# AP600 DOCUMENT COVER SHEET

TDC: _____ IDS: 1 _____ S _____

Form 58202G(5/94) [t:\xxxx.wpf:1x] AP600 CENTRAL FILE USE ONLY:

0058.FRM RFS#: RFS ITEM #:

| AP600 DOCUMENT NO. | REVISION NO. | | ASSIGNED TO |
|---|---|---|---|
| GWGL022 | 10 | Page 1 of 1 | NRC Document Control Desk |

ALTERNATE DOCUMENT NUMBER: WORK BREAKDOWN #: 3.1.2

DESIGN AGENT ORGANIZATION: Westinghouse

TITLE: AP600 Probabilistic Risk Assessment

| ATTACHMENTS: | DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION: |
|---|---|
| CALCULATION/ANALYSIS REFERENCE: | |

| ELECTRONIC FILENAME | ELECTRONIC FILE FORMAT | ELECTRONIC FILE DESCRIPTION |
|---|---|---|
| | | |



☐ WESTINGHOUSE PROPRIETARY CLASS 2

This document contains information proprietary to Westinghouse Electric Corporation; it is submitted in confidence and is to be used solely for the purpose for which it is furnished and returned upon request. This document and such information is not to be reproduced, transmitted, disclosed or used otherwise in whole or in part without prior written authorization of Westinghouse Electric Corporation, Energy Systems Business Unit, subject to the legends contained hereof.

☐ WESTINGHOUSE PROPRIETARY CLASS 2C

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Corporation and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

☒ WESTINGHOUSE CLASS 3 (NON PROPRIETARY)

**COMPLETE 1 IF WORK PERFORMED UNDER DESIGN CERTIFICATION OR COMPLETE 2 IF WORK PERFORMED UNDER FOAKE.**

1 ☐ **DOE DESIGN CERTIFICATION PROGRAM** - GOVERNMENT LIMITED RIGHTS STATEMENT [See page 2]

Copyright statement: A license is reserved to the U.S. Government under contract DE-AC03-90SF18495.

☒ DOE CONTRACT DELIVERABLES (DELIVERED DATA)

Subject to specified exceptions, disclosure of this data is restricted until September 30, 1995 or Design Certification under DOE contract DE-AC03-90SF18495, whichever is later.

EPRI CONFIDENTIAL: NOTICE: 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ CATEGORY: A ☒ B ☐ C ☐ D ☐ E ☐ F ☐

2 ☐ **ARC FOAKE PROGRAM** - ARC LIMITED RIGHTS STATEMENT [See page 2]

Copyright statement: A license is reserved to the U.S. Government under contract DE-FC02-NE34267 and subcontract ARC-93-3-SC-001.

☐ ARC CONTRACT DELIVERABLES (CONTRACT DATA)

Subject to specified exceptions, disclosure of this data is restricted under ARC Subcontract ARC-93-3-SC-001.

| ORIGINATOR | SIGNATURE/DATE | |
|---|---|---|
| C. L. Haag | C L Haag 6/26/97 | |
| AP600 RESPONSIBLE MANAGER | SIGNATURE* | APPROVAL DATE |
| B. A. McIntyre | | 6.26.97 |

*Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

Form 58202G(5/94)

## LIMITED RIGHTS STATEMENTS

**DOE GOVERNMENT LIMITED RIGHTS STATEMENT**

(A) These data are submitted with limited rights under government contract No. DE-AC03-90SF18495. These data may be reproduced and used by the government with the express limitation that they will not, without written permission of the contractor, be used for purposes of manufacturer nor disclosed outside the government; except that the government may disclose these data outside the government for the following purposes, if any, provided that the government makes such disclosure subject to prohibition against further use and disclosure:
(I) This "Proprietary Data" may be disclosed for evaluation purposes under the restrictions above.
(II) The "Proprietary Data" may be disclosed to the Electric Power Research Institute (EPRI), electric utility representatives and their direct consultants, excluding direct commercial competitors, and the DOE National Laboratories under the prohibitions and restrictions above.

(B) This notice shall be marked on any reproduction of these data, in whole or in part.

**ARC LIMITED RIGHTS STATEMENT:**

This proprietary data, furnished under Subcontract Number ARC-93-3-SC-001 with ARC may be duplicated and used by the government and ARC, subject to the limitations of Article H-17.F. of that subcontract, with the express limitations that the proprietary data may not be disclosed outside the government or ARC, or ARC's Class 1 & 3 members or EPRI or be used for purposes of manufacture without prior permission of the Subcontractor, except that further disclosure or use may be made solely for the following purposes:

This proprietary data may be disclosed to other than commercial competitors of Subcontractor for evaluation purposes of this subcontract under the restriction that the proprietary data be retained in confidence and not be further disclosed, and subject to the terms of a non-disclosure agreement between the Subcontractor and that organization, excluding DOE and its contractors.

