Duke Power®
A Duke Energy Company

R. A. JONES
Vice President

Duke Power
29672 / Oconee Nuclear Site
7800 Rochester Highway
Seneca, SC 29672

864 885 3158
864 885 3564 fax

March 20, 2003

U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Attention: Document Control Desk

Subject: Oconee Nuclear Station
Docket Numbers 50-269, 270, and 287
Defense in Depth and Diversity Assessment
Associated with the Digital Upgrade of Oconee's
Reactor Protective System and Engineered
Safeguards Protective System

Duke Energy Corporation (Duke) plans to replace the current analog based Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) with a digital computer-based RPS and ESPS, the Framatome Advanced Nuclear Power (FANP) Teleperm XS (TXS) System. By letter dated May 5, 2000, the NRC found the TXS System acceptable and found the Topical Report EMF-21 1 0(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," acceptable for referencing in license applications to the extent specified in the topical report and NRC Safety Evaluation. As part of the justification for this planned digital upgrade, Duke has completed a defense-in-depth and diversity (D-in-D&D) assessment in accordance with Standard Review Plan (SRP) Chapter 7, Appendix 7-A, Branch Technical Position (BTP) HICB-19.

Duke requests NRC to review the attached D-in-D&D assessment. This assessment is associated with a future License Amendment Request (LAR) that will be submitted for the RPS/ES digital upgrade. Duke is submitting this request in advance of the LAR to expedite approval of the D-in-D&D assessment.

The results of the D-in-D&D assessment demonstrate that the Oconee design has significant defense-in-depth and diversity to withstand an assumed software common mode failure (SWCMF) of the digital Reactor Protective System (RPS) and the Engineered Safeguards Protective System (ESPS). The existing Diverse Scram System (DSS) successfully mitigates

A001

many of the transients and accidents of concern. The acceptance criteria were met for all transients and accidents with the exception of the Large Break Loss of Coolant Accident (LBLOCA). For the LBLOCA, the assumed SWCMF of the automatic ESPS actuation of the Low Pressure Injection (LPI) System causes an unacceptable delay in the delivery of the emergency core coolant. Rather than add a diverse LPI actuation to mitigate this beyond design basis event, Duke has justified the elimination of the LBLOCA event from consideration for this assessment. This justification takes credit for leak detection capability, as discussed in BTP HICB-19, along with the low probability of occurrence of a SWCMF to the TXS system concurrent with the LBLOCA event. The radiological analysis methodology used in the D-in-D&D assessment is consistent with the methodology and assumptions used in the alternative source term (AST) LAR (October 16, 2001). The AST LAR credits dual Control Room intakes, which are scheduled to be installed by the end of 2005.

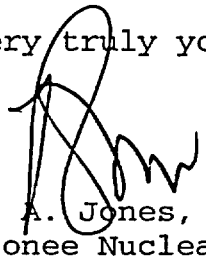
The analysis which supports the digital upgrade will only be performed once and not revised for each reload since the SWCMF is a low-probability, beyond-design basis event. This is consistent with the position Duke presented in a March 7, 2002, meeting regarding the planned RPS/ESPS digital upgrade. In the meeting, the NRC staff indicated they generally agreed that Duke's planned licensing approach appeared to be reasonable and to meet NRC guidelines for digital upgrades (reference NRC meeting minutes dated April 24, 2002).

Duke requests approval of the attached D-in-D&D assessment by June 15, 2003. Duke has delayed design work associated with adding a diverse LPI actuation until after this date. Therefore, approval by this date would allow Duke to avoid unnecessary design work. The first digital RPS/ESPS replacement modification is scheduled for the Fall 2004 outage for Unit 3. Duke plans to submit the LAR for the digital RPS and ESPS upgrade by June, 2003.

This request has been reviewed and approved by the Plant Operations Review Committee and Nuclear Safety Review Board.

If there are any additional questions, please contact Boyd Shingleton at (864) 885-4716.

Very truly yours,



R. A. Jones, Vice President
Oconee Nuclear Site

cc: Mr. L. N. Olshan, Project Manager
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Mail Stop O-14 H25
Washington, D. C. 20555

Mr. L. A. Reyes, Regional Administrator
U. S. Nuclear Regulatory Commission - Region II
Atlanta Federal Center
61 Forsyth St., SW, Suite 23T85
Atlanta, Georgia 30303

Mr. M. C. Shannon
Senior Resident Inspector
Oconee Nuclear Station

Mr. Henry Porter, Director
Division of Radioactive Waste Management
Bureau of Land and Waste Management
Department of Health & Environmental Control
2600 Bull Street
Columbia, SC 29201

R. A. Jones, being duly sworn, states that he is Vice President, Oconee Nuclear Site, Duke Energy Corporation, that he is authorized on the part of said Company to sign and file with the U. S. Nuclear Regulatory Commission this revision to the Renewed Facility Operating License Nos. DPR-38, DPR-47, DPR-55; and that all the statements and matters set forth herein are true and correct to the best of his knowledge.

R. A. Jones, Vice President
Oconee Nuclear Site

Subscribed and sworn to before me this 20th day of March, 2003

Connie M. Greazale
Notary Public

My Commission Expires:
12-19-12

Attachment

Oconee Nuclear Station
Defense-in-Depth and Diversity Assessment
for the RPS/ESPS Digital Upgrade

ABSTRACT

Duke Power Company is replacing the analog Reactor Protective System (RPS) and the Engineered Safeguards Protective System (ESPS) at the Oconee Nuclear Station (ONS) with a digital computer-based system (Framatome ANP (FANP) TELEPERM XS (TXS)). With an integrated digital protection system, there is a concern that a software common mode failure (SWCMF) of redundant elements within the digital protection system could propagate in such a fashion that the acceptance criteria for the ONS Updated Final Safety Analysis Report (UFSAR) transient and accident analyses would not be met. The NRC has established a methodology and acceptance criteria for Defense-in-Depth and Diversity assessments that are to be used when digital based protection systems are implemented in operating nuclear power plants. The methodology and acceptance criteria are documented in Standard Review Plan (SRP), Chapter 7, Appendix 7A, Branch Technical Position (BTP) HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems." This report presents the methodology used by Duke to address defense-in-depth and diversity and documents the results of an engineering study that examines the capability of the plant to withstand a hypothetical software common mode failure that results in a total failure of the digital RPS/ESPS to function. The methodology assumes a complete loss of RPS/ESPS and re-analyzes the thermal-hydraulic response, the core and fuel response, and the offsite and control room dose consequences for a spectrum of transients and accidents. This report demonstrates that Duke's methodology to address defense-in-depth and diversity are consistent with NRC requirements and acceptance criteria for this topic. The acceptance criteria were met for all transients and accidents with the exception of the Large Break Loss of Coolant Accident (LBLOCA). For the LBLOCA, the failure of the automatic ESPS actuation of the Low Pressure Injection (LPI) System causes an unacceptable delay in the delivery of the emergency core coolant. Rather than add a diverse LPI actuation to mitigate this beyond design basis event, Duke has justified the elimination of the LBLOCA event from consideration for this assessment. This justification takes credit for leak detection capability, as discussed in BTP HICB-19, along with the low probability of occurrence of a SWCMF to the TXS system concurrent with the LBLOCA event.

March 20, 2003
Attachment

Table of Contents

List of Figures

1.0 INTRODUCTION

This Report presents the methodology used by Duke to ensure that the requirements of the NRC position on Defense-In-Depth and Diversity (D-in-D&D) for I&C systems incorporating a digital computer-based Reactor Trip System (RTS) and an Engineered Safety Features Actuation System (ESFAS) are followed for the replacement of analog Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) instrumentation at the Oconee Nuclear Station (ONS). This report demonstrates that the Duke and Framatome Advanced Nuclear Power (FANP) concepts to address D-in-D&D are consistent with NRC requirements and acceptance criteria for this topic.

With a digital protection system, there is a concern that a software common mode failure (SWCMF) of redundant elements could propagate in such a fashion that the acceptance criteria for the Updated Final Safety Analysis Report (UFSAR) transient and accident analyses would not be met. At ONS, the RTS is the RPS and the ESFAS is the ESPS with the actuation portion designated the Engineered Safeguards Actuation. The NRC staff has established a methodology and acceptance criteria for D-in-D&D assessments that are to be used when digital based systems are implemented in operating nuclear power plants. The methodology and acceptance criteria are documented in the Standard Review Plan (SRP), Chapter 7, Appendix 7A, Branch Technical Position (BTP) HICB-19 (Reference 1).

This report presents analyses for a spectrum of transients and accidents using the worst-case software common mode failure (SWCMF) that has the potential to occur within the FANP TELEPERM XS (TXS) system (Reference 2) and then discusses the results with particular attention to the protection methods that remain available to recover from the event. A primary or backup automatic protection is provided for most events and is either a safety-related system or a control system. Some events will require operator action to provide the necessary protection functions.

2.0 REGULATORY POSITION

As a result of the reviews of Advanced Light Water Reactor (ALWR) design certification applications that used digital protection systems, the NRC established the following position on D-in-D&D for the advanced reactors. Points 1, 2, and 3 of this position apply to digital system modifications to operating plants.

1. The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

The additional manual capability required by Point 4 is considered necessary in advanced reactors because all of the protection and control systems typically are digital computer-based, and thus potentially vulnerable to common mode failure.

As set forth in points 1, 2, and 3 above, the NRC requires that a D-in-D&D assessment be performed for the proposed digital I&C system to demonstrate that vulnerabilities to common mode failures have been adequately addressed. As described in BTP HICB-19, the D-in-D&D assessment is only required for digital RPS and ESPS replacements. EPRI Technical Report (TR)-102348 Revision 1, "Guidelines on Licensing Digital Upgrades " (Reference 3) provides additional guidance on D-in-D&D assessments. This guidance was endorsed by the NRC (Reference 4) and used in the development of this report and aided in the establishment of certain boundaries. The descriptions that identify those systems which are considered part of ESPS and those which are not are provided in the ONS UFSAR (Reference 5).

In this assessment each of the applicable design basis events identified in the safety analysis report is examined. If a postulated common mode failure could disable a safety function that is required to respond to the design basis event being analyzed, then a diverse means of effective response (with documented basis) is necessary. The diverse means may be a non-safety system, automatic, or manual, if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

The purpose of this assessment is to demonstrate for the proposed ONS I&C digital upgrade with the TXS system, adequate D-in-D&D is provided in the design approach described in EMF-2267 (P), "Siemens Power Corporation Methodology Report for Diversity and Defense-in-Depth," (Reference 6) to satisfy the criteria established by NRC requirements. The NRC approved the FANP generic approach, which was discussed in FANP Topical Report EMF-2267 and applied in a limited fashion in FANP Topical Report EMF-2340 (Reference 7).

3.0 ASSESSMENT METHODOLOGY

The systems included in the four echelons of defense-in-depth consist of the control system, the RPS, the ESPS and the monitoring and indication system. These four echelons are ranked according to the preferred mode for handling an incident. First, the control systems are the preferred method to use to handle any event as they are in normal use throughout the plant cycle. The RPS is next, in that it is actuated to prevent any reactivity excursion, reactor building overpressure, reactor coolant system high pressure or low pressure, and reactor coolant system (RCS) high outlet temperature. Third, the ESPS is used to mitigate any event that has not been handled by the first two echelons. The monitoring and indication systems are the last echelon and provide the operator with the means to manually control the plant.

The failure of all automatic RPS and ESPS functions was postulated coincident with a SWCMF and an analysis was performed to show that a diverse means exist, not subject to the same failure, such that the conditions as outlined above are still met.

The goal of the ONS assessment has been to implement the Commission's positions cited in BTP HICB-19, to determine and correct vulnerabilities to undetected software common mode failures occurring coincident with the UFSAR transients and accidents identified below, and ensure that operators have enough diverse instrumentation to follow proper and acceptable manual actions. Effects of the combined failure, the SWCMF and the failure causing the event, including the event sequence are reviewed using the acceptance criteria in Section 9.9 of this report.

This defense-in-depth and diversity (D-in-D&D) study consists of four basic tasks. The first task is to identify the set of transients and accidents that are to be considered in combination with the assumed total failure of the digital RPS and ESPS. This task was accomplished by first listing the transient and accident events in the ONS Updated Final Safety Analysis Report, Chapters 10 and 15. Additions to and deletions from this list were then made with the intent of creating a list that is typical of the spectrum of transients and accidents for pressurized water reactors. The following list was then proposed to the NRC in a meeting on March 7, 2002.

- Control Rod Bank Withdrawal at Zero Power
- Control Rod Bank Withdrawal at Full Power
- Boron Dilution at Full Power
- Loss of Coolant Flow
- Locked Rotor
- Dropped Control Rod
- Turbine Trip
- Steam Generator Tube Rupture
- Control Rod Ejection
- Large Steam Line Break
- Small Steam Line Break
- Small-Break LOCA
- Loss of Main Feedwater
- Loss of Offsite Power
- Main Feedwater Line Break

Subsequent to this NRC meeting, the large break LOCA (LBLOCA) event was added to this list. The second task was an evaluation of this list of transients and accidents to identify which could challenge the acceptance criteria given a complete failure of the RPS and ESPS. Those events were then simulated using computer codes (Reference 8). The third task was to define acceptance criteria and to determine which events failed the acceptance criteria. The first three of the following four acceptance criteria were proposed at the March 7, 2002 NRC meeting. The fourth was included when the LBLOCA accident was added to the list of transients and accidents.

- Offsite dose limits are consistent with the ONS licensing basis unless BTP HICB-19 allows higher.
- Reactor Coolant System pressure is maintained less than ASME Code Service Limit C.
- Reactor Building pressure is maintained less than realistic failure pressure.
- Coolable geometry is maintained.

The fourth task was to determine what plant modifications or other resolution may be necessary to address the events for which the results of the D-in-D&D study showed that the plant design was not capable of withstanding the software common mode failure. In general, the methodology follows Duke's NRC-approved methodology for analyzing non-LOCA transients and accidents. FANP, the fuel vendor and supplier of the LOCA analysis of record, evaluated the LOCA events.

For each event analyzed, alternate mitigation actuation functions are identified that will prevent or mitigate core damage and unacceptable release of radioactivity. Where a common mode failure is compensated by a different automatic function, a basis is provided which demonstrates that the different function constitutes adequate mitigation for the conditions of the event. Where operator action is cited as the diverse means for response to an event, then the availability of adequate information (indication) and sufficient time for operator action is demonstrated. This assessment does not attempt to demonstrate that existing conservative safety analysis acceptance criteria are satisfied because the postulated occurrence of a SWCMF to the TXS system is extremely unlikely and beyond the design basis for any typical nuclear power plant.

These evaluations were examined to find any results showing that the plant design was not capable of withstanding the software common mode failure. If so, alternative justifications or plant modifications to address the D-in-D&D findings were identified.

These alternative justifications may be based upon the availability of systems outside of the scope of the analysis that act to prevent or mitigate the event of concern such as taking credit for the leak detection capability to prevent loss of coolant accidents. BTP HICB-19 indicates that certain identified vulnerabilities may be acceptable. For example, Section 4 of BTP HICB-19 notes "I&C system vulnerability to common mode failure affecting the response to large-break loss-of-coolant accidents and main steam line breaks has been accepted in the past. This acceptance was based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs." Duke's assessment takes credit for leak detection capability to eliminate the need to re-analyze the large break LOCA. ONS does not have secondary coolant system leak detection so this provision could not be applied to main steam line breaks.

There is a difference between the conservative rules defined in Appendix K of 10CFR50 (Reference 9), which are used to evaluate Emergency Core Cooling System (ECCS) performance and demonstrate compliance with the 10CFR50.46 criteria, and the acceptance criteria used in this assessment (refer to Section 9.9). The Appendix K requirements impose much conservatism on the analysis of plant responses to LOCAs. These conservatisms include the requirement that the core decay heat is 20% higher than the design value, the accident occurs in conjunction with a failure of one ESPS digital channel, and none of the safety injection (SI) system accumulator inventory contributes to core refill prior to the end of the blowdown period. In a more realistic analysis of this scenario, the core heatup rate is reduced, realistic delivery of accumulator injection to the core is credited, and a single failure of ESPS equipment is not assumed. As a result, the operator has a longer period of time to respond in the unlikely event of failures in the automatic protection systems.

4.0 ONS DIGITAL DESIGN

The TXS system as described in FANP Topical Report EMF-2110 (NP), Revision 1, " TXS: A Digital Reactor Protection System" (Reference 2) will replace the present ONS RPS. In addition, the TXS platform will replace the ESPS as described in ONS FSAR Chapter 7. The data acquisition process, the signal validation, the protection logic and the voting for these systems will now be performed by TXS.

Reactor Protective System

The following RPS trip functions will be TXS based:

- Over Power (High Neutron Flux)
- Nuclear Over Power Trip Based on Flow and Imbalance
- Reactor Coolant Pump Monitor Trip
- Reactor Outlet Temperature
- Variable Pressure-Temperature
- Reactor Coolant Pressure-High and Low
- Main Turbine Trip
- Loss of Both Main Feedwater Pumps
- High Reactor Building Pressure

The trip functions that are assumed in the safety analyses are high flux, high pressure, low pressure, variable low pressure-temperature, high temperature, flux-flow and RCP pump monitor.

Engineered Safeguards Protective System

The Engineered Safeguards Protective System (ESPS) actuates the following safeguards systems on the following parameters. The automatic actuation of the ESPS is assumed to fail in this study due to the software common mode failure. Manual ESPS actuation is credited as described for the events analyzed.

- High Pressure Injection System (HPIS) on low hot leg pressure or high Reactor Building pressure
- Low Pressure Injection System (LPIS) on low-low hot leg pressure or high Reactor Building pressure
- Reactor Building Spray System (RBS) on high-high Reactor Building pressure
- Reactor Building Cooling System (RBCS) on high Reactor Building pressure
- Non-essential Reactor Building isolation on low hot leg pressure or high Reactor Building pressure
- Essential Reactor Building isolation on low-low hot leg pressure or high Reactor Building pressure

FANP has carefully designed the redundancy structure and the functional separation; in order to assure that the unlikely event of a TXS software common-mode failure does not affect the monitoring and indication functions required or the manual control of safety actuators. The isolated output signals to the Nuclear Steam Supply System (NSSS) control systems are not affected by the unlikely event of a postulated SWCMF in the TXS Protection System. The Post Accident Monitoring (PAM) indicators are not affected by the unlikely event of a postulated SWCMF in the TXS Protection System since no outputs are passed through the RPS to PAM. All TXS monitoring and indication functions that are vital to the D-in-D&D analysis are designed to be independent of the TXS software and do not result in SWCMF. In addition, some signals are taken between the output of the signal-conditioning module, but before the input module of the TXS platform. Therefore, these signals, taken upstream of any software actions, would qualify as a diverse Defense-in-Depth echelon.

The remaining safety related and non-safety related I&C systems will maintain their present design and, as a result, will remain independent and diverse from the TXS platform. The TXS system is divided into the following parts:

- Signal input modules
- Data processing (CPU)
- Voting of actuation signals
- Monitoring and Service

RPS Functions

The input signals for the TXS sets are grouped exactly like the existing Process Protection Sets. They are connected to the TXS automation system via Signal Conditioning Modules. The TXS sets exchange their process data via point-to-point fiber-optic data links. Each of four TXS sets has a complete set of all connected safety related process values. By comparison (Data Validation) between the redundant values, outlying signals are rejected and the optimum representative signal is selected.

The complete plant protection functions will be carried out in each of the four sets (i.e., four times compared to only one time in the existing system). Therefore, for each different RPS actuation, four actuation signals are now available.

The outputs of the four digital TXS Protection Sets are voted by relay, "2-out-of-4" configurations, in each of the channel sets, before actuating the Trip contacts. For each relay an additional contact is wired to the TXS Monitoring and Service Interface as a relay check-back signal. This is used for test and monitoring purposes.

ESPS Functions

The input signals for the TXS sets are grouped exactly like the existing Process Protection Sets. They are connected to the TXS automation system via Signal Conditioning Modules. In addition, the signals are sent from the signal conditioning module via an isolation amplifier to the corresponding RPS Protection Set (i.e., from ESPS Set 1 to RPS Set A). The three TXS ESPS sets exchange their process data via point-to-point fiber-optic data links. Each TXS set has a complete set of all connected safety related process values. By comparison (Data Validation) between the redundant values, outlying signals are rejected and the optimum representative signal is selected.

These three TXS RPS sets exchange their ES related process data via point-to-point fiber-optic data links. Each of these TXS sets has a complete set of all connected safety related process values. By comparison (Data Validation) between the redundant values, outlying signals are rejected and the optimum representative signal is selected. The complete ESPS protection functions, for both digital channels, will be carried out in each of the six sets (i.e., six times compared to only one time in the existing system). Therefore for each different ESPS actuation, six actuation signals are now available.

The actuation signals are connected to TXS digital actuation voters, which are assigned to either digital channel, voting "2-out-of-3", from each of the redundant actuation signals from the six

TXS channel sets. The TXS digital actuation voter is formed by a computer configuration consisting of two Master/Checker pairs. They are connected to the TXS channel sets via fiber optic point-to-point data links. One of the Master/Checker pairs performs the "2-out-of-3" voting for the actuation signals coming from the RPS sets; the other Master/Checker pair performs the "2-out-of-3" voting for the actuation signals coming from the ESPS sets. The binary outputs of the two Master/Checker pairs are OR gated by diode modules. Master and Checker compute the same application function and compare the results at the end of the cycle. In case of a disagreement, the complete Master/Checker pair shuts down. Only the other Master/Checker pair now handles the outputs of the respective ESPS actuation channel.

