutionary Power Reactor (EPR) application (UniStar's Calvert Cliffs 3) appear headed down this process pathway, again.
- Lack of experienced, trained staff has already been cited as potentially affecting the ability to deliver new nuclear projects.

Whether the new plant regulatory framework can achieve project schedules remains unproven. Knowledgeable responsible persons have expressed reservations; NRC's additional resource requests for





Congress are public record. Today's loan guarantees would not have started to cover losses for the last nuclear plants constructed. Charging forward, leaving long lead-time problems unresolved until they became oppressive real-time, without forethought, planning or oversight created the conditions like those surrounding TMI. Pressing for startup, industry deferred addressing operational problems like nuclear steam system suppliers (NSSS), Architect Engineers and Owner/Operators technical material integration.

In hindsight, inconsistent performance indicated all was not well during the last construction wave. The opportunity to avoid repeating similar errors is now, yet participants struggle to pause long enough to self-assess historical root causes for technical problems. These suggest new methods approaching integrated plant design. Ironically, thirty-years of *Design Basis Loss*-themed NRC industry generic communications appears lost on not only industry, but the NRC itself. We are thus poised to repeat history.

For these reasons, NRC should challenge the staff to demonstrate their success path for new plant construction. It should embody the best tools available. Objective, independent analysts should monitor NRC progress resolving the difficult issues whose clear resolution supports new, safe nuclear construction. Scheduled Commission hearings should monitor progress. We recommend:

- NRC disclosure of actions taken to address design basis development and integration through design and construction phases into operations
- NRC identification of steps to improve design cycle review turnaround and technical material accuracy in light of past experience
- Presentation of complementary industry positions by prospective licensees
- Independent NRC technical assessment incorporating design and other materials into a design basis that effectively supports new plant licenses for their entire lifetimes

The COL process addresses historically scrapping newly-completed, licensed nuclear plants. The solution remains incomplete, however. Only by challenge can NRC assure that agency's effectiveness preventing the confusion and delays that beset the last round of nuclear construction. While it's easy to blame 1980-era nuclear collapse on TMI-based problems, we must not forget what led to those events. Regulatory delays raised costs, eroding public support. We all share responsibility for that record, but must assure such events never happen again, creating yet another round of nuclear plant cancellations.

Although NRC's recent record is exemplary, no new U.S. nuclear construction has started for the past 25+ years. To build new nuclear units safer, faster, at lower cost, in record time and with greater public assurance than ever before, all approaches must be objectively examined. New methods like relational databases should be considered on merit addressing historical design basis process deficiencies. Since June 1 2007, CORE has initiated over twenty relational method NRC communications to create awareness of the potential to improve the regulatory/plant design framework. Considering NRC's nuclear safety communications focus, we're frankly surprised to be waiting for an engaging response six months later. We seek an open, engaging dialogue with technical experts over relational design methods. Surely, where the supplicant makes significant safety claims as we have, from a staff of 2500, someone with knowledge and authority can be found able to discuss plant regulatory design bases on technical and administrative process methods!

CORE, Inc. brings proven design controls learned over thirty chronological years developing commercial nuclear generation operations tools. The relational design method fills a design basis void, eliminating systematic errors and operating problems that have persisted as long as commercial nuclear generation itself. Relational methods substantially improve design/review cycle productivity, design basis integration, and operating material development/update. Before startup time pressures suboptimize new plant designs, we should review design basis programs. Strengthening and implementing the best process improvements today in a common framework makes sense.

Sincerely,
J.K. August
President, CORE
(303) 425-7408/(303) 507-5272

Attachment: **Relational Design Framework Description**

2 of 9





c/

David Matthews
Director, Division of New Reactor Licensing
Nuclear Regulatory Commission
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Thomas Bergman
Deputy Director, Division of New Reactor Licensing
Nuclear Regulatory Commission
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

R. William Borchardt
Director, Office of New Reactors
U.S. NRC TWFN
11555 Rockville Pike, MS O-12 E13
Rockville, MD 20852

Gary Holahan
Deputy Director, Office of New Reactors
Nuclear Regulatory Commission
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

James Dyer,
Director, Nuclear Reactor Regulation
Nuclear Regulatory Commission
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Luis A. Reyes
Executive Director for Operations
U.S. NRC TWFN
11555 Rockville Pike, MS O-12 E13
Rockville, MD 20852

Pete Lyons, Commissioner
Nuclear Regulatory Commission
U. S. Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD 20852

Gregory Jaczko, Commissioner
U. S. Nuclear Regulatory Commission
US Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD 20852

Dale Klein
Chairman, Nuclear Regulatory Commission
U.S. Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD 20852



Relational Design Framework Description

Summary: Relationally approaching design presents a paradigm shift. Although concepts are common in everyday life, like all new technology relational format benefits and value are still hard to understand without seeing actual integrally presented designs results. To improve understanding, several problem metaphors follow presenting relationship design concepts. For demonstration software applications, please call CORE to arrange demonstration presentation of a CE System 80 plant in this format.