## DEFINITIONS

**CONTRACT/DELIVERED DATA** — Consists of documents (e.g. specifications, drawings, reports) which are generated under the DOE or ARC contracts which contain no background proprietary data.

## EPRI CONFIDENTIALITY / OBLIGATION NOTICES

**NOTICE 1:** The data in this document is subject to no confidentiality obligations.

**NOTICE 2:** The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for limited purposes only. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited except as agreed to in advance by the Electric Power Research Institute (EPRI) and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted.

**NOTICE 3:** The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for use only in evaluation tasks specifically authorized by the Electric Power Research Institute (EPRI). Any use, disclosure to unauthorized persons, or copying this document or parts thereof is prohibited except as agreed to in advance by EPRI and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted. This document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

**NOTICE 4:** The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is being revealed in confidence and trust only to Employees of EPRI and to certain contractors of EPRI for limited evaluation tasks authorized by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. This Document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

**NOTICE 5:** The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. Access to this data is given in Confidence and Trust only at Westinghouse facilities for limited evaluation tasks assigned by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. Neither this document nor any excerpts therefrom are to be removed from Westinghouse facilities.

## EPRI CONFIDENTIALITY / OBLIGATION CATEGORIES

**CATEGORY "A"** — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is contained in an issued reported.

**CATEGORY "B"** — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is not contained in an issued report, except for computer programs.

**CATEGORY "C"** — Consists of CONTRACTOR Background Data except for computer programs.

**CATEGORY "D"** — Consists of computer programs developed in the course of performing the Work.

**CATEGORY "E"** — Consists of computer programs developed prior to the Effective Date or after the Effective Date but outside the scope of the Work.

**CATEGORY "F"** — Consists of administrative plans and administrative reports.

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

# CHAPTER 26

# PROTECTION AND SAFETY MONITORING SYSTEM

## 26.1 System Analysis Description

This chapter evaluates the reliability of the protection and safety monitoring system (PMS) and its ability to initiate the safety-related functions necessary to shut down the plant and to maintain the plant in a safe shutdown condition. Included in the assessed functions are the PMS's capability to control safety-related components in the plant that are operated from the main control room or remote shutdown workstation and to monitor the plant safety-related functions during and following an accident. In particular, the assessed functions of the PMS include the availability of the system to:

- Automatically initiate operation of appropriate systems, including reactivity control systems and to ensure that specified acceptable reactor core and internals design limits, and design limits of the reactor coolant and moderator pressure boundaries, are not exceeded as a result of anticipated operational occurrences, maintenance, and testing

- Sense accident conditions and initiate operation of systems and components important to safety

A description of the PMS function is provided in Chapter 7 of the *AP600 Standard Safety Analysis Report* (SSAR).

The AP600 instrumentation and control architecture contains the following three major components: 1) the protection and safety monitoring system (PMS), 2) the plant control system (PLS), and 3) the diverse actuation system (DAS). This section focuses on the assessment of the PMS; the DAS and PLS are discussed in Chapters 27 and 28, respectively.

The scope of the system analyses includes the following equipment:

- Integrated protection cabinets (IPC)
- Engineered safety features actuation cabinets (ESFAC)
- Protection logic cabinets (PLC)
- Protection logic bus
- Qualified data processing system (QDPS)
- Reactor trip switchgear (RTS)
- Operator controls
- Main control room multiplexers and remote shutdown workstation multiplexers

The following systems, although not formally included in the PMS, are also addressed in this chapter:

- Control rod drive mechanisms (CRDM)
- Sensors

The analysis of the PMS is divided into the following functional groupings:

- Reactor trip
  - Automatic - sensors through breakers and CRDMs
  - Manual - control inputs through breakers and CRDMs

- Engineered safety features (ESF) actuation
  - Automatic - sensors through output driver modules
  - Manual - control inputs through output driver modules

- Indication - QDPS, PMS/PLS/data display system (DDS), DAS

- Reactor coolant pump trip - sensors through breakers (Note that while the reactor coolant pump trip is a function of the engineered safety features, system level trees are developed and reactor coolant pump trip is therefore treated separately from the engineered safety features)

The following paragraphs discuss the general approach taken for the modeling of each of the functional groupings.

**Reactor Trip**

Three reactor-trip-signal-related trees are developed in this section. These are RTPMS, RTPMS1, and RTSTP. These trees, described later in this chapter, form the models that are used to evaluate the availability of the reactor trip system to shut the reactor down in a swift and safe manner.