The output signals of the voters are connected to interposing relays, which provide direct access to the actuators. The purpose is to fan-out the actuation signal to a component level and to adapt to the appropriate 118 VAC / 125 VDC component actuation voltage level. Each contact replaces the final output contact of the existing ESPS System.

5.0 TXS SYSTEM DEPENDABILITY

The TXS platform at ONS employs several techniques that aid in reducing the likelihood of the occurrence of a software common mode failure by maximizing TXS dependability.

Quality software design and development programs and D-in-D&D set stringent standards for safety-related software. The TXS software is of the highest quality and has been accepted by the NRC for use in safety related systems (NRC SER dated May 5, 2000 (Reference 10)). Quality features of the TXS software are discussed in many FANP documents including EMF-2267 and EMF 2110 and within the NRC SER. The TXS software was designed using the guidance provided in IEC 880 (Reference 11), the supplement to IEC 880 (Reference 12) and Regulatory Guide 1.152 (Reference 13).

The TXS system is designed to exhibit deterministic instrumentation and control (I&C) system behavior. This means that the overall system behavior in response to any input data trajectories is determined by the validated application software and is free of any unintended interference from the operating system software or the system hardware. To ensure that the system's operating behavior is independent from any input data trajectories, the following set of system features is implemented: strict cyclic system operation, no process-dependent interrupts, and static allocation of system resources.

The application software is designed using the advanced SPACE engineering system. This tool was approved by the NRC as being qualified and, therefore, code produced by this tool is acceptable and of high quality. To minimize the probability of design errors, the design notation for the intended application functions is prepared in the proven format of function diagrams. Function diagrams are easy for I&C engineers and system designers to understand. The I&C system architecture is also designed using the SPACE engineering system.

Advanced automatic checks are integrated in the SPACE engineering system in order to detect errors in input data. SPACE also allows the engineer to design processor and busloads by optimizing the architecture (e.g. by parallel processing), and to allocate functionality to different processors within the I&C system. These checks also include the prediction of the overall response time. The documentation of the I&C system specification, which is stored in the design data bank, is reviewed against the basic requirements specification.

SPACE's most effective technique for eliminating design errors is the functional validation of the generated application software. For the functional validation, the generated application software includes not only the code for the designed functionality but the complete code for the redundant system, including communication between redundant digital channels. This software package is linked into a previously validated simulator (e.g., on a powerful workstation) and then checked by computing the relevant design transients. The functional validation process can also be used to generate the input/output data test files for the factory acceptance tests.

Another SWCMF prevention measure is that the items of equipment used in TXS are tested periodically at staggered times. These periodic tests include a restart of a function processor with a re-initialization. If, despite this testing, a concealed time-dependency is still present, simultaneous failure of several function processors is nonetheless precluded because each function processor "sees" a different time, resulting from the time of its last test cycle. The input channel test is performed every outage and checks both the accuracy and the response time for all inputs. The function test is a start up self-test and a software identity check that is performed every outage. The ESF actuator test is performed every outage and is a GO-NO-GO test. The Reactor Trip Breaker test is staggered monthly. ONS Technical Specifications (TS) set the frequency and extent of all required testing for the TXS system.

The self-monitoring software performs a sequence of checks on the various hardware components of the processing module. These checks include a Random Access Memory test and EEPROM test and a watchdog timer test. This activity is performed during time intervals when the cyclic processing of the function diagrams is inactive. This is a continuous check and is monitored by the runtime environment (RTE). The exception handler receives the errors, stores them, and responds properly. The watchdog timer is reset every cycle to a certain value that is greater than the activation cycle for the RTE cycle time. If the RTE does not terminate correctly because of a fault, the watchdog timer times out and generates a hardware interrupt request. This request activates the interrupt service in the exception handler, saves the current state of the processor for subsequent analysis, and places the processor in a defined fault state. The first watchdog fault is considered a transient and the CPU is rebooted where a complete start-up self-test is executed. This provides for an in-depth check of the CPU hardware. If the watchdog times out again, then the complete I&C sub rack has to be reset via manual means. A complete check of the failure information would be performed before the reset.

In addition, the self-monitoring features for TXS consist of a startup self-test which confirms operation upon system initialization, and a cyclic self-test. There are an exception handler, error detection by the runtime environment, cabinet monitoring devices and engineered monitoring features. The self-monitoring features monitor several important runtime environment features, including CRC sum check, message age monitoring, message header check, plug-in monitoring, computing time monitoring, cyclic self-test monitoring, and master/checker result monitoring on the TXS voters. The RTE also increments the cycle counter. The cycle count at the time of transmission is appended to every message. This information is used to monitor the validity of the message and the correct function of the transmitter.

Selected failure management techniques have been employed within the TXS System. Software architectures have been designed to minimize SWCMFs. Detecting all of the types of failures that are possible through the TXS testing techniques makes the probability of the TXS system detecting a software failure very high and significantly lowers the likelihood of a SWCMF occurring without detection. This detection is available either through automatic or manual means giving adequate compensatory action to ONS and its operators.

The mature operating history for the TXS system, which is on the order of more than 15 million accumulated hours for the SVE1 and SCP1 modules, includes no failures that have degraded plant operation. To date, all of the reported failures have been related to hardware, with no reported software failures occurring during plant operation.

6.0 DEFENSE-IN-DEPTH

There must be adequate diversity between the TXS software and the plant control systems, indications, alarms and read-outs, and manual actuation circuitry to show acceptable defense-in-depth so that a successful diversity assessment can be performed. In addition, the systems in place to meet the ATWS Rule (Reference 30) have to continue to meet the diversity provisions of that Rule. Diverse blocks for equipment/systems must be established to depict the equipment/systems that are not subject to the same SWCMF and, as a result, will provide a path for meeting the provisions of BTP HICB-19 as it relates to the ONS UFSAR analyses.

6.1 RPS/ESPS System Representation as Diverse Blocks

It is readily apparent that a SWCMF to the CPU (SVE1, SVE2, SCP1, and SCP2) will render the digital portion of the TXS platform inoperable. This is because of the commonality of the software within the CPU modules, which are part of every functional channel. Taking this into consideration it was determined to take the more conservative path at this time and to make the decision that a SWCMF would render the programmable portions of the TXS based RPS and ESPS inoperable and that the advantage of choosing diverse blocks within the TXS platform is not desirable. However, certain applications or future modifications could show the need for diversity between the input modules, the voting modules, the communication modules, and the CPU module. This could occur if an input signal would be processed via a TXS analog input module and then sent to an analog meter or other device, bypassing the CPU module. This would mean that this signal would not be affected by the SWCMF and its function (read-out or an actuation) would be treated as a diverse function in the D-in-D&D analysis. For this reason and to illustrate the defense-in-depth provisions provided by the TXS platform, a review of the modular aspects of the TXS platform is presented below.

The TXS platform is partitioned into blocks in accordance with NUREG/CR-6303, Section 2.5 (Reference 14) and NUREG-0493 (Reference 15). Diversity is determined at the block level. The different forms of diversity used are as follows:

- Design Diversity
- Equipment Diversity
- Software Diversity
- Functional Diversity
- Signal Diversity
- Human Diversity

The following assumptions are inherent to the D-in-D&D methodology and the interpretation of the assessment guidelines:

When a failure is assumed for a software block, RPS and ESPS actuations associated with this block, which should occur from both primary and backup channels, may not activate.

If the action credited to mitigate the consequences of the postulated accident is assumed to fail either as-is, high, or low due to a software block failure, then it is acceptable to conclude that all other actuations associated with the failed software block will fail in the same direction. It is not necessary to assume "smart" failures or the worst possible combination of all postulated failures.

Instrumentation channels that are not credited in the accident analysis to provide protection for the postulated event under assessment will not fail in a manner to worsen the consequences.

The purpose of examining software blocks within the TXS system is to configure blocks where failures either inside or outside the block cannot propagate across block boundaries. Postulated failures within a block are assumed to cause the most detrimental credible output signal, so that the entire block fails and all of its output signals assume detrimental values. All identical blocks are assumed to fail concurrently (including across divisions) and this assumption is repeated until the list of diverse blocks is exhausted. Also, blocks are assumed to be identical if the likelihood of common-mode failure is high.

Since the only module type containing software is the TXS CPUs, these are the only modules that can fail due to a software failure. Although other modules would remain operable, the information being propagated from the CPUs to these non-software modules would be corrupted with erroneous data. The propagation of the logic failures from certain groups of these modules would not inhibit the operation of the remaining groups of modules. This assessment identified that the following candidate blocks should be diverse from the CPU modules (they are not susceptible to the SWCMF) within the TXS digital platform:

- Analog Input/Output Modules
- Digital Input/Output Modules
- Counter Module
- Signal Conditioning Module
- 4-Channel Isolation Amplifier
- Communication Components for SINEC H1 and SINEC L2
- Interface Module LEBUS
- Power Supply

By using the guidance provided in NUREG/CR 6303, software diversity can be established between the RPS and the ESPS for the ONS application by taking advantage of the software diversity within the TXS platform between the RPS and the ESPS and establish diverse blocks for both.

The discussion provided below shows that a SWCMF to both the RPS and ESPS occurring at the same time is not probable and, as a result, the RPS and the ESPS failing concurrently due to a SWCMF is not considered plausible. By using the guidance provisions contained in NUREG/CR 6303 (*APPENDIX-BLOCK EXAMPLES)*, the case can be made that the RPS functions and the ESPS functions processed by the TXS platform are both diverse and independent from each other. While it is apparent that a SWCMF will render the TXS platform inoperable due to the

common CPU, there is inherent strength in the defense-in-depth provisions that exists within the TXS platform and within the ONS RPS/ESPS design. The numerous blocks, as discussed above, provide ample hardware diversity between them such that the probability of a CMF between these blocks is very small. The diversity between the modules noted above leads to a strong defense-in-depth capability within the TXS platform. Likewise the probability of a SWCMF between the RPS and ESPS is limited due to the diverse application software required for the different actuation modes and the timing differentials between them. By meeting the provisions established within the NUREG to eliminate the operating software as a source for a SWCMF, this contribution is reduced to an acceptable level.

This reduction is accomplished through several TXS design features. As per NUREG/CR-6303, the assumption has been made that the operating software programming is such that software failures are related to service demands and that service demands are distributed differently enough in the dissimilar chosen blocks (RPS/ESPS) to exclude the operating system as a separate cause of common mode failure. NUREG/CR 6303 states that the assumption is not valid if the operating system is complex or multitasking, or where more than a simple clock-updating timer is used. The operating system software for the TXS platform is simple and not multitasking and has been previously approved by the NRC SER. The TXS operating system can perform up to three tasks, but only one task is processed during the operational mode. First is the runtime environment, which is the actual platform for the application function. Second, the runtime environment activates the service task if it identifies a permissible request from the service unit. This can only occur when the TXS system is not in an active run-mode. Third, automatic self-monitoring operates as a background task, which cyclically checks the hardware equipment of the function processor for correct operating behavior. This self-monitoring task only occurs after the TXS has cycled through its operation phase and before it begins the next operational phase. Two other tasks are included in the operating system, which are only activated during startup or under fault conditions. As a result, the software during active run mode is only processing one task. The other tasks are processed when the system is not in the run mode, either after a data cycle or when a channel is not in use. The TXS channels run asynchronously, so the simultaneous failure of any kind is unlikely. Furthermore the channels run with a simple run-time updating timer. If a concealed time-dependency is still present, simultaneous failure of several function processors is nonetheless precluded because each function processor "sees" a different time, resulting from the time of its last test cycle.

NUREG/CR 6303 establishes that the standard for independence between two systems (RPS/ESPS) is that they must differ significantly in parameters, dynamics and logic. The actuation logic between the RPS and ESPS is structured differently (2-out-of-4 versus 2-out-of 3) and one is de-energize to actuate (RPS) and the other energize to actuate (ESPS). In addition, the technology for the logic of both systems is different. The RPS actuation voting logic is relay-based and the ESPS actuation voting logic is digital-based. The system design is based both on principles of fault exclusion and restricting the consequences of failures to the safety system. Even here, two diverse measures are taken to ensure that the consequences of a fault are restricted. First, the system design ensures that different loading profiles affect only the associated application function and not the system functions. The following design features achieve this:

- The entire application software functions cyclically. Process-dependent interrupts are excluded both in the user software and in the operating software to ensure cyclic processing of the user software in a deterministic way.
- The application software is free from data interference, which in this context means that any input signal related disturbance for one or more I&C functions

will only impact functions that are similar. It will not impact data processing in the diverse, independent I&C functions. Thus, SWCMFs in the application software will affect related variables whose computational block functions have the same software. As an example, the application software for the neutron flux function will not contain software similar to the application software for the pressurizer pressure function.

- Input data is only handled in the application software, meaning that there is no possibility of interference of input data on the operating system software and the runtime system.
- The program control in the system services is completely independent of the loading. This means that there is neither a direct dependency (e.g., in the form of process data dependent function calls) or an indirect dependency via the use of resources (e.g., CPU load).
- The operations on process signals are performed only in function block modules whose quality has been verified.
- The definition ranges of input signals for function blocks have been selected such that input data combinations that are possible from the analog to digital converter cannot cause values to fall outside the defined range.

At the same time, freedom from interference between independent application functions is also verified in the above tests. Independent application functions are coupled via their common processor system. Both the timing and the setpoint values for ESPS are different from the values within the RPS. The sensors for both systems are different, thereby eliminating sensor malfunctions as a source contributing to the occurrence of a SWCMF.

For two blocks performing similar functions but having different input values combined by different logic, it is assumed that the two blocks do not have a software common mode failure concern. The programming will differ in timing and logic because of the different input values and processing code, which are precisely the design features inherent between the TXS RPS and ESPS application software. The above reasoning, in combination with the inherent quality of the TXS operating and application software, the projected and measured reliability of the TXS platform, and with the numerous testability features supports the conclusion that the RPS and ESPS can be designated and treated as separate, diverse blocks when a SWCMF is applied to the TXS system at ONS.

Even though the RPS and ESPS can be treated as two diverse blocks and not subject to the same SWCMF, the analysis presented in Chapter 10 of this report treats these systems as the same block subject to the same SWCMF. For the ONS implementation, Duke has chosen the more conservative approach and does not take credit for the software diversity between the ESPS and RPS. That is the analyses assume that both the RPS and ESPS will fail when the same SWCMF is postulated. However, this conservative approach could be revisited as part of the final resolution of this Defense-in-Depth and Diversity Analyses.

6.2 Manual Control/Monitoring Diversity

In the current and upgraded I&C concept, the manual initiation of the reactor trip is performed by hard-wired push buttons on the Main Control Board (MCB), which bypass the TXS trip logic, and are connected directly to the control circuits of the trip breakers. Also, in the current I&C architecture, a manual trip switch is provided in each ESPS channel. There are eight manual trip

pushbuttons on the control console, one for each protective channel. For reasons of diversity and independence, these paths cannot pass through the programmable portion of the TXS and independent, diverse manual initiation paths are designed to be implemented in conjunction with the TXS platform. These manual initiation paths are independent from the TXS software.

Duke assures that all monitoring/indication that is necessary as a result of the D-in-D&D analysis is provided in an acceptable diverse and independent manner. The TXS system design provides the necessary monitoring information output downstream of the signal conditioning but upstream of the TXS platform input modules through qualified isolation devices where necessary. Therefore, the required monitoring and indication information are not subject to the TXS platform SWCMF as this information is upstream and therefore, independent (and diverse) from the TXS software.

6.3 ONS Systems Diverse from RPS/ESPS

ONS Instrumentation and Control systems' attributes have been evaluated for diversity from the TXS based RPS/ESPS for the categories of Design Diversity, Human Diversity, Equipment Diversity, Software Diversity, Functional Diversity, and Signal Diversity.

The following are the major differences between the TXS and other digital ONS I&C systems such as the ATWS Mitigating System Actuation Circuitry (AMSAC), the Diverse Scram System (DSS), or others:

- The design architectures are completely different.
- The design organization, management, designers, programmers, and testing engineers are different.
- The CPU modules, input/output circuit boards and bus structure are different.
- The power supplies are different.
- The software operating systems are different.
- The software development tools are different.
- The software validation tools are different.
- The software algorithms, logic, program architecture, timing, and order of execution are different.
- The application programs are functionally diverse.

The design architecture diversity attribute is a powerful type of diversity because this forces different configurations and functionality through the use of different compilers, linkers, and other auxiliary programs to be used. The ONS design for the control systems, which consist of non-safety related digital equipment, is clearly diverse and independent from the TXS platform. The analog based control systems are diverse from RPS/ESPS and not subject to any type of software failure. As such, actions to mitigate any event using any ONS system that is not TXS based will meet the guidance within the SRP (BTP HICB-19).

If control systems are modified in the future along the lines of a digital design, then the diversity arguments presented in this report will be applied and the control blocks will have to be reevaluated.

The following is a listing of the diverse systems within the ONS design that are used in the analyses presented in Chapter 10 of this assessment. Duke evaluated the impact of potential

failures of credited systems due to harsh environments. This evaluation is provided for the affected diverse systems below.

Integrated Control System

The Integrated Control System (ICS) coordinates the control of the reactor heat source via the Control Rod Drive System, the secondary heat sink via the Main Feedwater System, and the electrical load via the Main Turbine Control System. The ICS responds to all upsets in process parameters (decrease in RCS flow, trip of a main feedwater pump turbine, change in electrical load, etc.) and is designed to minimize challenges to the Reactor Protective System. The ICS is assumed to respond as designed, and will perform such functions as reactor runbacks, and secondary pressure control. This system is not affected by the SWCMF to the RPS/ESPS.

Since many of the ICS components are not qualified for a harsh environment and may not perform as assumed, Duke evaluated the potential effect of a harsh environment on ICS response and how this could affect the results of the analyses described in Chapter 10 of this assessment. This evaluation concluded that an ICS response different than that assumed, would have an insignificant effect on the results. Duke identified six events (Rod Ejection, Large Steam Line Break, Small Steam Line Break, SBLOCA, LBLOCA, and Main Feedwater Line Break) that are subject to harsh environment and have the potential to affect ICS response.

ATWS Mitigation System Actuation Circuitry

The ATWS Mitigation System Actuation Circuitry (AMSAC) was installed in compliance with 10 CFR 50.62 (Reference 30) requirements to improve the capability to mitigate an anticipated transient without scram (ATWS) event. The AMSAC is part of another independent and diverse block and will continue to meet the ATWS Rule. The AMSAC system provides an independent and diverse backup to the TXS based ESPS protective features. This system mitigates a loss of main feedwater ATWS event by tripping the turbine and starting the Emergency Feedwater System. This system is not affected by the SWCMF to the RPS/ESPS. Duke evaluated potential AMSAC failures due to a harsh environment for the events in which AMSAC is credited and confirmed the failures would not adversely affect the results of the analyses described in Chapter 10 of this assessment.

Diverse Scram System

The Diverse Scram System (DSS) was installed in compliance with 10 CFR 50.62 (Reference 30) requirements to improve the capability to mitigate a primary system overpressure event, such as an ATWS event. The DSS is part of another independent and diverse block and will continue to meet the ATWS Rule. The DSS system provides an independent and diverse backup to the TXS based RPS protective features. The DSS successfully mitigates many of the transients and accidents of concern (refer to Section 10). If the Reactor Coolant System pressure exceeds 2450 psig, then the DSS trips control rod Groups 5-7. The negative reactivity associated with Groups 5-7 is sufficient to shut down the reactor. The DSS is independent of the RPS, and so a failure of the RPS has no effect on the DSS. Therefore, the ONS DSS has a redundant capability to trip the reactor following the SWCMF of the digital RPS for any event that pressurizes the RCS to 2450 psig. Actuation of the DSS is the key mitigation action credited for many of the events considered in this study. This system is not affected by the SWCMF to the RPS/ESPS. DSS is not affected by harsh environments for events in which it is credited.

Main Feedwater System

The Main Feedwater System (MFW) provides main feedwater to the steam generators during power operation and also post-trip. The Emergency Feedwater System is only required when the MFW System has been lost. This system is not affected by the SWCMF.

Emergency Feedwater System
The Emergency Feedwater System (EFW) actuates on low main feedwater pump turbine hydraulic oil pressure, on low steam generator level, and on AMSAC actuation. It is only relied on when the MFW System is not available. The EFW consists of two 100% capacity motor-driven pumps, one aligned to each steam generator, and one 200% capacity turbine-driven pump supplying both steam generators. The EFW System actuates independently from the RPS and ESPS Systems, and is not affected by the SWCMF.

Automatic Feedwater Isolation System
The Automatic Feedwater Isolation System (AFIS) isolates MFW and EFW to a faulted steam generator following events that result in steam generator depressurization. The MFW pumps and the turbine-driven EFW pump are stopped at 550 psig steam generator pressure, and the affected motor-driven EFW pump is stopped below 550 psig provided that the depressurization rate is greater than -3psi/sec. The valves required to isolate MFW are also closed at 550 psig. This system is not affected by the SWCMF. Duke evaluated potential AFIS failures due to a harsh environment for the events in which AFIS is credited and confirmed the failures would not adversely affect the results of the analyses described in Chapter 10 of this assessment.

Core Flood Tank System
The Core Flood Tank System (CFT) consists of two passive accumulators pressurized with nitrogen to 600 psig. When the RCS pressure decreases below 600 psig, the associated check valves open and injection starts. This passive system is unaffected by the SWCMF.

7.0 SPECTRUM OF TRANSIENTS AND ACCIDENTS

The transients and accidents that are evaluated in the context of a complete failure of the RPS/ESPS are defined in this section.

Control Rod Bank Withdrawal at Zero Power
The control rod bank withdrawal at zero power transient is analyzed in UFSAR Section 15.2 Startup Accident. The control rods begin to withdraw as the initiating event, and insert positive reactivity. The reactor trips on either high flux or high pressure. This is the limiting RCS overpressure transient for ONS.