Library research projects don't provide fast, straight answers

Imagine working at a nuclear plant, and being asked to resolve three operational references to safety valve liftoff setting setpoints identified at 585, 595 and 615 psig respectively for a PWR pressure relief system late one Friday evening. Operating procedures cite 585 psig, training materials 595 psig, but actual setpoint calibration records call for 615 psig. How would you – the operating engineer – resolve this? This is the bread and butter daily work routine for many nuclear plant operations support engineers. For safety purposes, Operations probably needs a conservative answer fast – within the hour, to know whether or not to commence an orderly shutdown. This is because 615 psig – the actual setting, appears non-conservative in light of other design basis information provided. You have the uncomfortable chore of presenting Operations with an answer. You must address three tough challenges:

1. Establishing the final absolute authoritative source of the safety valve safety system setpoint limit
2. Doing research in a timely way to support operations
3. Avoiding unnecessarily calling “wolf,” forcing an unnecessary plant shutdown

Challenge 1: Establishing the final absolute authoritative source of safety valve setting limit requires a knowledgeable engineer review design materials to sift through the multiple setting requirements to find the limiting setting system source. In fact, the plant's licensed final safety analysis report (FSAR) Chapter 15 “Safety Analyses,” should summarize and provide all limiting safety system settings, and should provide a starting point for research. Equipment specifications must also be followed, which requires assuring the specified valve could support the FSAR Chapter 15-identified safety setting. (After all, a valve that won't operate because the design relief setpoint is above the service specification limit may not lift, or lift within range, or lift and reseal when pressure falls ...etc. etc.) Such efforts often involve research through several sets of documents, with repeated forays to a site design document library, computer historian database PDF document files list, approved final full-size drawings (process and instrumentation drawings, equipment drawings, isometrics...), master equipment list (MEL) calibration setpoints lists, operating procedures, technical specifications, and so forth. An engineer well-versed in the design can perform such a study in 4-8 hours, depending on personal expertise and design basis verification experience.

Challenge 2: Doing research in a timely way to support operations requires finding the answer before a technical specification grace period expires. Plants operate by technical specifications that assure they operate within the design basis of the FSAR analyses specified in the license. Most plant technical specification grace periods allow one, twenty-four, or seventy-two hour periods for degraded or indeterminate operations before forcing shutdown.

Challenge 3: Calling “wolf” forces plant shutdown. Unnecessary calls may be the single greatest concern for operations support engineers at the plant level. While safety culture and safety consciousness are laudatory ideals, practically, many engineers face tough career challenges with interpretations that force otherwise avoidable plant shutdowns. Shutdown to hot standby and restart minimally causes two or more shifts of high work load, lost revenues, and higher risks of equipment failure. Unnecessary evolutions are undesirable, for many reasons of which aging equipment is not the least. Professionalism, ethics and safety require conservative calls that demonstrate total public health and safety commitment. “*When in doubt, shutdown,*” provides an operating thumbrule. Fortunately, years of experience operating plants resolved most touchy requirements developing action support Tech Spec interpretations. However, aging plants and multiple historically-developed design bases continues to create ambiguous circumstances will continue to



arise as long as nuclear plants operate in the current framework. Examining a recent design basis loss illustrates how difficult and tough developing these answers is not located relationally within an integral, current design basis. Culture, attitudes and design complexity pose practical design basis barriers illustrated with recent examples.