Control Rod Bank Withdrawal at Full Power
The control rod bank withdrawal at full power transient is analyzed in UFSAR Section 15.3 Rod Withdrawal at Power Accident. The control rods begin to withdraw as the initiating event, and insert positive reactivity. The reactor trips on either high flux or high pressure. This event is analyzed for both RCS overpressure and DNBR, but is not a limiting event for ONS.

Boron Dilution at Full Power
The boron dilution at full power transient is analyzed in UFSAR Section 15.4, Moderator Dilution Accidents. A boron dilution event causes an insertion of positive reactivity and an increase in reactor power. The reactor trips on either high flux or high pressure. This is a slow reactivity addition event and is not limiting for ONS.

Loss of Coolant Flow
The loss of coolant flow transient is analyzed in UFSAR Section 15.6, Loss of Coolant Flow Accidents. This event is initiated by a loss of power to one or more reactor coolant pumps. The

decrease in RCS flow causes a decrease in the DNBR. The reactor will trip on either the pump monitor trip, or the flux/flow imbalance trip. This is a limiting DNBR transient for ONS.

Locked Rotor
The locked rotor accident is analyzed in UFSAR Section 15.6, Loss of Coolant Flow Accidents. This event is initiated by the shaft of one reactor coolant pump stopping due to a mechanical failure. The decrease in RCS flow causes a rapid decrease in the DNBR. The reactor will trip on the flux/flow/imbalance trip. This is a limiting DNBR transient for ONS.

Dropped Control Rod
The dropped rod transient is analyzed in UFSAR Section 15.7, Control Rod Misalignment Accidents. This event is initiated by one control rod dropping into the core. This causes a negative reactivity insertion and a severe core power tilt. Subsequent control rod withdrawal increases reactor power and decreases the DNBR. The reactor will not necessarily trip. This is a limiting DNBR transient for ONS.

Turbine Trip
The turbine trip transient is analyzed in UFSAR Section 15.8, Turbine Trip Accident. This event is initiated by a trip of the main turbine. The reactor trips on high pressure. This event is not limiting for ONS.

Steam Generator Tube Rupture
The steam generator tube rupture accident is analyzed in UFSAR Section 15.9, Steam Generator Tube Rupture Accident. A rupture of one steam generator tube causes a decrease in pressurizer level and RCS pressure. Flow from the High Pressure Injection System (HPIS) is increased and the unit is stabilized without tripping the reactor. The reactor is shut down, and then the unit is taken to cold shutdown to terminate the event. This event is one of the limiting offsite dose events for ONS.

Control Rod Ejection
The control rod ejection accident is analyzed in UFSAR Section 15.12, Rod Ejection Accident. The ejection of a control rod causes a rapid power excursion, and the reactor trips on high flux. A small break LOCA also results. The HPIS is automatically actuated on low hot leg pressure. This event is the limiting reactivity addition event, and is also one of the limiting offsite dose events for ONS.

Large Steam Line Break
The large steam line break accident is analyzed in UFSAR Section 15.13, Steam Line Break Accident. A double-ended rupture of a main steam line causes a rapid secondary depressurization, and a trip of the reactor on variable pressure/temperature. The decrease in RCS pressure actuates the HPIS. This event is the limiting overcooling event, and the results are significant relative to the DNBR limit and the offsite dose consequences. For break locations inside containment, the Reactor Building Cooling System (RBCS) and Reactor Building Spray (RBS) actuate on high Reactor Building pressure. This event is limiting for containment temperature and pressure response.

Small Steam Line Break
The small steam line break transients are analyzed in UFSAR Section 15.17, Small Steam Line Break Accident. A small break in a main steam line causes a plant response that is similar to an increase in load. The reactor power increases and reaches a new steady-state condition. Due to the elevated power level, this event is limiting for DNBR and centerline fuel melt for ONS. For

break locations inside containment, the RBCS and RBS actuate on high Reactor Building pressure.

Small-Break LOCA
The small break LOCA accident is analyzed in UFSAR Section 15.14, Loss of Coolant Accidents. A small break LOCA event causes a rapid decrease in RCS pressure that trips the reactor on low hot leg pressure and actuates the HPIS on low hot leg pressure also. For larger break sizes the core flood tanks will inject at 600 psig. The resulting mass and energy release to containment actuates the RBCS and the RBS on high Reactor Building pressure. This event is not limiting for ONS.

Loss of Main Feedwater
The loss of main feedwater transient is addressed in UFSAR Section 10.4.7.1.1, Loss of Main Feedwater (LMFW). The event is initiated by a loss of both main feedwater pumps. The reactor trips on loss of both main feedwater pumps or on high hot leg pressure. The EFW System automatically starts and controls steam generator level post-trip. This event is not limiting for ONS.

Loss of Offsite Power
The loss of offsite power transient is addressed in UFSAR Section 10.4.7.1.2, LMFW With Loss of Offsite AC Power. The loss of offsite power results in a loss of the MFW flow, loss of power to the reactor coolant pumps, and causes the control rods to insert. The EFW System automatically starts and controls steam generator level post-trip. This event is not limiting for ONS.

Main Feedwater Line Break
The main feedwater line break accident is addressed in UFSAR Section 10.4.7.1.7, Main Feedwater Line Break. The rupture of a main feedwater line causes one steam generator to blow down, and a loss of MFW flow to the other steam generator. The reactor trips on high hot leg pressure. The plant response is initially a minor overcooling, and then transitions to an overheating event. EFW is actuated on trip of both MFW pump turbines by the Automatic Feedwater Isolation System (AFIS). EFW is then isolated to the affected SG by AFIS. EFW flow to the unaffected SG provides for decay heat removal. The resulting mass and energy release to containment actuates the RBCS and the RBS on high Reactor Building pressure. This event is not limiting for ONS.

Large Break LOCA
The large break LOCA accident is analyzed in UFSAR Section 15.14, Loss of Coolant Accidents. A large break LOCA event causes a rapid decrease in RCS pressure that trips the reactor on low hot leg pressure, and actuates the HPIS and Low Pressure Injection System (LPIS) on low hot leg pressure also. The core flood tanks inject when pressure reaches 600 psig. The resulting mass and energy release to containment actuates the RBCS and the RBS on high Reactor Building pressure. This event establishes the core power peaking limits for ONS. This event is also limiting for containment pressure response.

8.0 DESCRIPTION OF COMPUTER CODES USED

RETRAN-3D/MOD3.1
The Electric Power Research Institute (EPRI) RETRAN-3D/MOD3.1 code (Reference 16) is used for the non-LOCA system thermal-hydraulic analysis. RETRAN-3D was developed by

Computer Simulation & Analysis, Inc. for EPRI for simulation of most thermal-hydraulic transients of interest in PWRs and BWRs. RETRAN-3D has flexibility to model any general fluid system by partitioning the system into a one-dimensional network of fluid volumes and junctions. Models for components such as heat transfer surfaces, pumps, valves, and control systems are included. Equations for single and two-phase flow and a non-equilibrium pressurizer are included. The three-dimensional core model in RETRAN-3D is not used in this report.

VIPRE-01/MOD2

The EPRI VIPRE-01/MOD2 code (Reference 17) is used for the core thermal-hydraulic analysis. VIPRE-01 was developed by Battelle Pacific Northwest Laboratories for EPRI. The subchannel analysis approach is employed, which divides the core and fuel assemblies into a number of quasi-one-dimensional channels that communicate laterally by crossflow and turbulent mixing. VIPRE-01 is used to calculate the departure from nucleate boiling ratio (DNBR) and the fuel centerline temperature.

FATHOMS/DUKE-RS

The FATHOMS/DUKE-RS code (Reference 18) is used to simulate the containment pressure and temperature response to pipe rupture events. FATHOMS was developed by Numerical Applications, Inc. and is a predecessor to the GOTHIC code. FATHOMS solves the conservation equations for mass, energy, and momentum for multi-component, two-phase flow. Models for containment fan coolers and spray systems and included. The analyses in this report use the lumped-parameter approach.

CASMO-3/SIMULATE-3P

The CASMO-3/SIMULATE-3P code system (Reference 19) is used for the neutronic elements of core design for ONS. CASMO-3 calculates macroscopic cross sections for input to SIMULATE-3P. SIMULATE-3P is a three-dimensional nodal simulator code used for calculating core power distributions and core physics parameters.

RELAP5/MOD2-B&W

The RELAP5/MOD2-B&W code (Reference 20) is used by FANP for the ONS LOCA peak cladding temperature analysis. It is also used by Duke Power for the LOCA mass and energy release analysis. The RELAP5 code can be used to solve the transient behavior of any general hydraulic system. The system to be modeled is discretized into a one-dimensional network of control volumes that are joined by junctions. The code solves the continuity, energy, and momentum equations for both the liquid and steam phases. Constitutive relationships are used to model interactions between phases. Special component models for reactor kinetics, heat conductors, pumps, valves, and control logic are included.

LOCADOSE

The LOCADOSE computer code system (Reference 21) is used to calculate radioisotope activities within regions, radioactive releases from regions, doses and dose rates within regions for humans and equipment, and inhalation and immersion doses and dose rates at offsite locations.

9.0 METHODOLOGY

This chapter presents the methodology (Reference 8) for performing the D-in-D&D analysis for the replacement RPS/ESPS for ONS. The fundamental assumption in this study is that a SWCMF results in a total failure of the RPS and ESPS. The methodology is therefore a

simulation of the design basis transients and accidents with no automatic reactor trip via the RPS, and no automatic engineered safeguards actuation via the ESPS. The objective of this study is to demonstrate that ONS can meet specified acceptance limits without automatic actuation of RPS and ESPS. The first step in the methodology is to identify the transients and accidents to be considered and which require analysis to bound the plant response. The next step is to select acceptance limits. The next step is to perform the analyses - system and core thermal-hydraulic analyses, neutronics analyses, containment response analyses, and dose consequence analyses. These involve selection of computer codes, initial and boundary conditions, and assumptions for each analysis. Any credit for manual operator action in the analyses needs to be identified and justified. The final step is to compare the results of the analyses to the acceptance limits to determine if the acceptance limits are met, and if not, what course of action is necessary. Each of these methodology elements is discussed in this chapter.

9.1 Selection and Screening of Transients and Accidents

BTP HICB-19 states, "In this assessment, the applicant/licensee should analyze design basis events (as identified in the safety analysis report)." Section 7.0 of this report describes the spectrum of transients and accidents in the ONS UFSAR that are considered in the methodology. These events include loss of secondary heat sink events, overcooling events, reactivity insertion events, loss of forced flow events, and loss of primary system inventory events. Anticipated transients (ANS Condition II type events), and infrequent events (ANS Condition III and IV type events) are included as the initiating events. Then, for each of these initiating events, a total failure of the RPS to automatically actuate is assumed. Also a total failure of the ESPS to automatically actuate is assumed. Manual actuation capability for both RPS and ESPS remains functional. The plant response is then determined by the action of the control systems, the reactivity feedback due to moderator and fuel temperature, and the response of the operator as directed by the emergency operating procedure (EOP). An important design capability at ONS for many of these events is the Diverse Scram System (DSS), described in Section 6.3 above. If the hot leg pressure increases to 2450 psig, the DSS will actuate and insert control rod groups 5-7, and that negative reactivity insertion will successfully shut down the reactor. The DSS will terminate many of the events quickly and with acceptable consequences. Events that normally require RPS actuation and do not actuate DSS require a combination of control system actions and operator actions to terminate the event. Events that require ESPS actuation, either for emergency core cooling or containment safeguards, rely on operator action to manually start the required safety systems.

Based on existing UFSAR analysis results, each event in the spectrum of transients and accidents assuming a failure of the RPS/ESPS can be assigned to one of five categories.

Category 1 - RPS and ESPS not actuated in the UFSAR analysis and no adverse impact

Category 2 - Event terminated by DSS actuation and no adverse impact

Category 3 - Event bounded by another event (not a limiting event)

Category 4 - Analysis required and results show acceptance limits are met

Category 5 - Analysis required and results show acceptance limits are not met (or this conclusion can be made without analysis). Events in this category do not meet the defense-in-depth and diversity requirements.

The methodology determines which of the above five categories each event is assigned to. The screening process based on experience with the UFSAR analyses, dispositions those events that fall into Categories 1, 2, and 3 without further analysis. Justification for the screening out of any events is detailed in Chapter 10 of this report. The remaining events require new thermal-hydraulic, neutronic, containment, and dose analyses to determine which fall into Category 4 and which fall into Category 5.

9.2 Selection of Initial and Boundary Conditions

The non-LOCA analyses use initial conditions that are selected based on the same conservative considerations as UFSAR Chapter 15 analyses. This is in contrast with BTP HICB-19, which states that "best-estimate (realistic assumptions)" can be used. This introduces an element of conservatism in the analysis results, but this is not very significant since the transient responses are strongly dependent on the boundary conditions.

The boundary conditions for each non-LOCA analysis are a combination of those used in the existing UFSAR analyses, which are conservatively modeled, and new boundary conditions involving control systems and operator actions (see Section 9.3) that are not credited in the existing UFSAR analyses. BTP HICB-19 states that, " . . . a diverse means of effective response (with documented basis is necessary). The diverse means may be a non-safety system, automatic, or manual if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time." The new analyses model the response of the Integrated Control System (ICS). The ICS has a very significant and beneficial impact on many of the events analyzed. The ICS is assumed to function as designed.

The initial and boundary conditions for the small-break LOCA analysis are conservative and consistent with the UFSAR Chapter 15 analysis, which employs the requirements of 10 CFR 50 Appendix K. The following exceptions to the existing UFSAR analysis and methodology were made.

- Core flood tanks at nominal pressure and liquid volume
- Core axial peaking factor = 1.17
- Core radial peaking factor = 1.6
- Three HPI pumps available
- Both LPI pumps available
- ICS assumed to withdraw control rods

These exceptions are more realistic and are appropriate for the purposes of this study.

9.3 Credit for Operator Action

The assumed total failure of the RPS/ESPS would be responded to by the operating crew by procedure. Anticipated transients without scram (ATWS) events (failure of RPS) are explicitly addressed in the ONS EOP. The EOP guidance for ATWS includes manually tripping the reactor from the Control Room, locally opening the control rod drive electrical breakers, manually inserting the control rods, emergency boration, and controlling RCS temperatures. This guidance is included in the EOP sections entitled Subsequent Actions, Rule 1 - ATWS/Unanticipated

Nuclear Power Production, and Unanticipated Nuclear Power Production. For this study the necessary manual operator actions for each event requiring analysis were identified. The operator response time for each action was then provided by the ONS Operations organization. These times are based on experience with testing operating crews on the ONS Simulator. Establishing operator action times using experience and knowledge rather than actual validation is considered appropriate for the beyond design basis events analyzed in this assessment. The following new operator actions (relative to the existing UFSAR analyses) are credited for event mitigation in the analyses in Chapter 10 of this report.

Control Rod Ejection

- Manual HPI actuation at 5 minutes
- Manual RBCS and RBS actuation at 8 minutes

Small-Break LOCA

- Manual reactor trip at 2 minutes
- Manual HPI & LPI actuation at 5 minutes
- Manual RBCS and RBS actuation at 8 minutes

Operator actions currently credited in the UFSAR analyses are not listed above, but are discussed in Chapter 10 in the description of the results of the analyses for each event.

9.4 System Thermal-Hydraulic Analysis Methodology

The non-LOCA system thermal-hydraulic analyses were performed using Duke Power's RETRAN-3D methodology for ONS. This methodology is described in topical reports DPC-NE-3000 (Reference 22) and DPC-NE-3005 (Reference 23). Revisions to these topical reports associated with the replacement steam generators and the RETRAN-3D code are currently under NRC review. Topical report DPC-NE-3000 details the RETRAN-3D modeling for ONS. Topical report DPC-NE-3005 details the analysis of the UFSAR Chapter 15 transients and accidents. The analyses performed use the methodology for the replacement steam generators as described in the revised topical reports. Minor modeling changes are included in the analyses in this report to simulate the RPS/ESPS failure scenarios of interest.

The small break LOCA analysis was performed by FANP using their RELAP5-based NRC-approved LOCA evaluation model for the Oconee class plants (Reference 24). As stated in Section 9.2, changes in certain initial and boundary conditions were made for the purposes of this analysis.

9.5 Core Thermal-Hydraulic Analysis Methodology

The core thermal-hydraulic analyses, which consist of calculating DNBR and the approach to centerline fuel melt, were performed using Duke Power's VIPRE-01 methodology for ONS. This methodology is described in topical reports DPC-NE-3000 (Reference 22) and DPC-NE-3005 (Reference 23). Revisions to these topical reports associated with the replacement steam generators and the RETRAN-3D code are currently under NRC review, but do not include any VIPRE-related revisions. Topical report DPC-NE-3000 details the VIPRE-01 modeling for ONS. Topical report DPC-NE-3005 details the analysis of the UFSAR Chapter 15 transients and accidents.

9.6 Nuclear Analysis Methodology

The nuclear analyses were performed using Duke Power's NRC-approved core design methodology for ONS. This methodology is described in topical report DPC-NE-1004A (Reference 19). The CASMO-3/SIMULATE-3P code system is used to calculate physics parameters and core power distributions for the transients and accidents. The limiting transient statepoints from RETRAN and VIPRE are input to CASMO-3/SIMULATE-3P for three core designs that are typical of current and future designs. Editing codes are then used to perform the census of those fuel rods failing either the DNBR limit or the centerline fuel melt limit, and the fraction of the core exceeding the fuel melt limit. Those pin census results are then used in the radiological dose analyses to quantify the source term.

9.7 Containment Response Analysis Methodology

The mass and energy release and containment response analyses were performed using Duke Power's NRC-approved methodology for ONS. This methodology is described in topical report DPC-NE-3003 (Reference 25). A revision to this topical report associated with the replacement steam generators and the RETRAN-3D code is currently under NRC review. RETRAN-3D is used for the steam line break mass and energy release analysis. RELAP5/MOD2-B&W is used for the LOCA mass and energy release analysis. FATHOMS is used for the containment response analysis.

9.8 Radiological Analysis Methodology

The radiological analysis methodology is based on methodology and assumptions presented in the alternative source term (AST) license amendment request submitted to the NRC (Reference 26), and subsequent responses to requests for additional information. Dose modeling assumptions follow the regulatory guidance specified in Regulatory Guide 1.183 (Reference 27). All doses are calculated with the LOCADOSE code, Version 6.0. The results of the thermal-hydraulic and neutronic analyses provide the percentage of fuel pins experiencing cladding failure due to exceeding either the DNBR criterion or the centerline fuel melt criterion (gap inventory release), and the fraction of the fuel experiencing fuel melt (pellet inventory release).

The limiting percentages of cladding failures and fuel melt failures from the power distribution analysis were used in combination to produce a bounding source term for each transient. Since both DNB and centerline fuel melt are assumed to result in the failure of the fuel rod cladding, the fission product gas inventory in the gap for the entire rod was used for the source term. For centerline fuel melt failures only, the fuel pellet inventory for those segments of the rod that fail also contributed to the source term. The entire mass of fuel material that reached the centerline melt temperature was assumed to release radioactivity according to the release fractions in Table 2 of RG 1.183. This table was derived from LOCA core melt assumptions, and is considered conservative for this application.

The fuel pins which are postulated to fail constitute a greater contribution to the source term than the average fuel pin. Since the core inventory used was determined for the average total core, a peaking factor is applied to the source term to account for the increased isotopic contribution from failed pins. Peaking factors are derived separately to represent the population of fuel rods that experience cladding failure and gap release and the population of fuel rods that experience

fuel melting. These factors are calculated for both the large steam line break and the loss of coolant flow events.

The radioactivity released from the fuel is assumed to be deposited instantaneously and homogeneously into the Reactor Coolant System inventory. Radioactivity is then transferred to the secondary side at primary-to-secondary leak rates calculated to occur during the event, until the release is terminated by operator actions. The radioactivity which leaks to the secondary side is assumed to be instantaneously released directly to the environment. No holdup or plateout in the steam generators is credited.

Atmospheric dispersion (χ/Q) factors calculated using the methods submitted in Reference 26 were used for dispersion from the release point to the Control Room air intakes. These models credit dual Control Room intakes, which are scheduled to be installed by the end of 2005. For this best estimate analysis, flowrates are assumed to be balanced between the dual intakes. Nominal 1998 tracer gas test results (plus 10 cfm for ingress and egress during the course of an accident) were used for unfiltered inleakage rates into the Control Room. These results are more conservative than the unfiltered inleakage rates derived from the 2001 ONS tracer gas test.

As stated above, the models credit dual Control Room intakes, which are scheduled to be installed by the end of 2005. This approach was selected because ONS is in the process of a full upgrade of the licensing basis for Control Room Habitability using AST. As described above, the ONS AST submittal is currently under NRC review. The analyses in review assume the dual intake installation. The ONS approach for AST implementation for RPS/ESPS discussed at the March 7, 2002 meeting with the NRC staff recommended that a consistent set of analysis assumptions for Control Room dose calculations be retained. This allows direct comparisons with the analysis approaches and results in the LAR under review. Depending on the timing of installation of the RPS/ESPS, the Control Room air intake modifications may lag the RPS/ESPS installation. However, if this were to cause a concern, a more realistic analysis using Control Room unfiltered inleakage values based upon the results of the 2001 tracer gas test would demonstrate that Control Room dose limits can be met without the air intake modifications.

The model used for the loss of flow transient was modified to credit the condenser for scrubbing of particulates, and removal of isotopic groups other than iodine and noble gases from the source term. These elements (such as alkali metals and lanthanides) are released in particulate form, and as such, are retained by the condenser and not released to the environment. This is a conservative assumption in that it does not credit any removal of iodine in the condenser.

9.9 Acceptance Criteria

Reactor Coolant System Overpressure

The Reactor Coolant System overpressure acceptance criteria are taken to be the acceptance criterion established for the ATWS analyses performed for ONS. That limit is 3000 psig, which corresponds to ASME Service Limit C.

Radiological
The dose acceptance criteria conform to Regulatory Guide (RG) 1.183, and are as follows. It is noted that RG 1.183 does not specify dose limits for the loss of flow event. The lower EAB and LPZ limits corresponding to the locked rotor event are assumed valid for the loss of flow event.

Location	Regulatory Guide 1.183 Limit	
	Large Steam Line Break	Loss of Flow
EAB Boundary	25 rem TEDE	2.5 rem TEDE
LPZ Boundary	25 rem TEDE	2.5 rem TEDE
Control Room	5 rem TEDE	

The dose calculations for each event that results in cladding failure use a pin census (% of fuel pins in the core that undergo cladding failure) based on the core power distribution at the limiting transient statepoints for each event. Calculations are performed to determine how many pins fail and release their gap inventory due to exceeding the DNBR or the centerline fuel melt acceptance criteria. Failures due to centerline fuel melt are also summed on a fuel pin segment basis to develop an additional source term that assumes the pellets in that segment melt and release their fission product inventory.

Reactor Building Pressure
The Reactor Building pressure limit is taken as the ultimate strength of the ONS Reactor Building at a 98% confidence level, which is 125 psi. This is based on actual material strength test data for the various structural components (concrete, reinforcing steel, tendons, etc), and defining the ultimate strength as the pressure required to yield the tendons after the liner plate and concrete reinforcing have already yielded.

Maintain a Coolable Geometry
The acceptance criteria for LOCA are specified in 10 CFR 50.46, "Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors." For the purposes of this study it is proposed that the fourth acceptance criterion from 10 CFR 50.46 be used. "(4) Coolable geometry. Calculated changes in core geometry shall be such that the core remains amenable to cooling." This criterion basically requires that cooling of the core does not allow the fuel assemblies to be physically changed to the extent that coolant cannot flow up through the channels and remove decay following the reflooding phase. This allows post-LOCA ballooning and rupture of the fuel pins, but not gross changes in core geometry that could obstruct flow.

10. ANALYSES AND RESULTS

This chapter presents the evaluation results or the analysis results for each of the transients and accidents. Each event is characterized as a Category 1 through 5 event as described in Section 9.1. For those events in Categories 4 and 5 that require new thermal-hydraulic, neutronic, containment, and dose analyses, the results of the analyses are discussed including figures of key parameters and the radiological consequences. Additional analysis details are provided in Reference 8.

10.1 Control Rod Bank Withdrawal at Zero Power

The UFSAR Section 15.2 startup accident analysis, assuming a software common mode failure of the digital RPS, will be successfully mitigated by the Diverse Scram System. No actuation of the ESPS is required. The reactor will be shut down and no significant adverse consequences will result. This is a Category 2 event.

10.2 Control Rod Bank Withdrawal

The UFSAR Section 15.3 control rod bank withdrawal transient analysis, assuming a software common mode failure of the digital RPS, requires thermal-hydraulic analysis to determine the plant response. The results of the RETRAN-3D analysis are as follows, and are shown in Figures 10-1 through 10-4. The withdrawal of the control rods adds positive reactivity and core power increases (Figure 10-1). The ICS responds by increasing MFW flow to match the increase in power. RCS pressure and hot leg temperature increase (Figure 10-2). RPS trip setpoints for high power, flux/flow/imbalance, high temperature, and high pressure are exceeded, but the assumed failure prevents reactor trip. The pressurizer PORV lifts at 289 seconds, but cannot limit the RCS pressure increase. The pressurizer code safety relief valves lift at 311 seconds. The DSS setpoint of 2450 psig hot leg pressure is reached at 310 seconds, and the control rods start to fall into the core and terminate the event at 313 seconds. The normalized core heat flux, core outlet pressure, core inlet temperature, and core flow are shown in Figure 10-4.

VIPRE is used to determine the set of core peaking factors at which the DNBR limit will be exceeded at the limiting statepoint. These peaking factor limit curves are then used in SIMULATE to analyze the pin census for the percent of fuel rods failing the DNBR and centerline fuel melt limits. The result of the SIMULATE pin census is no fuel cladding failures. Consequently, the radiological consequences for this event would not be significant and are not analyzed. The RCS overpressure and Reactor Building overpressure acceptance limits are also not challenged for this event. The results of the analysis of the uncontrolled rod bank withdrawal assuming a total failure of the RPS/ESPS show that the plant response meets all acceptance limits. This is a Category 4 event.

10.3 Boron Dilution

The UFSAR Section 15.4 boron dilution event analysis determines the allowable operator action time to terminate a boron dilution event. That time is not affected by the assumed failure of the RPS/ESPS. In addition, the reactivity insertion rate is bounded by the Section 10.2 control rod withdrawal event, and so the core power increase transient and resulting minimum DNBR are also bounded. This is a Category 3 event.

10.4 Loss of Coolant Flow

The UFSAR Section 15.6 loss of coolant flow transient analysis, assuming a software common mode failure of the digital RPS, requires thermal-hydraulic analysis to determine the plant response. Two cases are analyzed - a trip of all four reactor coolant pumps, and a trip of two

reactor coolant pumps. The results of the RETRAN-3D analysis are as follows and are shown in Figures 10.5 through 10.7.

Four Pump Coastdown

The trip of all four reactor coolant pumps causes an immediate decrease in flow (Figure 10-5) and an increase in moderator and fuel temperature. The ICS responds to the decrease in flow by inserting control rods. The thermal feedback and the insertion of the control rods adds negative reactivity and core power decreases (Figure 10-6). RPS trip setpoints for flux/flow/imbalance, high temperature, and high pressure are exceeded, but the assumed failure prevents reactor trip. The pressurizer PORV lifts at 27.3 seconds, but cannot limit the RCS pressure increase. The pressurizer code safety relief valves lift at 27.8 seconds. The DSS setpoint of 2450 psig hot leg pressure is reached at 26.1 seconds, and the control rods start to fall into the core and terminate the event at 29.1 seconds. The normalized core heat flux, core outlet pressure, core inlet temperature, and core flow are shown in Figure 10-7

VIPRE is used to determine the set of core peaking factors at which the DNBR limit will be exceeded at the limiting statepoint. These peaking factor limit curves are then used in SIMULATE to analyze the pin census for the percent of fuel rods failing the DNBR limit. The percent of fuel pins that exceeds the centerline fuel melt limit is also calculated. The results of the SIMULATE pin census is 26.0% fuel cladding failures and 2.14% fuel melt. The radiological consequences for this event have been analyzed and are bounded by the main steam line break event. The RCS overpressure and Reactor Building overpressure acceptance limits are also not challenged for this event. The results of the analysis of the four pump coastdown event assuming a total failure of the RPS/ESPS show that the plant response meets all acceptance limits. This is a Category 4 event.

Two Pump Coastdown

The trip of two reactor coolant pumps causes an immediate decrease in flow (Figure 10-8) and an increase in moderator and fuel temperature. The ICS responds to the decrease in flow by initially inserting control rods, and then withdrawing control rods. The thermal feedback and the insertion of the control rods adds negative reactivity initially, and core power decreases (Figure 10-9). Then the ICS withdraws rods and power increases. RPS trip setpoints for flux/flow/imbalance, high temperature, and variable pressure/temperature are exceeded, but the assumed failure prevents reactor trip. The runback under the control of the ICS is successful in preventing a reactor trip, and unit conditions stabilize. The normalized core heat flux, core outlet pressure, core inlet temperature, and core flow are shown in Figure 10-10.

VIPRE is used to determine the set of core peaking factors at which the DNBR limit will be exceeded at the limiting statepoint. These peaking factor limit curves are then used in SIMULATE to analyze the pin census for the percent of fuel rods failing the DNBR limit. The percent of fuel pins that exceeds the centerline fuel melt limit is also calculated. The results of the SIMULATE pin census is 26.6% fuel cladding failures and 2.46% fuel melt.

The radiological consequences for this event are as follows:

Location	Loss of Flow Dose	RG 1.183 Limit
EAB Boundary	2.0 rem TEDE	2.5 rem TEDE
LPZ Boundary	0.4 rem TEDE	2.5 rem TEDE
Control Room	1.2 rem TEDE	5 rem TEDE

The radiological consequences meet the Regulatory Guide 1.183 limits. The RCS overpressure and Reactor Building overpressure acceptance limits are not challenged for this event. The results of the analysis of the two pump coastdown event assuming a total failure of the RPS/ESPS show that the plant response meets all acceptance limits. This is a Category 4 event.

10.5 Locked Rotor

The UFSAR Section 15.6 locked rotor accident analysis, assuming a software common mode failure of the digital RPS, requires thermal-hydraulic analysis to determine the plant response. The results of the RETRAN-3D analysis are as follows, and are shown in Figures 10-11 through 10-13. The seizure of one reactor coolant pump shaft causes an immediate step-change decrease in flow (Figure 10-11) and an increase in moderator and fuel temperature. The ICS responds to the decrease in flow by inserting control rods. The thermal feedback and the insertion of the control rods adds negative reactivity initially, and core power decreases and stabilizes (Figure 3-12). The RPS trip setpoint for flux/flow/imbalance is exceeded, but the assumed failure prevents reactor trip. The runback under the control of the ICS is successful in preventing a reactor trip, and unit conditions stabilize. The normalized core heat flux, core outlet pressure, core inlet temperature, and core flow were determined (Figure 10-13) and used as input to the VIPRE-01 code to determine the transient minimum DNBR.

VIPRE is used to determine the set of core peaking factors at which the DNBR limit will be exceeded at the limiting statepoint. These peaking factor limit curves are then used in SIMULATE to analyze the pin census for the percent of fuel rods failing the DNBR limit. The percent of fuel pins that exceeds the centerline fuel melt limit is also calculated. The result of the SIMULATE pin census is no fuel cladding failures and no fuel melt. Consequently, the radiological consequences for this event would not be significant and are not analyzed. The RCS overpressure and Reactor Building overpressure acceptance limits are also not challenged for this event. The results of the analysis of the locked rotor accident assuming a total failure of the RPS/ESPS show that the plant response meets all acceptance limits. This is a Category 4 event.

10.6 Dropped Control Rod

The UFSAR Section 15.7 dropped rod analysis does not rely on an automatic reactor trip by the RPS or an actuation of the ESPS. Therefore, the assumed SWCMF of the digital RPS/ESPS has no impact on the plant transient response. This is a Category 1 event.

10.7 Turbine Trip

The UFSAR Section 15.8 turbine trip analysis, assuming a software common mode failure of the digital RPS, will be successfully mitigated by the Diverse Scram System. No actuation of the ESPS is required. The reactor will be shut down and no significant adverse consequences will result. This is a Category 2 event.

10.8 Steam Generator Tube Rupture

The UFSAR Section 15.9 steam generator tube rupture analysis does not rely on an automatic reactor trip by the RPS or an automatic actuation of the ESPS to mitigate this event. Therefore, the assumed SWCMF of the digital RPS/ESPS has no impact on the plant transient response. This is a Category 1 event.

10.9 Control Rod Ejection

The UFSAR Section 15.12 rod ejection accident analysis power excursion, assuming a software common mode failure of the digital RPS, will be successfully mitigated by the Diverse Scram System. Due to the assumed failure of the digital ESPS, manual actuation of the HPIS (5 minutes), RBCS (8 minutes) and RBS (8 minutes) will be required to provide emergency core cooling and containment heat removal. The radiological consequences of this event are bounded by the LBLOCA dose analysis results (Reference 26). This is a Category 3 event.

10.10 Large Steam Line Break

The UFSAR Section 15.13 steam line break accident analysis, assuming a software common mode failure of the digital RPS, requires thermal-hydraulic analysis to determine the plant response. The results of the RETRAN-3D analysis are as follows, and are shown in Figures 10-14 through 10-18. The rupture of the main steam line causes an immediate decrease in steam generator pressure (Figure 10-14) and a decrease in RCS temperature and pressure. The ICS responds to the decrease in temperature by withdrawing control rods. The thermal feedback and the withdrawal of the control rods adds positive reactivity and core power increases (Figure 10-15). The Automatic Feedwater Isolation System (AFIS) isolates main feedwater (MFW) and emergency feedwater (EFW) to the affected steam generator on low steam generator pressure at 550 psig (16.1 seconds), which actuates the AMSAC function and trips the turbine at 30.4 seconds. The RPS trip setpoints for variable pressure/temperature, low pressure, high power, flux/flow/imbalance, and reactor trip on turbine trip are exceeded, but the assumed failure prevents reactor trip. The isolation of MFW with the reactor still at power causes the RCS to heat up (Figure 10-16) and pressurize, and a DSS actuation on high pressure occurs at 35.6 seconds. The normalized core heat flux, core outlet pressure, core inlet temperature, and core flow are shown in Figure 10-17. These are input to the VIPRE-01 code to determine the transient minimum DNBR.

VIPRE is used to determine the set of core peaking factors at which the DNBR limit will be exceeded at the limiting statepoint. These peaking factor limit curves are then used in SIMULATE to analyze the pin census for the percent of fuel rods failing the DNBR limit. The percent of fuel pins that exceeds the centerline fuel melt limit is also calculated. The result of the SIMULATE pin census is 34.0% fuel cladding failures and 4.75% fuel melt.

The radiological consequences for this event are as follows:

Location	Main Steam Line Break Dose	RG 1.183 Limit
EAB Boundary	4.4 rem TEDE	25 rem TEDE
LPZ Boundary	0.9 rem TEDE	25 rem TEDE
Control Room	3.4 rem TEDE	5 rem TEDE

The radiological consequences meet the Regulatory Guide 1.183 limits. The steam line break also causes a mass and energy release into the Reactor Building. The release is terminated when the AFIS isolates all MFW and EFW to the faulted steam generator, and it boils dry. The operator is assumed to manually start the RBCS and RBS at 8 minutes; however this action is not required to terminate the pressurization of the Reactor Building. The containment pressure results are shown in Figure 10-18. The peak containment pressure is 44 psig, which is well below the acceptance limit of 125 psig. The RCS overpressure limit is also not challenged for this event. The results of the analysis of the large steam line break accident assuming a total failure of the RPS/ESPS show that the plant response meets all acceptance limits. This is a Category 4 event.

10.11 Small Steam Line Break

The UFSAR Section 15.17 small steam line break accident does not rely on an automatic reactor trip by the RPS or an automatic actuation of the HPIS by the ESPS. The limiting statepoint in the analysis occurs with the reactor stabilized at an elevated power level. The operator is then credited with tripping the reactor and controlling the post-trip conditions. The assumed SWCMF of the digital RPS/ESPS has a beneficial effect since the ICS controls the plant to less limiting conditions. The small steam line break does cause a mass and energy release into the Reactor Building. For larger break sizes the release is terminated when the AFIS isolates all MFW and EFW to the faulted steam generator, and it boils dry. For smaller break sizes the release is terminated manually by the operator at 10 minutes. The larger break size is more limiting in that the Reactor Building pressure result is higher. For the assumed RPS/ESPS failure, the operator is assumed to manually start the RBCS and RBS at 8 minutes; however this action is not required to terminate the pressurization of the Reactor Building. The containment pressure results are shown in Figure 10-19. The results of the containment analysis of the small steam line break accident assuming a total failure of the RPS/ESPS show the peak pressure is 45 psig, which is well below the acceptance limit of 125 psig. This is a Category 1 event for the RCS response, and a Category 4 event for the containment response.

10.12 Small-Break LOCA

The UFSAR Section 15.14 small break LOCA accident analysis, assuming a software common mode failure of the digital RPS, requires thermal-hydraulic analysis to determine the plant response. The SBLOCA analysis is performed by FANP using the RELAP5/MOD2-B&W code. The following assumptions are made consistent with the intent of BTP HICB-19, which allows realistic assumptions for this application:

- Core flood tanks at nominal pressure and liquid volume
- Core axial peaking factor = 1.17
- Core radial peaking factor = 1.6
- Three HPI pumps available
- Both LPI pumps available
- ICS assumed to withdraw control rods

The limiting small break LOCA was determined to be located at the core flood tank (CFT) nozzle. This break size (0.44 ft^2) is large enough to rapidly deplete the RCS inventory, and also results in spillage of the inventory of one CFT. Consequently, only one CFT remains available for ECCS injection until credit for manual ESPS actuation (HPIS & LPIS) by the operator at 5 minutes.

The opening of the break results in a rapid RCS inventory loss and depressurization. The low hot leg pressure reactor trip and ESPS setpoints, and the high Reactor Building pressure ESPS setpoints are exceeded, but the reactor does not trip and the engineered safeguards do not actuate due to the assumed failure. The ICS is assumed to withdraw control rods in an attempt to maintain full reactor power. The reactor is manually tripped by the operator at 2 minutes. The reactor coolant pumps are tripped immediately following reactor trip. Core uncovering begins at 160 seconds, just prior to injection from the intact CFT. The HPIS and LPIS are manually started at 5 minutes. The core heatup is limited to around 1000°F cladding temperature. Adequate core cooling is restored when HPIS and LPIS flow starts. These results indicate that the 10 CFR 50.46 acceptance criteria for LOCA are met, and therefore the assumed operator action times for RPS and ESPS actuation are acceptable. The proposed alternate source term radiological consequences for the large break LOCA presented in UFSAR Chapter 15, currently under review by the NRC, continue to bound the small break LOCA.

The small break LOCA also causes a mass and energy release into the Reactor Building. The containment response is bounded by the large break LOCA presented in UFSAR Chapter 15. The RCS overpressure limit is also not challenged for this event. The results of the analysis of the small break LOCA accident assuming a total failure of the RPS/ESPS show that the plant response meets all acceptance limits. This is a Category 4 event for the RCS response, and a Category 3 event for the containment response.

10.13 Large-Break LOCA

For a LBLOCA, Section 4 of BTP HICB-19 notes: "I&C system vulnerability to common mode failure affecting the response to large-break loss-of-coolant accidents and main steam line breaks has been accepted in the past. This acceptance was based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs."

Duke's analysis of the LBLOCA coincident with a SWCMF identified a plant vulnerability. The analysis concluded that the operator response time for manually actuating the ESPS (HPIS and LPIS at 5 minutes) would not be successful in maintaining the core in a coolable geometry. However, the LBLOCA coincident with a SWCMF event has a very low probability of occurrence and operators have indications of small leaks before a catastrophic failure occurs. In accordance with the BTP guidance, credit can be taken for leak detection capability to eliminate the LBLOCA as an event to be analyzed for the postulated SWCMF

The ONS RCS design and RCS leak detection capabilities provide ample justification for eliminating the LBLOCA from consideration for the SWCMF analyses. The size of the break for the loss of coolant accident will be limited due to these ONS design considerations as discussed below. The RCS has been designed and constructed so as to have an exceedingly low probability of gross rupture or significant leakage throughout its design lifetime. The RCS pressure boundary meets the following criteria:

- Material selection, design, fabrication, inspection, testing and certification in accordance with ASME codes for components excluding piping, which is done in accordance with the USAS B31.1 and B31.7 codes.
- Manufacture and erection in accordance with approved procedures.
- Inspection in accordance with code requirements plus additional requirements imposed by the manufacturer.
- System analysis to account for cyclic effects of thermal transients, mechanical shock, seismic loadings, and vibratory loadings.
- Selection of reactor vessel material properties to give due consideration to neutron flux effects and the resultant increase of the nil ductility transition temperature.

The ONS leak detection system is capable of detecting any unidentified leakage above a certain threshold and follows the guidance presented in Regulatory Guide 1.45 (Reference 28). The entire ONS Reactor Coolant System (RCS) is located within the secondary shielding and is inaccessible during reactor operation. Any leakage will drain to the Reactor Building normal sump. Any coolant leakage to the atmosphere will be in the form of fluid and vapor. The fluid will drain to the sump and the vapor will be condensed in the Reactor Building coolers and also reach the sump via a drain line from the cooler.

Reactor Coolant System pressure boundary integrity is continuously monitored in the control room by surveillance of variation from normal conditions for the following:

- Reactor Building temperature and sump level.
- Reactor Building radioactivity levels.
- Condensor off-gas radioactivity levels.
- Decreasing letdown storage tank water level (indicating system leakage).

Gross leakage from the reactor coolant boundary will also be indicated by a decrease in pressurizer water level and a rapid increase in the Reactor Building sump water level. The sump fill rate is also monitored. An On-Demand RCS leakage calculation is also available should the operator suspect a leak. This leakage calculation is also required to be performed every 72 hours by Technical Specification Surveillance Requirement (SR) 3.4.13.1.

RCS leakage rate is determined by comparing instrument indications of reactor coolant average temperature, pressurizer water level and letdown storage tank water level over a certain time interval. All of these indications are recorded at ONS. RCS leak detection is also provided by monitoring the Reactor Building Sump level and letdown storage tank level. Since the pressurizer

level controller maintains a constant pressurizer level, any RCS volume change due to a leakage would manifest itself as a Reactor Building sump level change and/or a corresponding letdown storage tank level change.

A reactor building sump level transmitter is used to satisfy the requirements of Technical Specification 3.4.15, RCS Leakage Detection Instrumentation." Alarm indication in the control room for the Reactor Building sump is provided at a low level of 6 inches of water and a high level of 15 inches of water. For the Letdown Storage Tank, alarm indication is provided at a low level of 60 inches of water and a high level of 90 inches of water. Considering the most adverse initial conditions of a low level in the sump and a high level in the storage tank, a 1-gpm leak from the RCS would initiate a sump high-level alarm indication in the control room within 3 hours and a storage tank low-level alarm indication in the control room within 17 hours. These detection times would be reduced by approximately one half when using realistic assumptions. For this case it would be assumed that the sump level and the storage tank level are at least at mid-level. Therefore, the sump alarm timing would be reduced to approximately 90 minutes for a 1gpm leak and 30 minutes for a 3gpm leak.