Three CE System 80 units operated without safety injection (SI) system suction lines charged with water from the reactor sump. These systems' safety requirement is to charge water to the reactor vessel in a loss of coolant event long enough to achieve safe shutdown, avoiding fuel damage and potential releases substantial amounts of highly-radioactive fission products to the containment or environment. By charging water to the reactor vessel for a long-enough period to achieve safe shutdown, public health and safety is assured. Drawing suction from safety injection storage tanks while the tanks remain full, and then swapping to pump water from the building sump suction, high-head centrifugal pumps charge high-pressure water to the reactor vessel indefinitely. In the example above, a plant's SI pump suction lines from the reactor building sump were uncharged, inconsistent with safety requirements for the high pressure safety pumps in question. (High head pumps, like all pumps, require net positive suction head supplied at the inlet to avoid cavitation, friction and binding). The (erroneous) operating assumption that water level filling to above the pump inlet suction eye level in a design basis accident event would "force" water through the pump inlet, charging the pump somehow became established in the plant's operating culture, training, and procedures, – even common experience (and vendor guidance) was high head pumps don't pump air, much less charge their suction lines.¹ Equipment specifications required charging suction lines, apparently lost upon those developing the plant's operating procedures, calibration setpoints, and other specifications as a part of plant startup. Only twenty-odd years later did assessment independently discover out-of-compliance pump setup conditions for two pumps in each of three unit's independent safety trains.

Performing design basis research from the plant's document control center library is very undesirable, compared to having a straight answer in a time-limited technical specification compliance crisis. In fact, leaving the plant operating state indeterminate, forcing interpretations during operations – our historical tradition – presents human factor's dilemmas. That available technology made this necessary for the first thirty years of nuclear operations doesn't mean legacy practices must continue forever. Plant technical requirements – new or legacy – are distributed over many documents, analyses and locations, not just the Chapter 15FSAR final safety analyses provided. Indeed, this is one reason why operations require operating engineer support. One FSAR analysis will have ten-to-hundreds of pages of calculations and discussion to provide one needed operating value – our safety valve limit, for example, in the discussion above. Operations actually use the final analysis result, available upon completion, in an accessible format, hot-linked with the source document PDF that generated the requirement. In this manner, an operator could access approved, controlled plant design master equipment list (MEL) SSC, double-click the hot link to the source document, and see the requirements. From this a qualified engineer should be able to determine the overriding requirement. Further, derivative licensed materials like Technical Specifications and Operating Procedures that implement the licensed plant design basis must trace to their source requirements, per 10CFR50 Appendices A & B. Tools that improve the plant design basis ability to do so effectively improve operations. Forty years ago the method described here was all that technology could support. Today, relationally-designed data bases can convey critical content in hot-linked "threads" much like the Internet, only with much greater structural control. This is what the relational method offers in a crisis: the obligatory eight-hour research project under duress, or a predeveloped solution from experts linked back to every design document source at its exact point of development with just a few seconds of mouse clicks. What's better, an immediate, validated answer, or a research project taking hours of trite "need it now" research? Which provides the better answer, supporting more predictable, safer operations?

Structural relational design development purges most conflicting requirements from the plant design basis. Developing design relationally by database stimulates resolving most ambiguities, compounding into proactive support of future plant operations in addition to speeding design construction.

¹ That requires self-priming pumps.



Incomplete work doesn't compare to predeveloped, finished analysis

Developing a plant design answers most design basis questions – it has to. Otherwise, plants could not start up based on indeterminate safety status. Documenting decision process answers that result from design engineers specifying equipment (and justifying their selections) removes indeterminacy from evaluations. “Why is that check valve in the instrument air line to the safety train swap-over valve?” “Was loss of instrument air affecting both trains considered credible in design?” “Why isn’t that accident discussed in the FSAR Chapter 15 safety analyses?” “Was it an omission oversight, or simply deemed too insignificant to include?” Design basis engineers wrestle with questions like these routinely until at the end of their careers, they know their plant’s design as intimately as its original designers. How long does training an effective design basis engineer to support operations take? What happens when the current crop retires? Could we capture what they know in their heads, rather than force their replacements to learn the same lessons from scratch, repeating the same lengthy analysis trails of their predecessors? Perhaps, you acquire, we already have. After all, nuclear plants with thirty years of operations have thousands of operability assessments and interpretations available in various files. How accessible are they, though? Our experience was we could never count on locating an infrequently-used reference assessment in less than a shift, unless done personally. What’s better, an immediate validated answer based on experience-based growth, or a new, repetitive research project started from scratch taking hours of time? Which provides the better answer, supporting more predictable, safer operations?

Structured hot links perform faster than randomly-embedded threads

Most current Information Technology experts think librarian software for plant design basis PDFs (or GIFs) can access and link design basis documents on networks as if they were equivalent to relationally-developed databases. Embedded document hot links point to other documents, and occasionally search engines on the Internet like Google find linked document content. The similarities end there, however. Random hot links arbitrarily embedded by a librarian or technician without a design basis structure – e.g., site, design-specific PRA (Probabilistic Risk Assessment), systems, functions, specifications, equipment hierarchy, equipment lists, specified requirements, suppliers, operational limits, calibration and maintenance requirements, scheduled maintenance plans, operating procedures, plant license Technical Specifications.... all related to each other in a highly-structured way depend on the design. Random links and threads improbably recreate a license design basis, as explained in the example above. Using such results, design engineers must still grind out the functional relationships by examining and tracing out the critical content, with PDFs and drawings like P&IDs that summarize tens, hundreds, or even thousands of pages of development analysis that generates the final results. What’s faster on Google, going to the known sources (like the NRC’s website), or performing a keyword search on general terms? What takes less time? Which provides the better answer, supporting more predictable, safer operations?

Internet hotlink threads out perform fetching hardcopy manuals and drawings

Historically, up until ten or so years ago research was done by hardcopy or microfiche. Today most plants have critical documents like FSAR Chapter 15 Safety Analyses, P&ID drawings, MEL, Technical Specifications, and Operating procedures on their local area network for immediate retrieval. (PDF images superseded microfiche in the 1990’s as the most reliable, quickly-retrievable documentation method available to support operations.) Clearly, those documents available in PDF allow search and retrieval for information faster than walking to the plant’s document control center – their onsite library. The relational method carries this one further step, just as if an expert had highlighted the critical result(s) of each document, hot linking that back to its supported (derivative) design basis materials. In this way the operator with a question about the limiting safety valve can hot link, double-clicking back to any (all) of the source documents that support that component, its safety function, the system’s safety functions, their PRA-based importance, ...and so on.) Some documents like engineering operability or safety assessments never converted to PDF format, or had sequential file assignment numbers that didn’t allow direct linking into the plant design basis by systems, functions, MEL or assigned supplied component. These documents can be migrated into the relational model directly, with brief analysis content, capturing their results placing them where they yield greatest support benefits. Maintaining an operating plant’s design basis,



these decisions can also be developed directly in applications today, where they are more readily retrieval. What provides faster answers, supporting safer more predictable, operations?

Design basis structures hot-link source documents for birth-to-death retrieval

The plant design basis is the fundamental design structure originated by rules, design standards, consensus standards, and established practices (supported by statute law, common law, and purchase order-specified contractual requirements). Providing materials organized directly based upon the plant design basis is the most transparent method to present information. Using a book's table of contents or index is easier and faster than reading the entire text to locate critical information. Tagging critical information with hotlinks makes jumping even faster. What's easier, hot linking critical information with other critical information in a highly-structured format, or looking it up again starting from scratch, by happenstance or another method, as needs arise?

Relationally-organized design basis database outperforms independent documents containing critical design attributes

The plant's integral design basis from PRA – fundamental reactor technology – safety requirements – systems & safety functions – Structures Systems and Components (SSC) – Inspections, Tests, Analyses and Acceptance Criteria (ITAACs) – Technical Specifications, flows from top level design requirements under top level regulatory criteria identified by rules like Title 10 of the Code of Federal Regulations, Parts 20, 50, 50.34, 72, and 100 (see ANS Standard 53.1 Safety Requirements for Modular Reactors - draft). Providing critical design basis content tied to the source structure of governing rules and standards removes ambiguity from information precedence, authority and flow. What's better, clear unambiguous guidance hierarchy or user-dependent selection to extract, weigh and order complex operating requirements accurately?

Loss of Design Basis

Operating experience provides pragmatic real-life arguments supporting relational design basis methods. Most operating events involve design basis loss, ranging from fundamental engineering design errors (though rare) through training. Put another way, Management Oversight Risk Tree (MORT) failure methodology classifies general root cause categories. Management Control, Schedule, Physical Barriers, Procedures, Design and Personnel are several. Most causes (other than Management and Personnel errors) stem directly from the design or its basis translation into actionable operating derivatives like operating and test procedures, safety limits and calibration settings, monitoring and maintenance schedules, etc. Operational failures caused by willful misconduct, or foreseeable interdictable events to manage are rare. Consider some actual events:

1. NPSH (net positive suction head) SI pump charge requirement misunderstood (Palo Verde)

Failure to understand and translate pump suction head requirements into pump inlet NPSH, as specified by design characterizes this event described above. Conventional wisdom directly applied based upon similar (self-priming) vertical low head pumps failed to apply to high-pressure SI pumps. Incorrect analysis embraced the operating culture, via training and folklore perpetuating a myth. Generic communication warnings about uncharged water lines applicable went unrecognized. Incorrect explanations for otherwise obvious requirements went unheeded by plant personnel. The net result was that three units operated for many years with their safety injection systems – fundamental safety systems – outside their design basis. Industry operating experience barely touches the broad risk implications of these events. To place this in perspective, other plants faced lengthy forced shutdowns in years past over much less significant events (based on PRA).