If the RCS leak allows primary coolant into the containment atmosphere, additional leak detection is provided by the Reactor Building Process Monitoring System and the Reactor Building Area Monitoring system. These radiation detectors have extended ranges to cover anticipated levels during normal operation, transient and accident conditions. They are also shielded against expected background radiation levels. These detectors are required by Technical Specifications that include surveillance requirements to demonstrate detector operability. The sensitivity and time for detection of a RCS leak by any of the radioactivity monitoring systems depends upon reactor coolant activity and the location of the leak. Alarm indication for each sample point in these systems is in the control room.

Class I fluid systems other than the RCS pressure boundary will be monitored for leakage by monitoring the various storage and/or surge tanks for the applicable systems. The Radiation Monitoring System for the station will aid in leak detection of systems containing radioactive fluids. In addition to the above, routine operator walkdowns performed each shift and Health Physics radiation surveillance will detect leakage in both radioactive and non-radioactive systems.

RCS leakage is controlled by Technical Specifications. No pressure boundary leakage is allowed that is indicative of material deterioration. Leakage of this type is unacceptable as the leak itself could cause further deterioration, resulting in a higher leakage rate. The limit allowed for this unidentified leakage is 1 gpm as the minimal detectable amount that the containment air monitoring and containment sump level monitoring equipment can detect within a reasonable period of time. This LCO is applicable in Modes 1, 2, 3 and 4. If the unidentified leakage is in excess of the LCO limit then the leakage must be reduced within four hours to an acceptable limit or the reactor must be shut down (Mode 3 within 12 hours and Mode 5 within 36 hours). These actions are discussed in Technical Specification Bases 3.4.13.

Therefore, the size of the break for the loss of coolant accident will be limited due to operator awareness/detection of the leak and all breaks will be classified as SBLOCAs. The leak detection capability at ONS is only one factor that lowers the likelihood of a large break occurrence. Another factor is the low probability of occurrence of a SWCMF concurrent with a LBLOCA, which is an ANSI IV event. The TXS System has proven dependability that significantly lowers the likelihood of a SWCMF. These are discussed in detail in Chapter 5 and 6 of this report but are summarized below:

- Development and quality assurance aspects of both the operational and application software
- Appropriate software standards
- Fault detection capability
- Failure management techniques
- Internal redundancy
- Diagnostic capabilities
- Maturity of the system (significant operating history) with an extremely low failure rate for hardware failures, where none have caused system inoperability, and no operational software failures
- Formal review by NRC resulting in TXS System approval.
- Extremely low probability of a simultaneous RPS and ESPS software failure

The defense-in-depth offered by the TXS system design and the ONS design leads to the conclusion that our design requirements offer sufficient capability to guard against a SWCMF and a LBLOCA from occurring in the first place. The reactor primary piping, the quality assurance during construction, periodic in-service inspection, the extremely low probability of a LBLOCA concurrent with the SWCMF and operation of qualified continuous leak detection systems all lower the likelihood of occurrence of a LBLOCA. Thus, Duke has concluded that sufficient defense-in-depth exists to prevent this event from occurring.

10.14 Loss of Main Feedwater

The UFSAR Section 10.4.7.1.1 loss of main feedwater transient analysis, assuming a SWCMF of the digital RPS, will be successfully mitigated by the Diverse Scram System. No actuation of the ESPS is required. The reactor will be shut down and no significant adverse consequences will result. This is a Category 2 event.

10.15 Loss of Offsite Power

The UFSAR Section 10.4.7.1.2 loss of offsite power transient analysis, assuming a SWCMF of the digital RPS, will be successfully mitigated by the Diverse Scram System. No actuation of the ESPS is required. The reactor will be shut down and no significant adverse consequences will result. This is a Category 2 event.

10.16 Main Feedwater Line Break

The UFSAR Section 10.4.7.1.7 main feedwater line break accident analysis, assuming a SWCMF of the digital RPS, will be successfully mitigated by the Diverse Scram System. No actuation of the ESPS is required. The reactor will be shut down and no significant adverse consequences will result. This is a Category 2 event.

FIGURE 10-1
CONTROL ROD BANK WITHDRAWAL - POWER

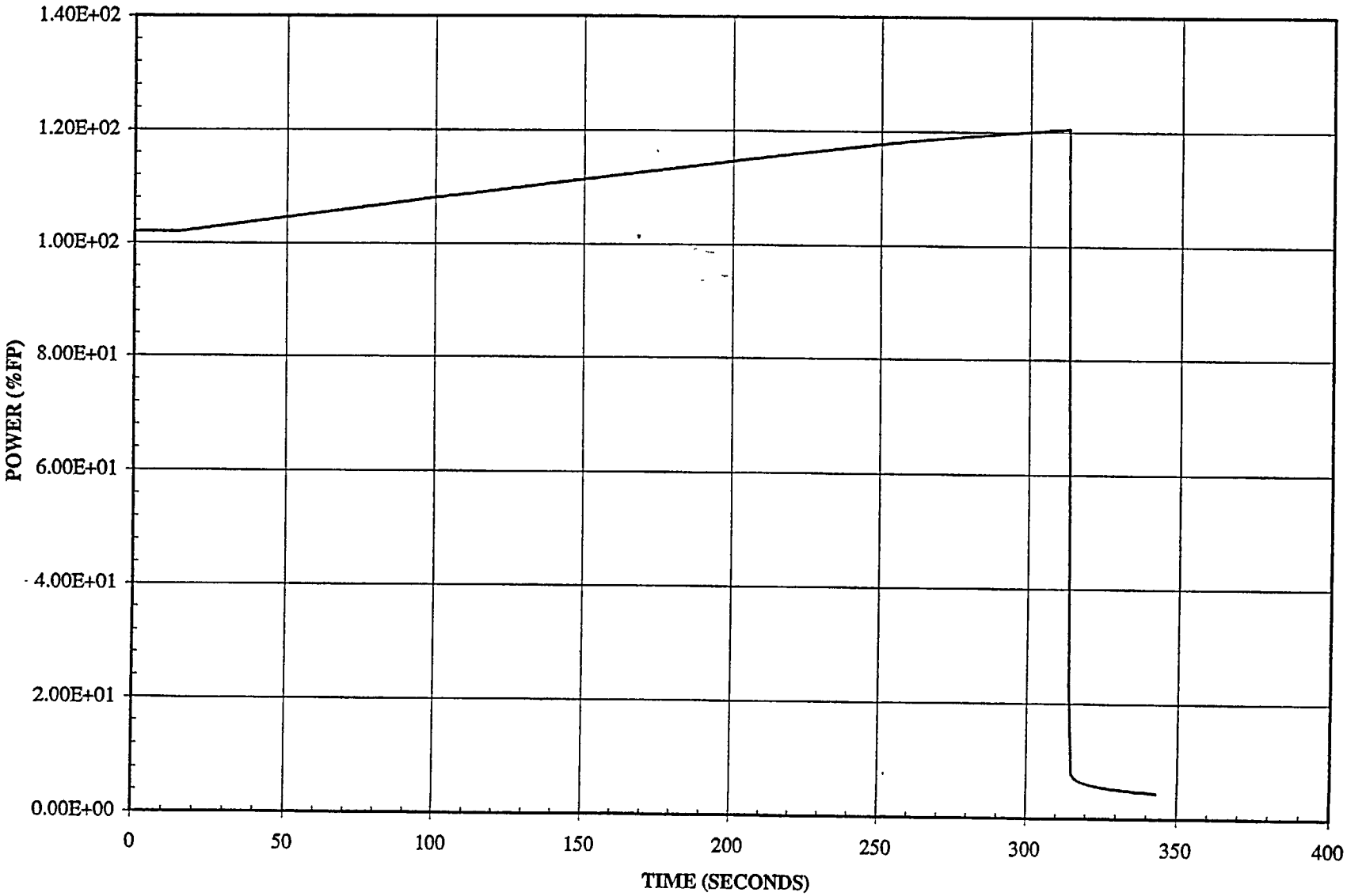


FIGURE 10-2
CONTROL ROD BANK WITHDRAWAL - PRESSURE

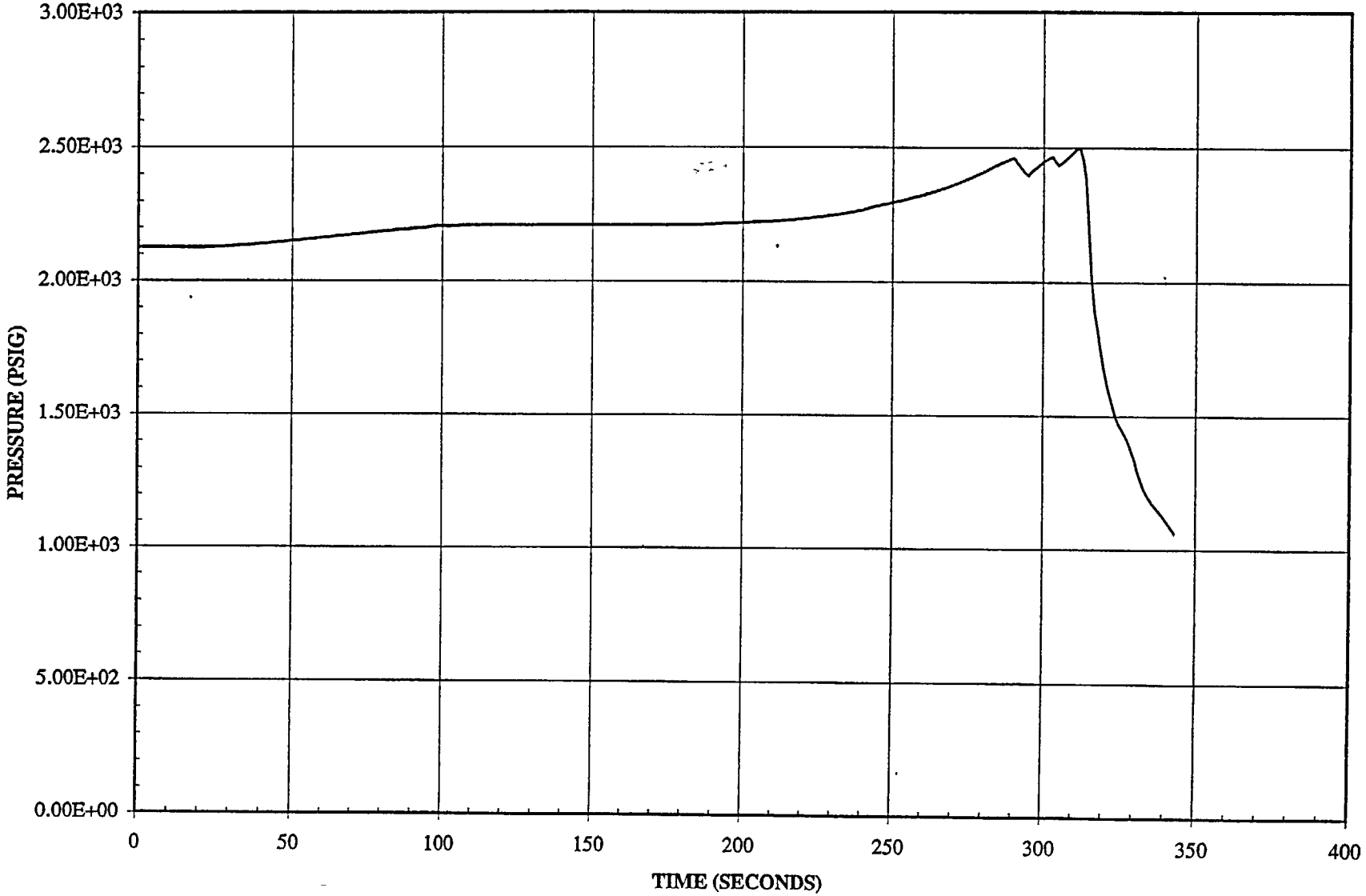


FIGURE 10-3
CONTROL ROD BANK WITHDRAWAL - HOT LEG TEMPERATURE

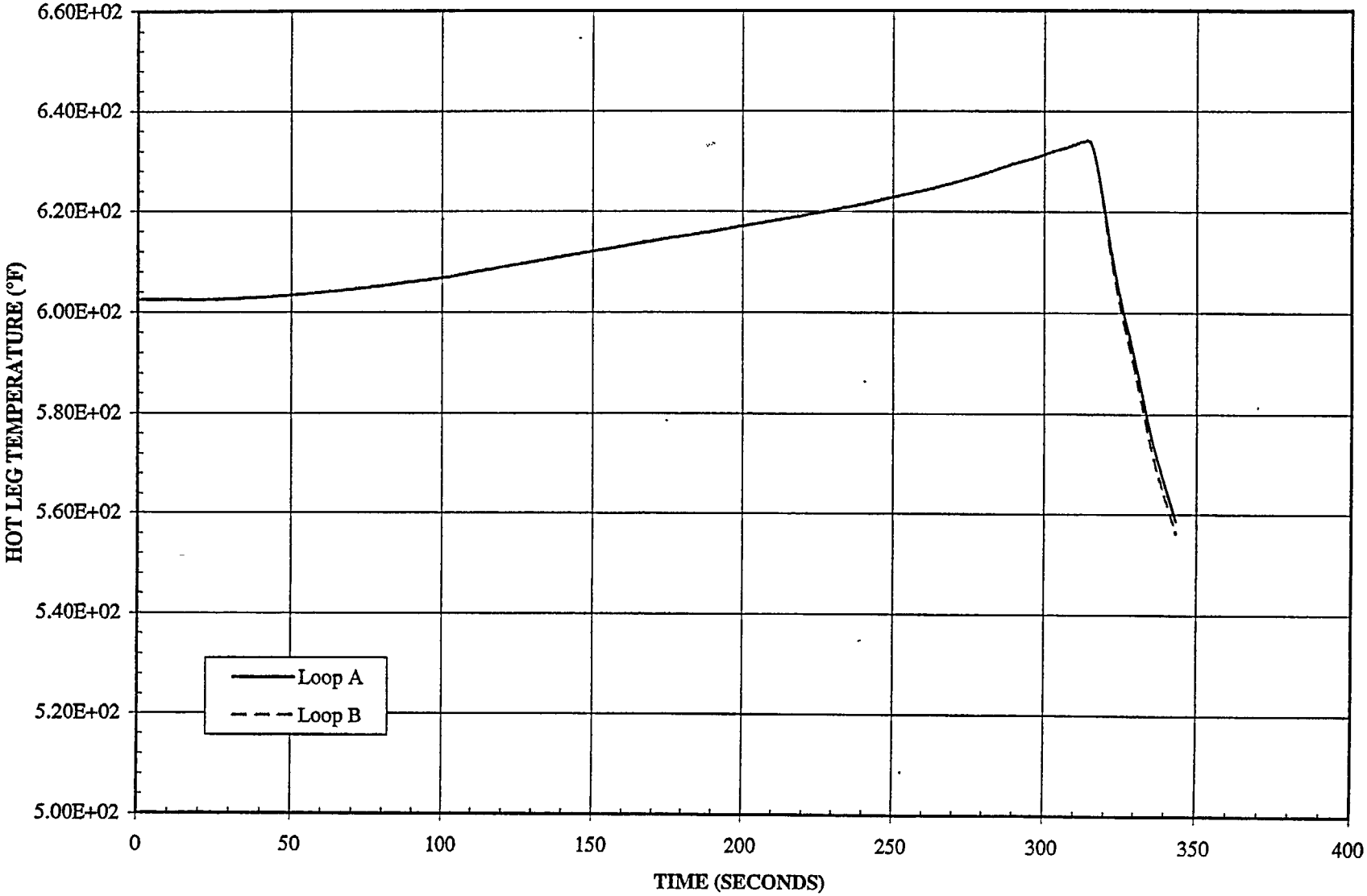


FIGURE 10-4
CONTROL ROD BANK WITHDRAWAL - NORMALIZED INPUTS TO VIPRE

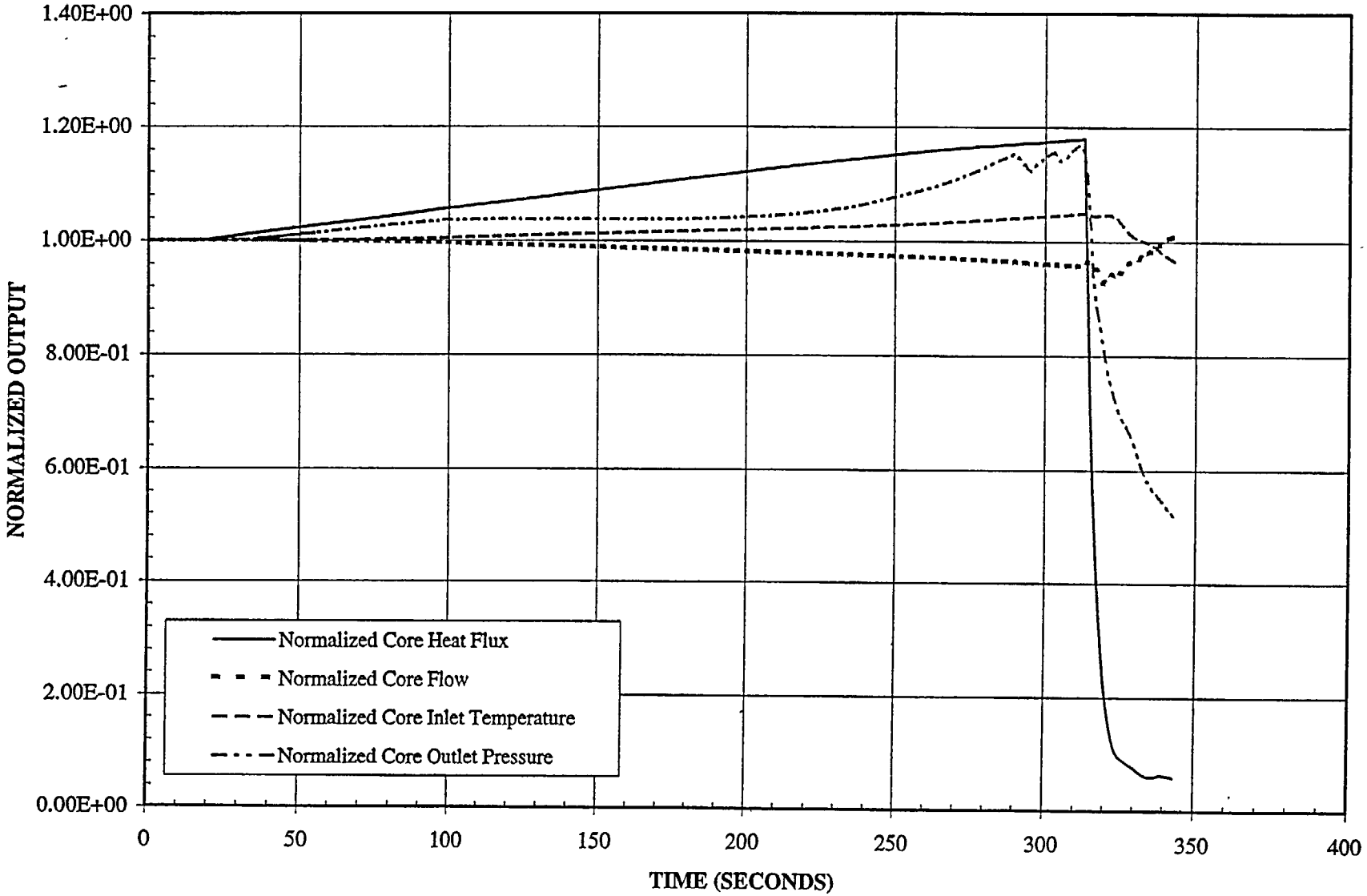


FIGURE 10-5
FOUR PUMP COASTDOWN - FLOW

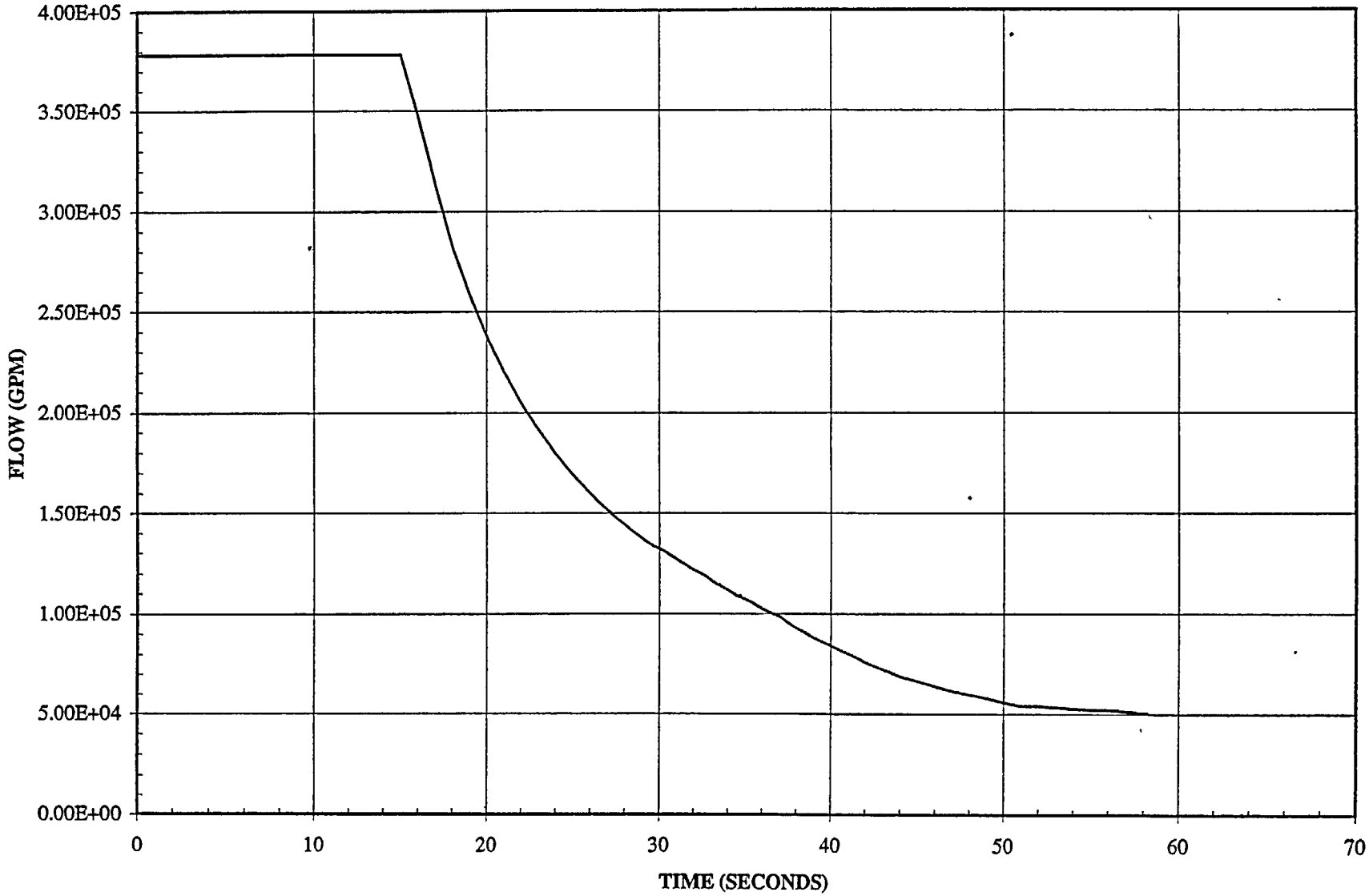


FIGURE 10-6
FOUR PUMP COASTDOWN - POWER

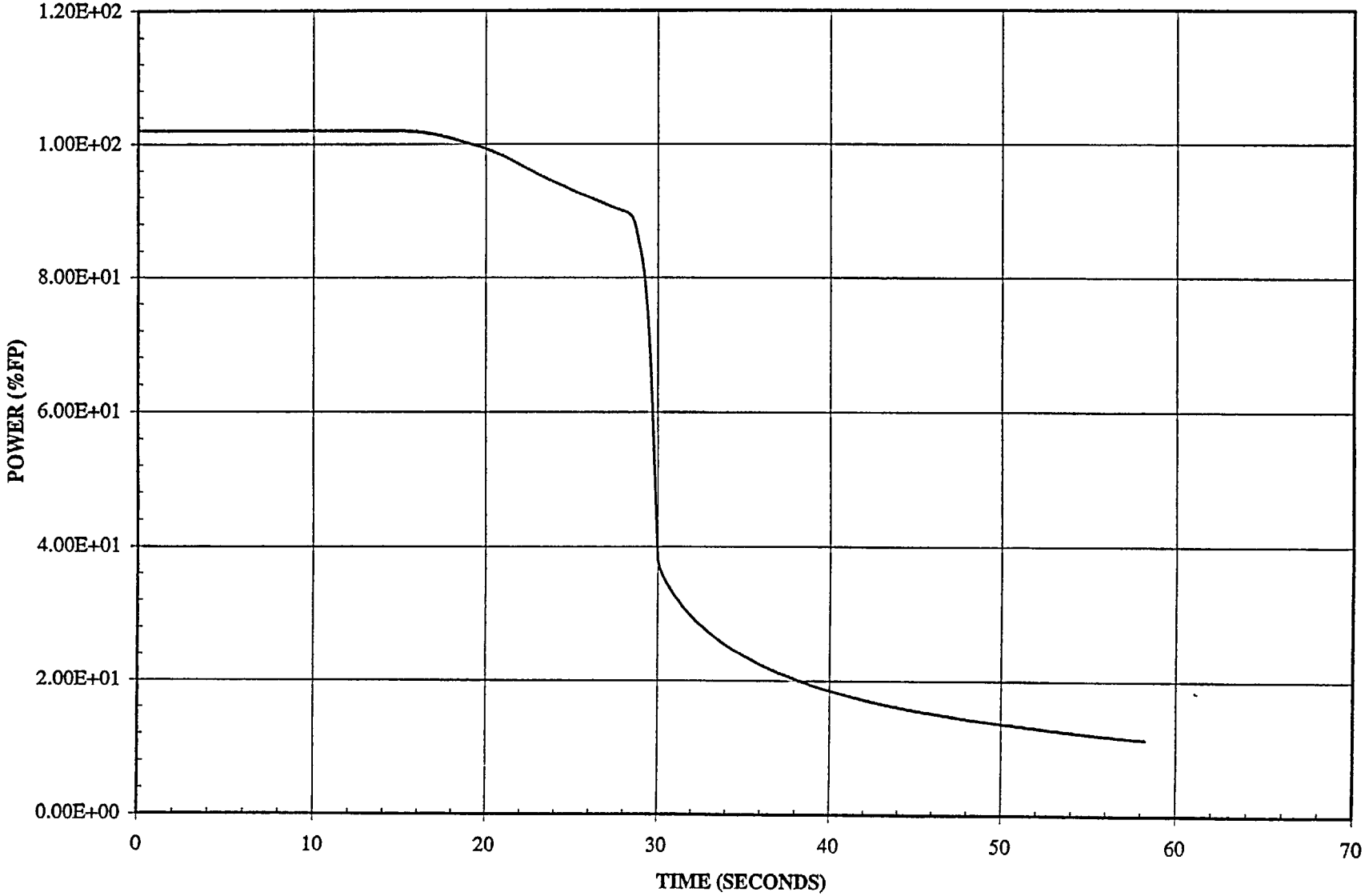


FIGURE 10-7

FOUR PUMP COASTDOWN - NORMALIZED INPUTS TO VIPRE

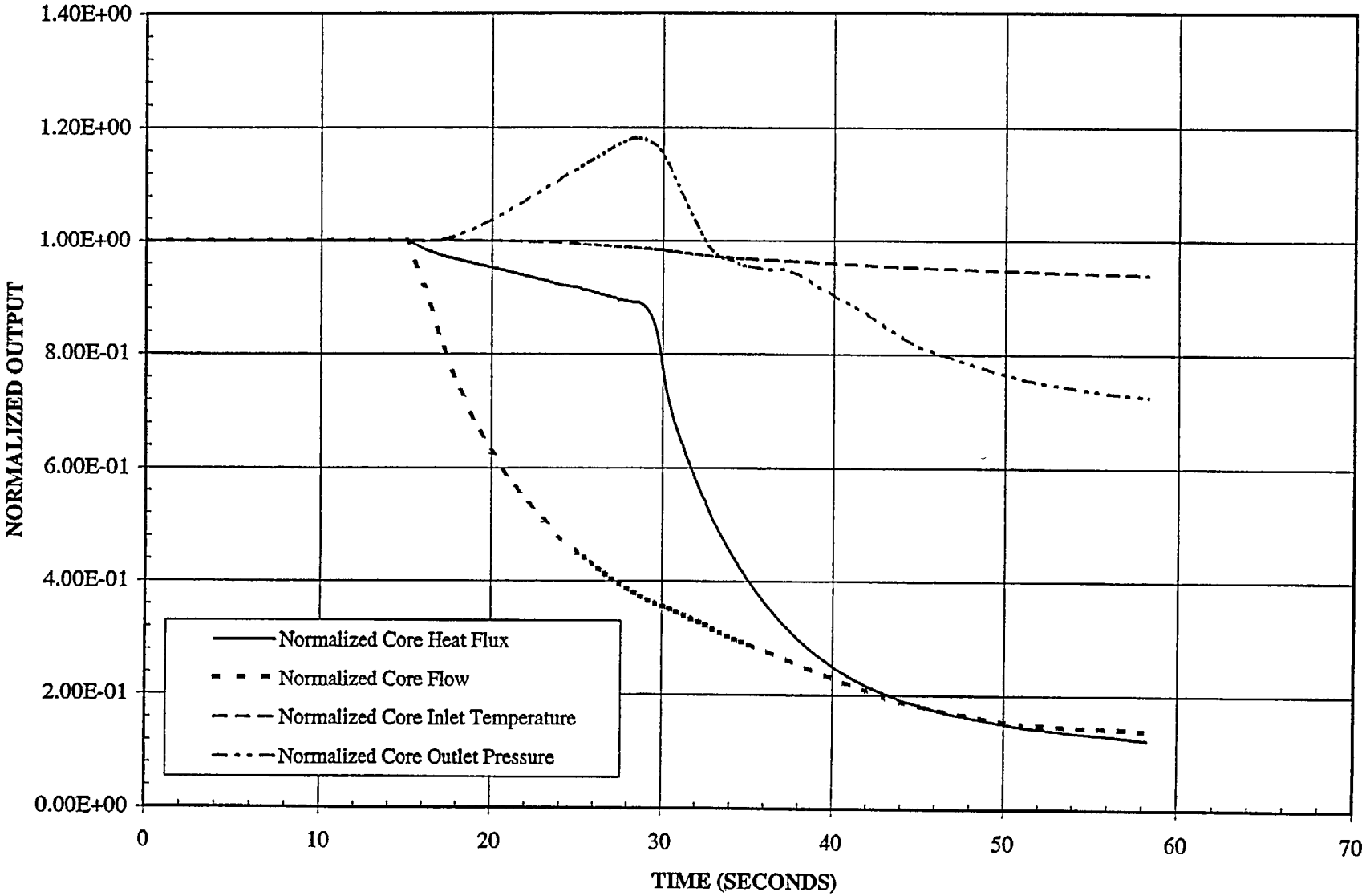


FIGURE 10-8

TWO PUMP COASTDOWN - FLOW

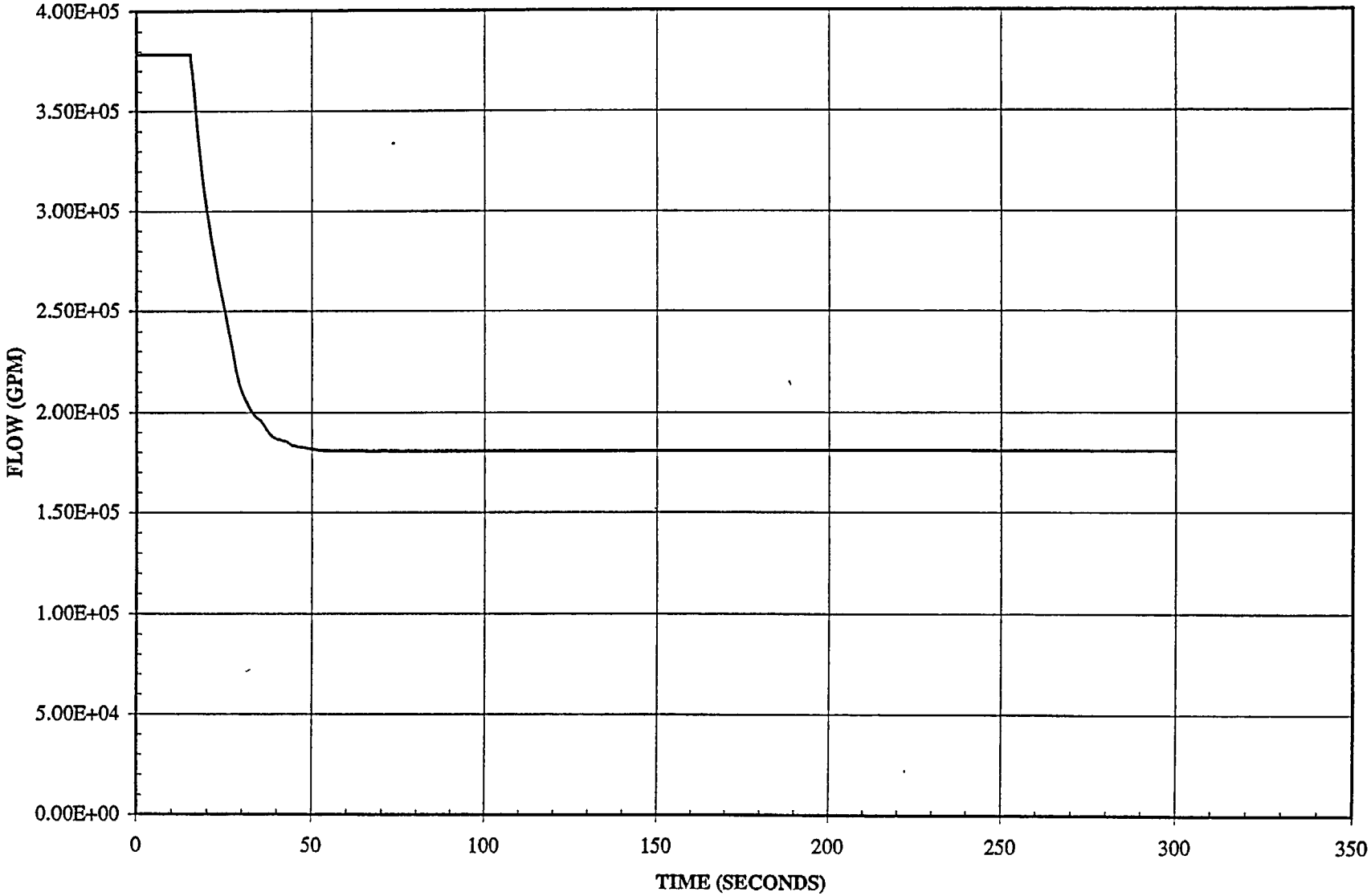


FIGURE 10-9
TWO PUMP COASTDOWN - POWER

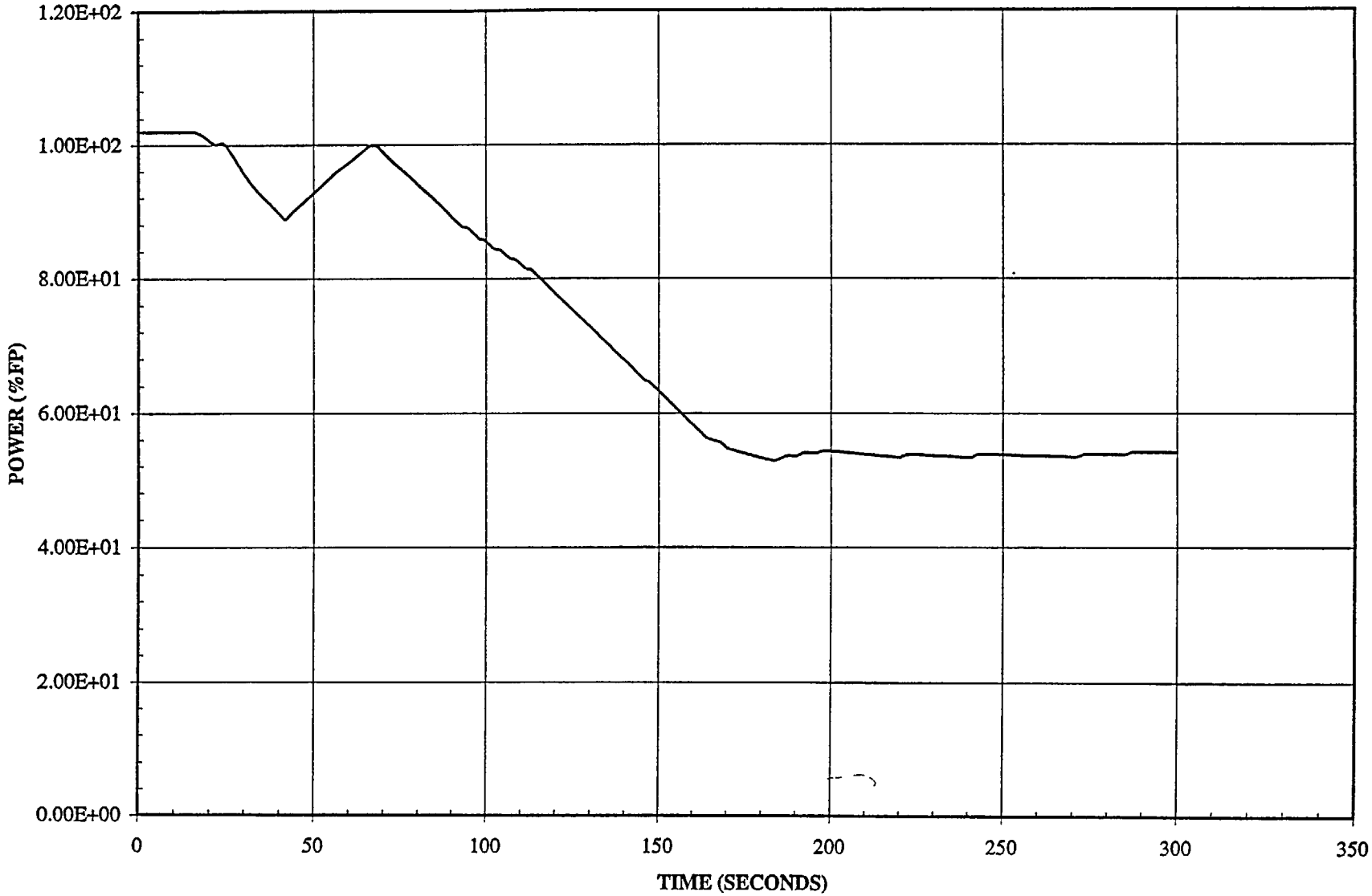


FIGURE 10-10
TWO PUMP COASTDOWN - NORMALIZED INPUTS TO VIPRE

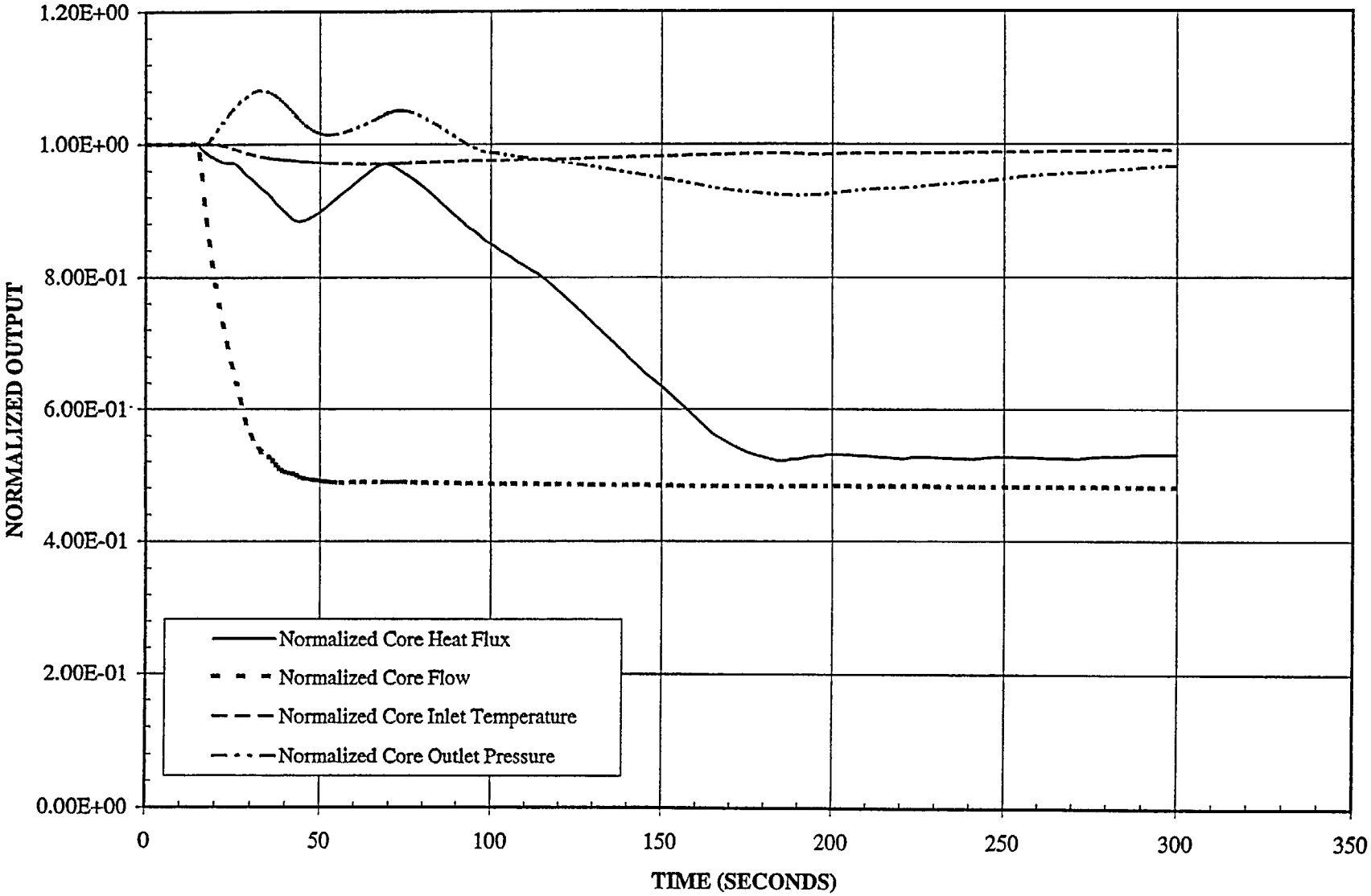


FIGURE 10-11
LOCKED ROTOR - FLOW

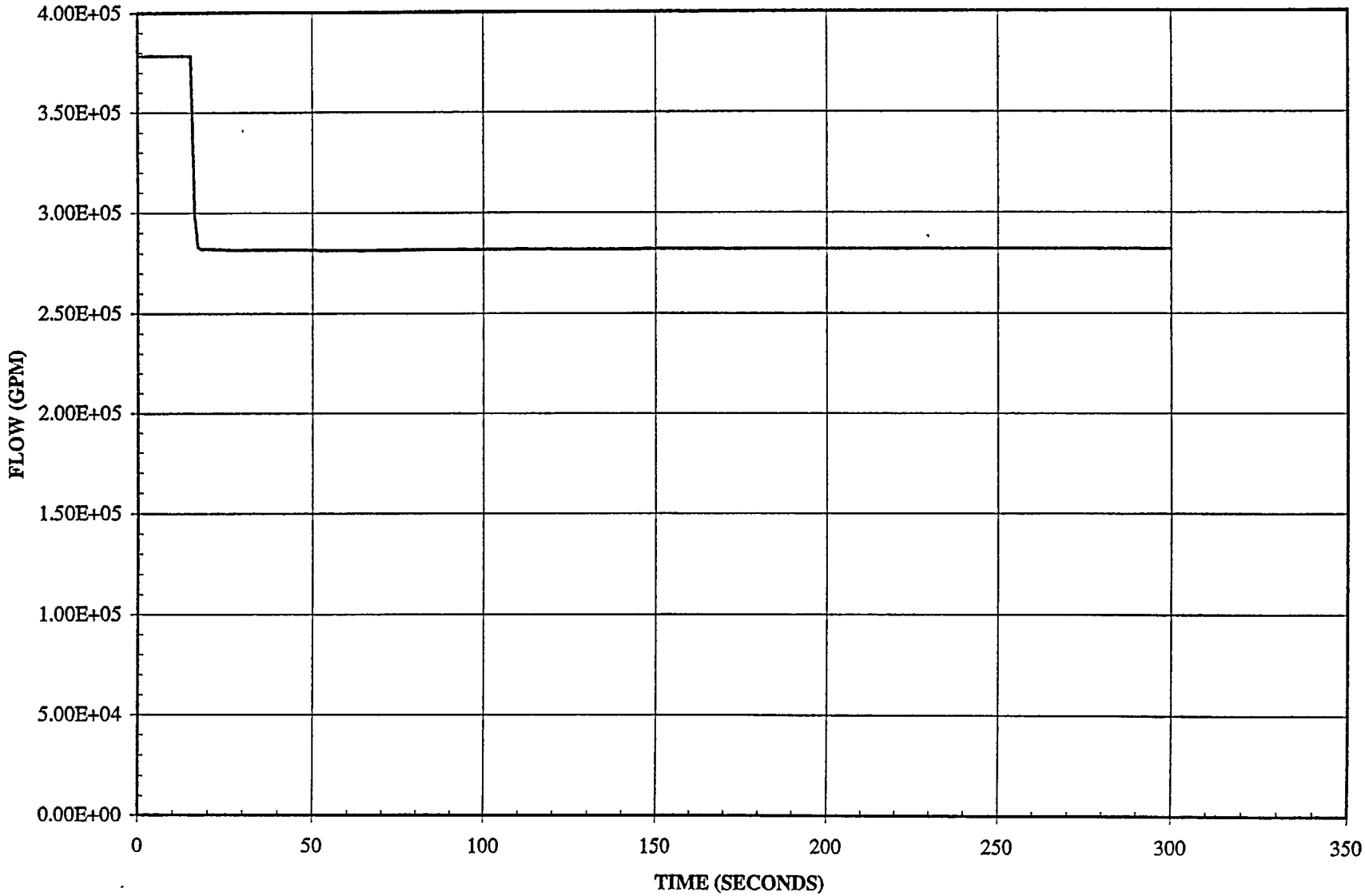


FIGURE 10-12
LOCKED ROTOR - POWER

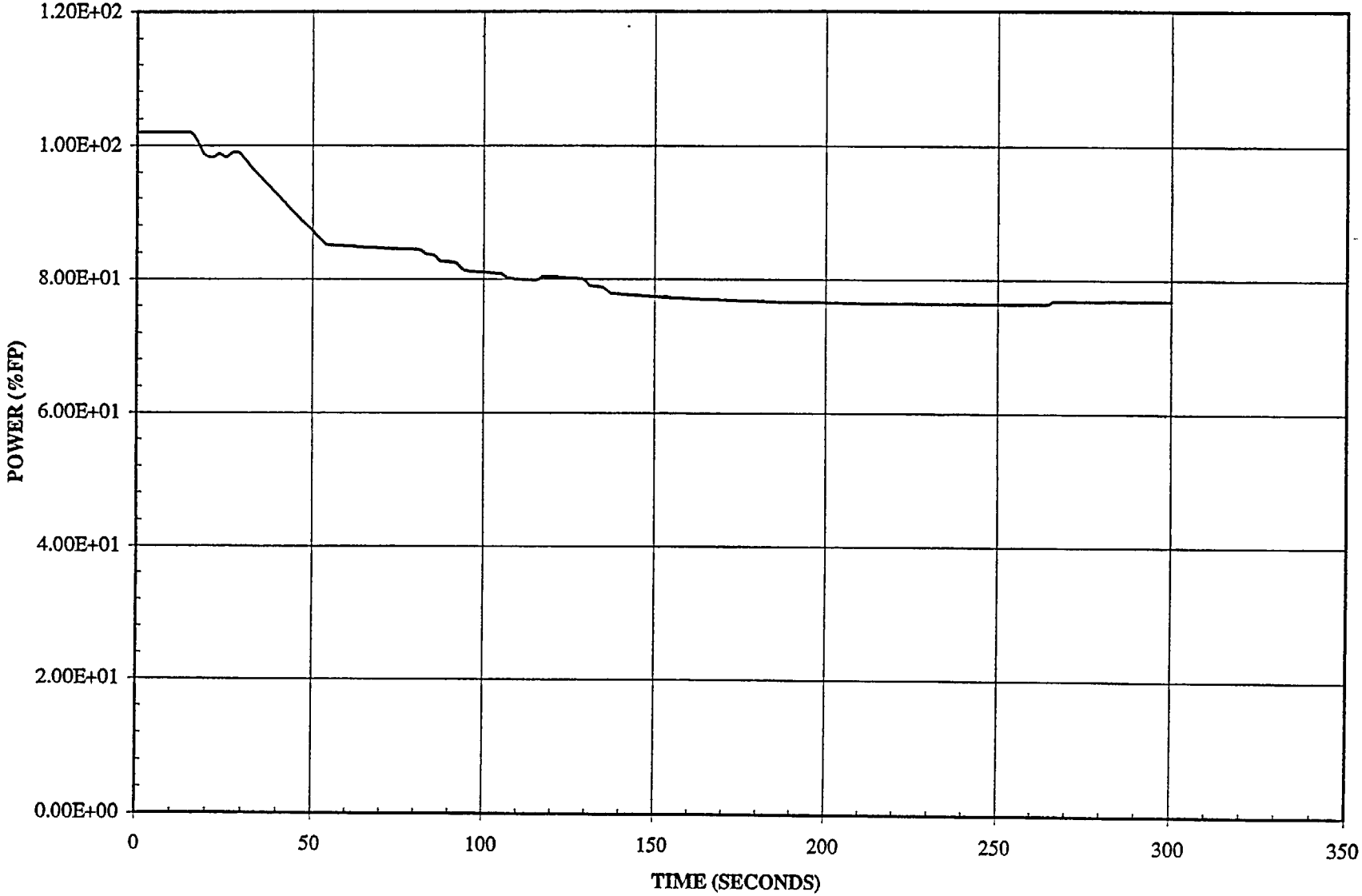


FIGURE 10-13
LOCKED ROTOR - NORMALIZED INPUTS TO VIPRE

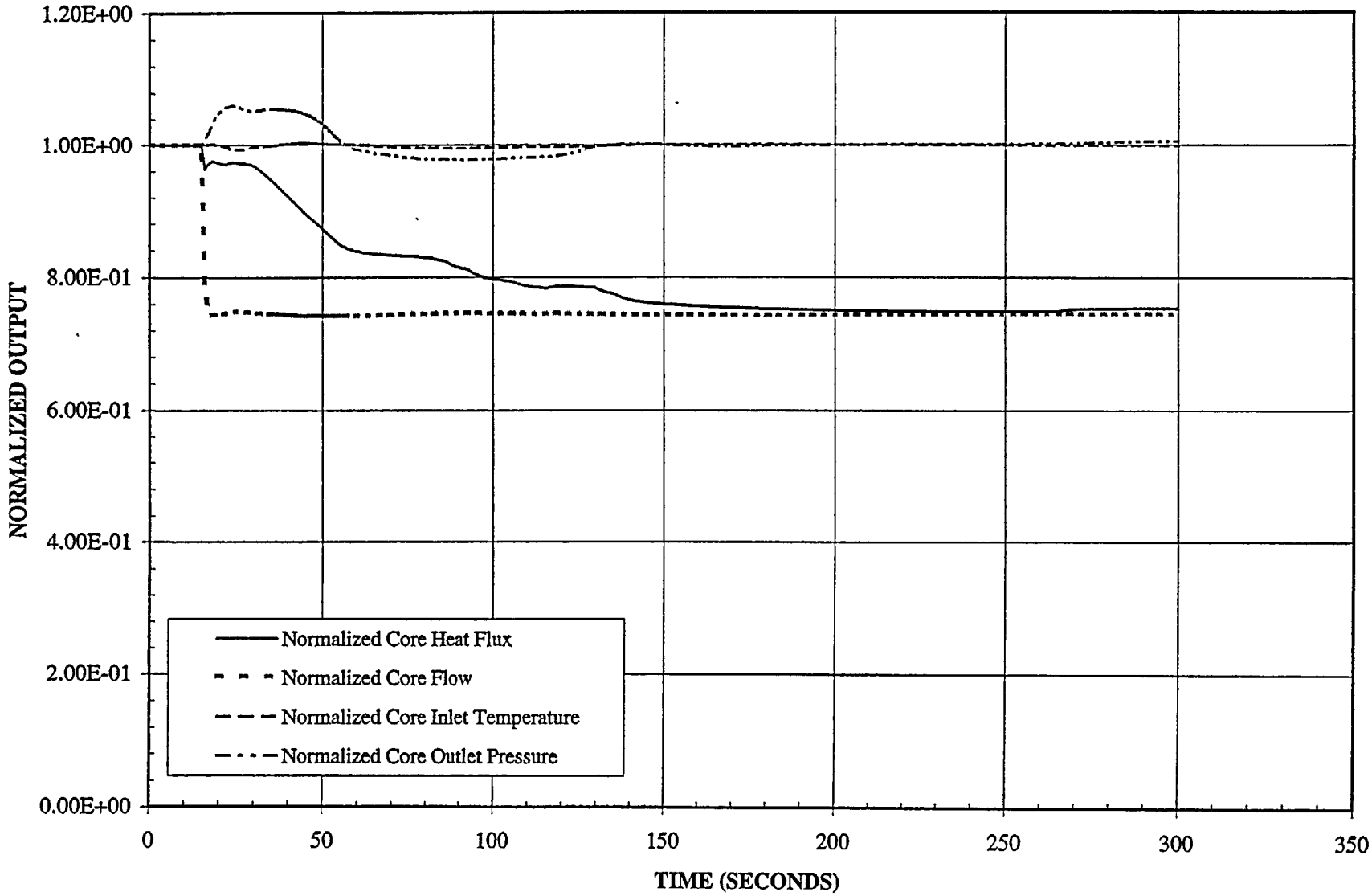


FIGURE 10-14

LARGE STEAM LINE BREAK - STEAM GENERATOR PRESSURE

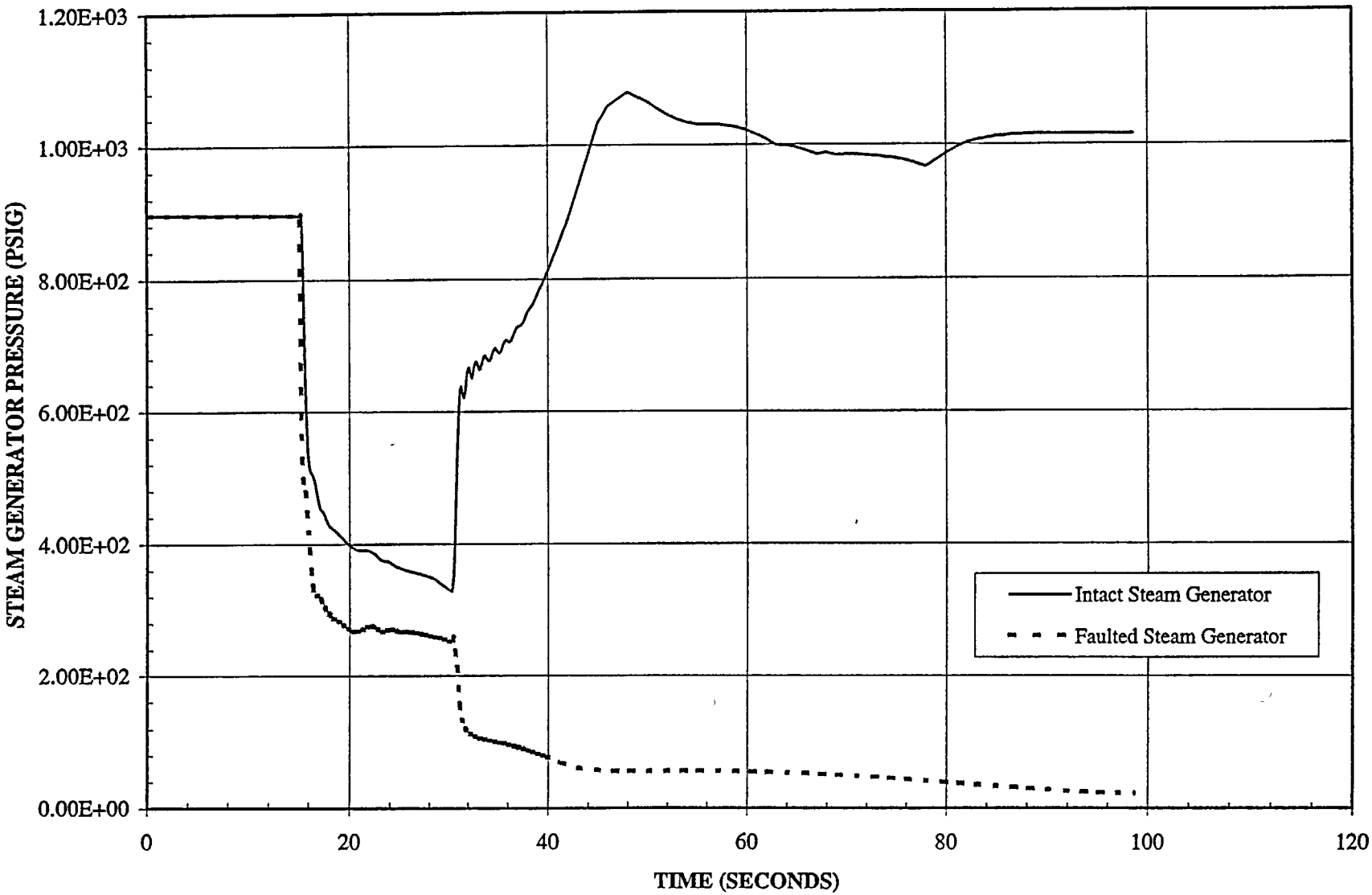


FIGURE 10-15
LARGE STEAM LINE BREAK - POWER

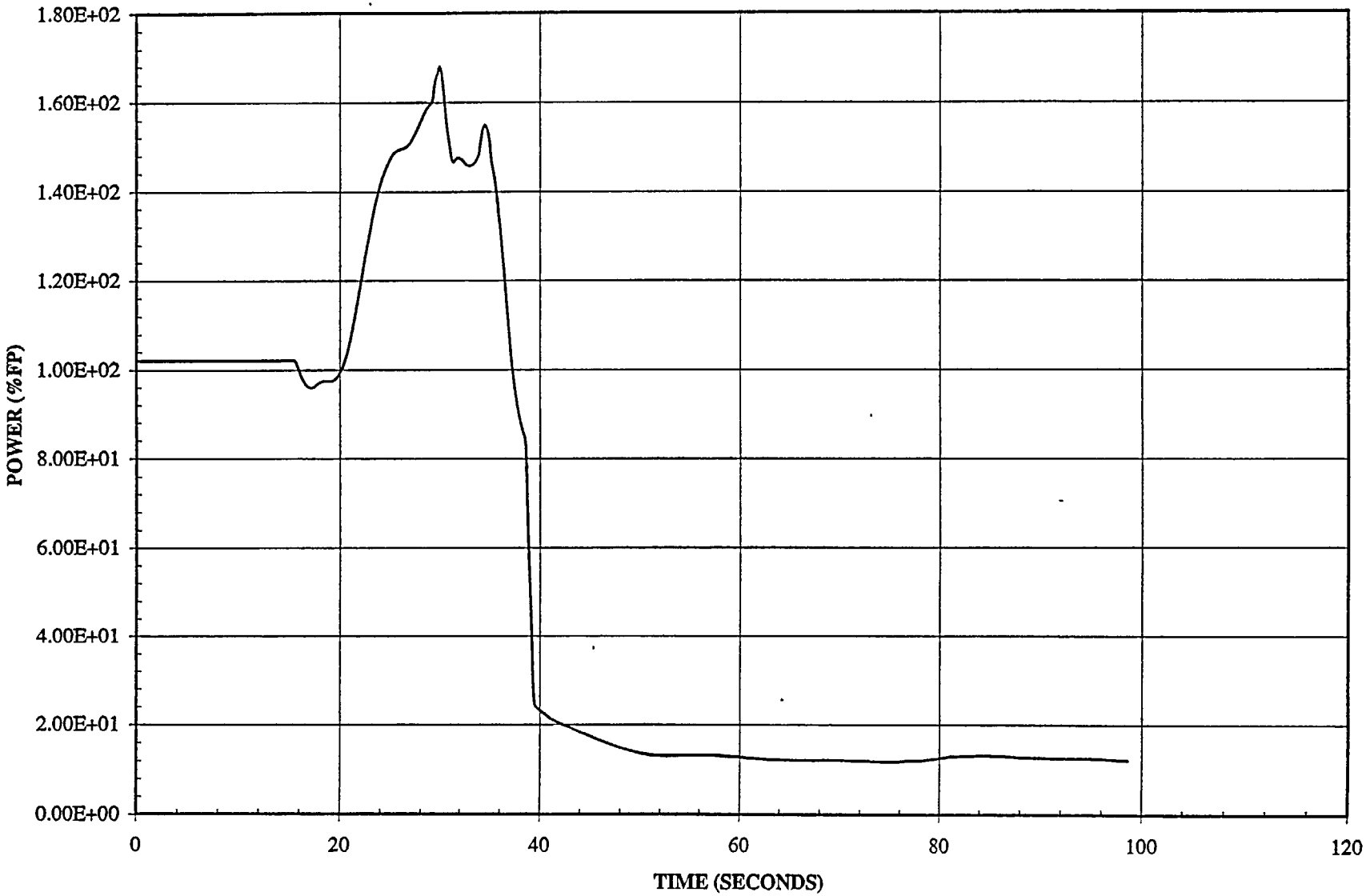


FIGURE 10-16

LARGE STEAM LINE BREAK - HOT LEG TEMPERATURE

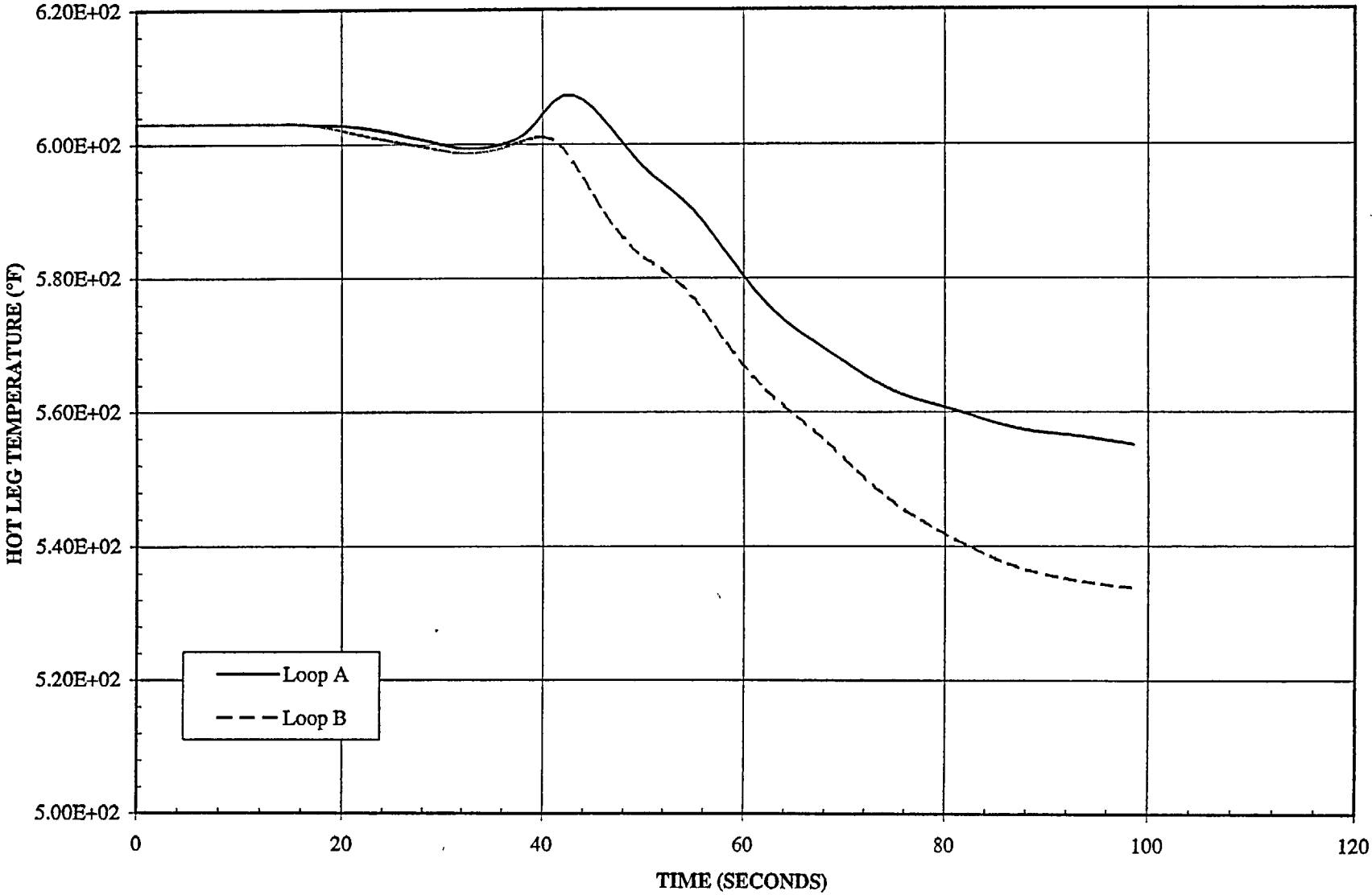


FIGURE 10-17

LARGE STEAM LINE BREAK - NORMALIZED INPUTS TO VIPRE

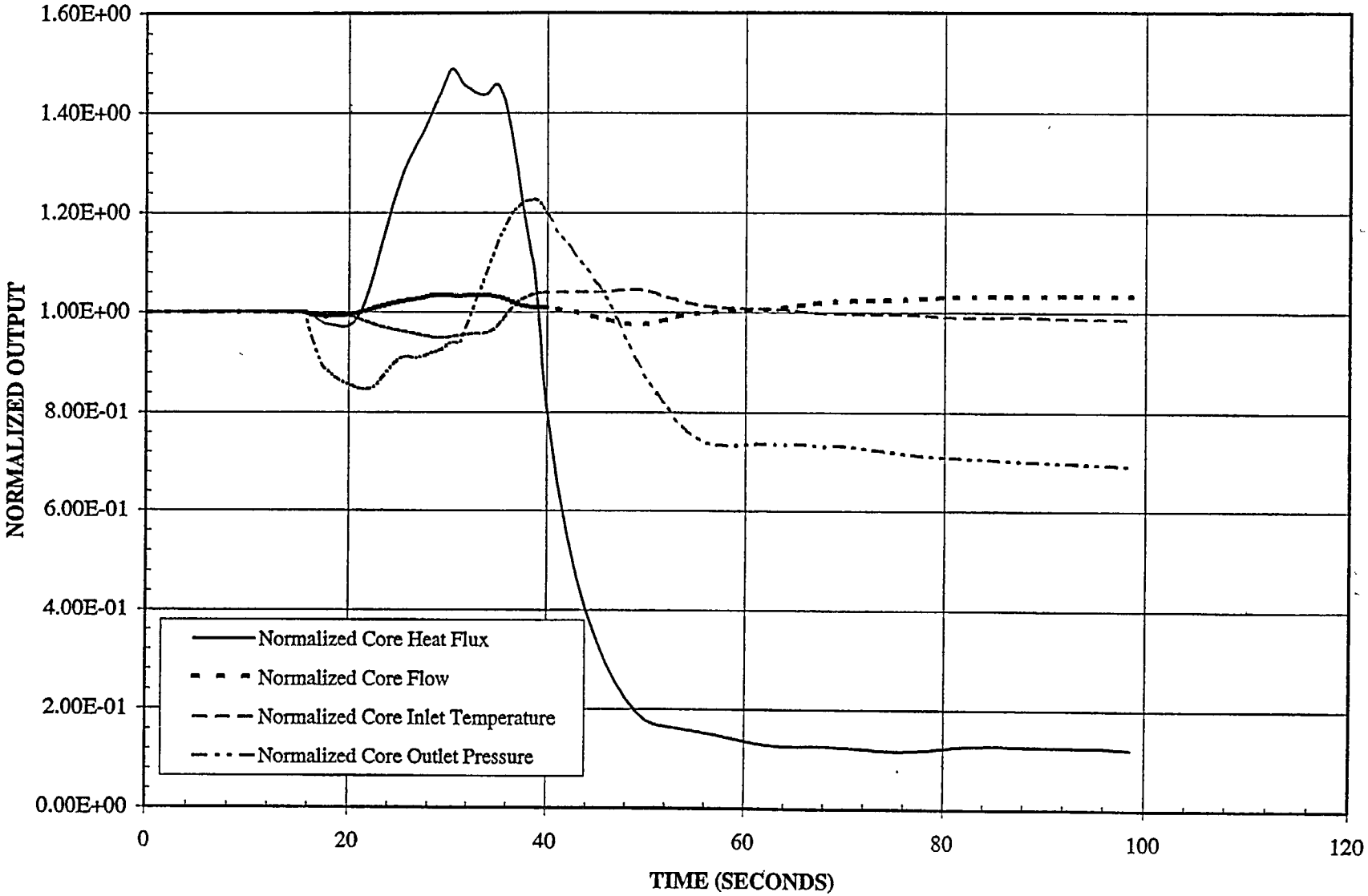


FIGURE 10-18

LARGE STEAM LINE BREAK - CONTAINMENT PRESSURE

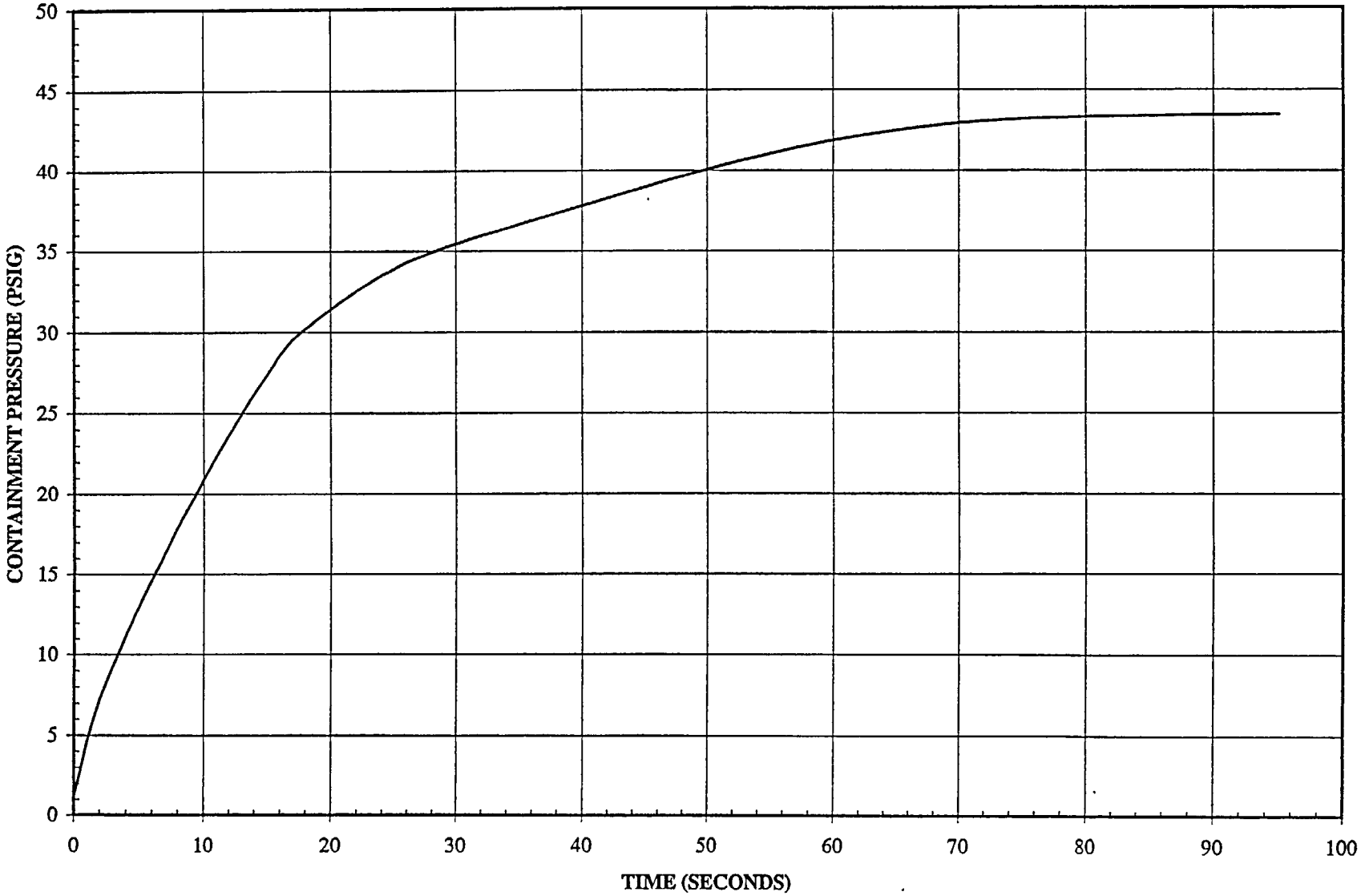
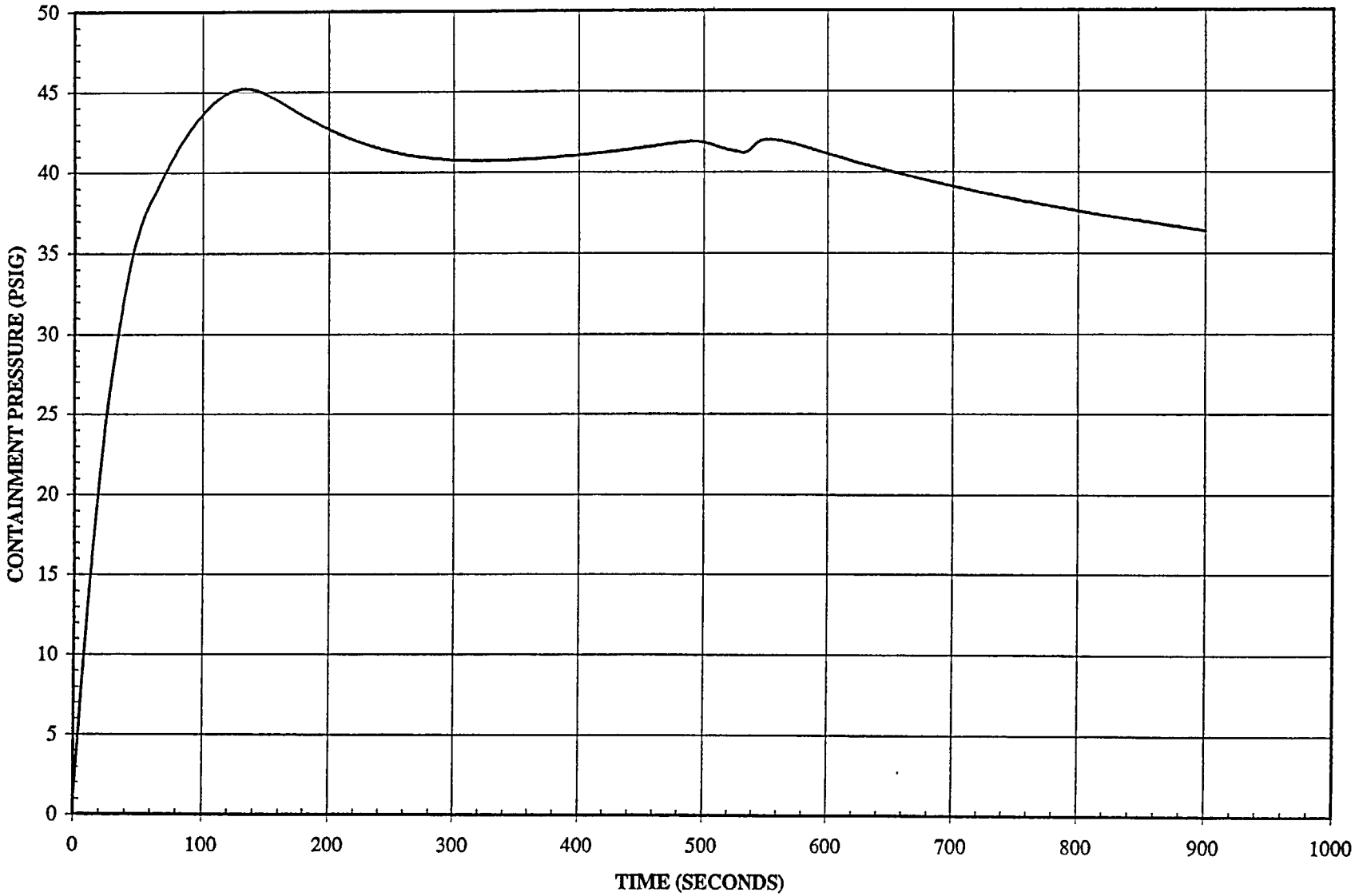


FIGURE 10-19

SMALL STEAM LINE BREAK - CONTAINMENT PRESSURE



11.0 CONCLUSION

The Duke methodology for assessing defense-in-depth and diversity capability is based upon a three-pronged approach: 1) defense-in-depth, 2) dependability (quality, testability and reliability), and 3) diversity.

The D-in-D&D methodology has been developed to satisfy NRC acceptance criteria while achieving two primary implementation goals:

- No requirement to add new diverse indications or manual controls. With a skillful design for I&C equipment arrangement, it is possible to preserve the integrity of signals to plant control systems, even in the presence of an unlikely SWCMF. The information available to the operator is sufficient to place and maintain the plant in a stable condition..

- No requirement to add or expand diverse actuation systems. With the ONS arrangement of existing diverse I&C equipment, it is not necessary to burden the plant with a requirement to add new diverse actuations. Existing diverse systems such as AMSAC and DSS fulfill their functions and do not require expansion.

Insofar as D-in-D&D is concerned, the design, qualification, and in-service testing afforded by the TXS systems are designed to minimize the probability of failures of all types. Moreover, ONS is designed so that challenges to the safety I&C systems occur at a significantly low rate. Interdependence between the RPS and the ESPS has been reviewed in the past and its resolution is in the form of the ATWS Rule (10CFR50.62) (Reference 30). In this assessment, special attention has been given to assure the diversity requirements between the ATWS System and the RPS/ESPS. The ONS design continues to meet the requirements of the ATWS Rule.