2. Primary Coolant Makeup Leakage (Davis Besse)

Generation communications cautioned loss of primary coolant inventory and moisture around insulation on water lines for a period of nearly twenty years prior to Davis-Besse's discovery of control rod nozzle



penetration structural carbon steel corrosion attack. Evidence of leakage and inventory makeup changes suggesting leakage went unheeded, subordinated to time pressures and cost concerns (examination around the head penetrations was an extensive task). Expected due-diligence implementing generic communications with follow-up to identify unknown leakage sources didn't occur. Workers observed serious structural loss reinstalling control rod assemblies, finally discovering the extent of metal loss. Safety concerns included coincident rod ejection/loss of coolant accidents. Although reactor coolant makeup requirements monitoring showed trends that appeared obvious leakage indicators in hindsight, explaining evidence of moisture on and around the reactor top head, lack of makeup tech spec limits and absent questioning attitude from plant personnel almost caused a much more serious event.

3. NUREG 0737 (0660) – Multiple coincident deficiencies (Three Mile Island)

NUREG's 0737 & 0660 discuss many TMI lessons. Many design basis errors, including power operated relief valve design limitations, instrumentation problems, configuration management, maintenance controls and training combine to create this classic catechism for the Nuclear Plant Professional. So many problems were uncovered, including potential Hydrogen generation and explosion that a decade was required to work off operating industry requirements. TMI identifies many lessons, including use of PRA, deterministic license analysis limitations, generic communications importance, and "common cause" program issues – a long list of cautions operating nuclear plants, many of which tie to the design basis. Perhaps the single greatest contribution from TMI was creating awareness that operating risks can fall outside those addressed by FSAR deterministic safety analyses. Plant culture understanding and management commitment must meet the intent, rather than just letter of plant license operating requirements. This created an awareness of the need to instill a nuclear plant operating safety culture. The Institute of Nuclear Plant Operations was born out of this event, recognizing the industry's greatest risk was itself.

4. Hydraulic Oil Fire: Fyre-quel™ "fireproof" Synthetic Hydraulic Fluid (Fort St Vrain)

Since Brown's Ferry, nuclear plant fire "common cause" failures invoked many rules (Appendix R), to control and/or manage fire risk consequences. Cultures incorporate erroneous information into their design basis informally, which later become "facts," impossible to disprove on technical grounds, not unlike religious beliefs. Fyre-quel™, a non-combustible hydraulic fluid, was marketed to nuclear plants as "fire proof." Prevailing plant mythology held that Fyre-quel™ hydraulic fluid wouldn't burn. Training promoted this misconception. Fortified by that knowledge, operators dispelled and eventually came to ignore leakage from fast-acting steam isolation valve hydraulic actuators. Reheat steam safety valves with exposed surfaces at 800 F one level below the actuators made fire inevitable, given enough time. Though HTGR procurement buyers should have ignored marketing on the basis of higher steam and contact surface temperatures, this never happened. In fact, the opposite occurred. They convinced operations of the opposite case, unsupported by facts. Leaky hydraulic actuators eventually overflowed their catch-basin trays, dripping fluid onto hot reheat line safety valves until flashover occurred. The resulting fire burned cables outside the auxiliary cable spreading room, causing substantial damage. This event illustrates subordinate equipment specifications' and plant cleanliness standards' importance. Valve leakage exceeding manufacturer guidance had become acceptable to Operations, and operators tolerated hydraulic leakage and its undesirable side effects. Catch trays, buckets, and manual drains required constant operator attention to avoid leakage overflow and cleanup. Better maintenance practices would have provided more effective means managing oil leakage in lieu of additional manual work, avoiding spills and lowering costs.

Design Continuity in Operating Plants

Nuclear plants operate for years following their successful startup. Most plants operating today started with thirty or forty-year licenses, and many successfully sought twenty-year life extensions. Plant designs use large amounts of commercial grade components off-the-shelf, or fabricate design specific components under the NSSS. In either case, replacements cover components as small as motor operated valves to large steam generators.