In the defense-in-depth concept of the plant, the RPS and the ESPS represent the main echelons of defense. A second line of defense is provided by a combination of plant control systems, such as ICS, as well as the ATWS System (DSS and AMSAC). In the very unlikely event the RPS is unavailable due to a postulated SWCMF, the TXS architecture has been carefully designed to assure that the plant control systems, AMSAC, and indications necessary for operator action remain available. The TXS design measures for error avoidance and fault tolerance are extremely effective at both preventing and minimizing the consequences of postulated software failures. Diversity at ONS is provided through the skillful application of both safety and non-safety related instrumentation and control system platforms including the TXS platform.

Indicators and alarms provided for each of the events (control rod ejection, large steam line break, small steam line break and small break LOCA) where operator action is required are through components that are not dependent on the TXS software. These indicators and alarms will alert the operator in a timely fashion that an event is occurring and that operator action is required in accordance with procedures. The criteria for operator action being a credible response is as follows:

- The postulated SWCMF and its effects do not impair controls or displays necessary for operator action,
- Sufficient information is available for the operator, and
- Sufficient time is available for operator analysis, decisions and action.

These criteria were all met.

The existing Diverse Scram System (DSS), which trips control rod groups 5-7 on hot leg pressure exceeding 2450 psig successfully mitigates many of the transients and accidents of concern. The acceptance criteria have been met for all transients and accidents with the exception of the large break LOCA event. For the large break LOCA the failure of the automatic ESPS actuation of the LPIS causes an unacceptable delay in the delivery of emergency core coolant. However, Duke has chosen to use an approach that justifies the elimination of the LBLOCA from consideration. The justification used is to take credit for the leak detection capability, as discussed in BTP HICB-19, along with the low probability of occurrence of a concurrent SWCMF to the TXS system and the LBLOCA event, and the inherent RCS quality to eliminate the large break LOCA from the scope of this study.

The result of this overall assessment demonstrates that there is adequate diversity for each event. The analysis for each event demonstrates that the diverse response is unlikely to be subject to the same SWCMF. In all events the diverse response performs either the same function or a different function and is performed by acceptable high-quality components.

This report demonstrates that the planned digital RPS and ESPS upgrade satisfies NRC acceptance criteria for diversity and defense-in-depth. Implementation of the ONS instrumentation and control system digital upgrade with the TXS system considering the analytical methodology described in the report assures that adequate diversity and defense-in-depth is provided in the design approach to meet the criteria established by the NRC's requirements.

12. REFERENCES

1. NUREG-0800, "Standard Review Plan", Chapter 7, Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems." Revision 4, June 1997.

2. Siemens Topical Report EMF-2110, Revision 1, "Teleperm XS: A Digital Reactor Protection System," September 1, 1999.

3. EPRI Technical Report (TR)-102348 Revision 1, "Guidelines on Licensing Digital Upgrades," March 2002.

4. NRC Regulatory Issue Summary 2002-22, Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule," November 25, 2002.

5. Oconee Nuclear Station updated FSAR Chapters 7 and 15, December 31, 2001.

6. Siemens Topical Report EMF-2267: "Siemens Power Corporation Methodology Report For Diversity And Defense-In-Depth," August 1999.

7. Siemens Topical Report EMF-2340, Revision 0: "Siemens Power Corporation Diversity And Defense-In-Depth Assessment In Accordance With The Methodology Of EMF-2267" January 2000.

8. Duke Power Report DPC-NE-3007, "Oconee Nuclear Station RPS/ESPS Digital Replacement Project Defense-in-Depth and Diversity Analysis," December 2002.

9. Code of Federal Regulations Title 10 Part 50, Revised as of January 1, 2002.

10. Letter from Stuart A. Richards, Director Project Directorate IV and Decommissioning, Division of Licensing Project Management, Office of Nuclear Reactor Regulation to Jim Mallay, Director, Nuclear Regulatory Affairs, Siemens Power Corporation dated May 5, 2000; Subject: ACCEPTANCE FOR REFERENCING OF LICENSING TOPICAL REPORT EMF-2110(NP), REVISION 1, "TELEPERM XS: A DIGITAL REACTOR PROTECTION SYSTEM".

11. IEC 880. "Software for Computers in the Safety Systems of Nuclear Power Stations," 1986.

12. IEC 880, Supplement 1 Draft. "Software for Computers in the Safety Systems of Nuclear Power Stations," 1996.

13. Regulatory Guide 1.152, Revision 1. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," 1996.

14. NUREG/CR-6303. "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.

15. NUREG-0493. "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.

16. RETRAN-3D - A Program for Transient Thermal-Hydraulic Analysis of Complex Fluid Flow Systems, EPRI, NP-7450(A), Volumes 1-4, Revision 5, July 2001.

17. VIPRE-01: A Thermal-Hydraulic Code for Reactor Cores, EPRI NP-2511-CCM Revision 3, EPRI, August 1989.

18. CAP-Containment Analysis Package (FATHOMS), Numerical Applications, Inc., October 10, 1989.

19. Nuclear Design Methodology Using CASMO-3/SIMULATE-3P, DPC-NE-1004A, Revision 1, Duke Power Company, September 1999.

20. RELAP5/MOD2-B&W - An Advanced Computer Program for Light Water Reactor LOCA and Non-LOCA Transient Analysis, BAW-10164-P, Babcock & Wilcox, December 1987.

21. LOCADOSE - A Computer System for Multi-Region Radioactive Transport and Dose Calculation, NE319/6.01 Theoretical Manual, Revision 8, Bechtel Corporation, September 5, 2002, Bechtel Proprietary.

22. Thermal-Hydraulic Transient Analysis Methodology, DPC-NE-3000-P, Revision 3, Duke Power Company, June 2002.

23. UFSAR Chapter 15 Transient Analysis Methodology, DPC-NE-3005-P, Revision 2, Duke Power Company, June 2002.

24. BWNT, Loss-of-Coolant Accident Evaluation Model for Once-Through Steam Generator Plants, BAW-10192-PA, Framatome Technologies, Inc., Revision 0, June 1998.

25. Mass and Energy Release and Containment Response Methodology, DPC-NE-3003-P, Revision 1, Duke Power Company, June 2002.

26. Letter, W. R. McCollum (Duke) to NRC Document Control Desk, October 16, 2001 (Alternative Source Term Application submittal for ONS), with supplements in response to Request for Additional Information dated May 20, 2002; September 12, 2002; and November 21, 2002.

27. Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Plants, Regulatory Guide 1.183, U.S. N.R.C, July 2000.

28. USNRC, Regulatory Guide 1.45, "Reactor Coolant Pressure Boundary Leakage Detection Systems," May 1973.

29. NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980.

30. Code of Federal Regulations Title 10 Part 50.62, "Requirements for Risk From Anticipated Transients Without Scram (ATWS) Events for Light Water-Cooled Nuclear Power Plants."