**Engineered Safety Features Actuation**

As part of the system trees that are developed in other chapters of this document, an engineered safety features actuation signal is typically needed as one of the inputs to a system tree to model complete actuation of an ESF-related component. For each of these required actuation signals, an instrumentation and control subtree is developed to model the unavailability of the engineered safety features to provide the actuation signal upon demand. There are 258 instrumentation and control subtrees developed in this section to support that purpose. The assigned systems/functions that they support in the models are as follows:

- Automatic depressurization system (ADS)
- Containment isolation system (CIS)
- Core makeup tank (CMT)
- Chemical volume and control system (CVS - valves only)
- IRWST/gravity feed (IRW)
- Passive containment cooling (PCS)
- Passive residual heat removal (PRHR)
- Normal residual heat removal (RNS)
- Reactor coolant pump trip (RPT)
- Steam generator system (SGS)

Detailed description of the instrumentation and control subtree development is presented later in this chapter.

**Indication**

Wherever manual action is credited in the assessment of the PMS, the availability of systems that collect and provide the appropriate information to be displayed as indications to the operator are modeled. A conservative simplified model is applied generically to the PMS assessments to bound the availability of the indication functions. That model is developed as follows:

There are three basic paths that are assumed to be normally available to provide indication to the operator. These are:

- Data display system
- Qualified display processing system
- Diverse actuation system

The assigned unavailability of each of these systems to provide a particular indication is 1.0E-02 failures/demand. While it is expected that the actual unavailabilities of each of these systems to provide indication would be substantially better than the assigned value, there is not a total overlap of indication functions provided across all systems, and the conservative assigned value reflects the consideration of that limitation. These values are also consistent with the assigned unavailability of 1.0E-02 failures/demand for the DAS in general. While this may be a conservative assignment, it is assumed that each of the systems is capable of providing the essential indications required for the PMS functions being modeled at that assigned rate. Therefore, failure of all three systems must occur before total loss of indication to the operator is achieved. This gives a total unavailability for the combinational loss of all indication systems of 1.0E-06 failures/demand. Contribution of common mode failure is minimized in this evaluation as the DAS is diverse from the DDS and QDPS, and hence, does not have a dominant contribution in this model.

Application of these results in the PMS models is achieved by implementing a node representing the failure of all indication, which has the resultant contribution of 1.0E-06, wherever a manual action is credited. It should be noted that wherever the failure-of-all-indication node is applied, a failure node representing the common mode failure of the associated instrumentation, namely sensors, is also applied. This is done to reflect the fact that while the cabinetry and functions of the DAS versus the PMS may be diverse, the sensors, although independent, are conservatively expected to be of the same type, and hence, susceptible to a common mode failure that could inhibit the availability of an accurate indication across all systems. This too is considered conservative, as multiple queues are usually available to the operator as indications relating to various plant parameters being monitored. The models of the PMS generally only consider the most direct sensor/queue path and do not credit alternate paths.

**Reactor Coolant Pump Trip**

Three trees are developed to address reactor coolant pump trip function in the assessment. These are the RCL, RCN and RCT trees. Note that these trees represent system level trees and are supported by a number of instrumentation and control subtrees, all of which are developed in this chapter.

The RCL tree addresses the unavailability of the PMS to trip all four reactor coolant pumps following a small LOCA, while the RCT tree addresses the unavailability of the PMS to trip all four reactor coolant pumps following a transient. The RCN tree addresses the unavailability of the PMS to trip all four reactor coolant pumps following an intermediate LOCA.

### 26.1.1 Analysis of Support Systems

**Power Distribution**

The incorporation of the ac power distribution scheme for the PMS in the analysis can be divided into the same functional groupings as above.

Reactor Trip

- Loss of power to modules that support reactor trip functions results in a default state that is towards the trip direction. Loss of power to reactor trip cabinetry results in an effective trip signal from affected cabinet trains. Loss of power to two or more reactor trip cabinet trains results in a reactor trip. Loss of power to trip breakers, and hence CRDMs, also results in a reactor trip. Therefore, no inclusion of the potential for loss of power is applied in reactor trip trees, as these trees are developed to determine the potential for a failure-to-trip-upon-demand state.

Engineered Safety Features Actuation

- Loss of power to modules that support ESF functions leads to a default state that generally results in an ESF actuation state. However, due to the complexity of determining appropriate default states for each plant scenario that could be modeled, a conservative modeling approach has been taken that assumes power is required for proper processing of information and final ESF actuation. Therefore, modeling of the potential for loss of power is included in ESF fault trees. Credit is taken for multiple trains of power that are available, which are backed by plant batteries.

Indication

- Loss of power is assumed to cause loss of the associated indication path under consideration. Contribution due to loss of power is included in the bounding 1.0E-02 unavailability assigned to each system in the indication model. Loss of power does not result in a high contribution due to redundant, battery backed busses that are available.

Reactor Coolant Pump Trip

- Loss of power can affect reactor coolant pump trip in two ways. First is through loss of power to the PMS, which generates the reactor coolant pump trip signal. As discussed above, loss of power is conservatively modeled in the PMS ESF trees. Also, loss of control power required to open reactor coolant pump breakers will cause a failure-to-trip state for reactor coolant pumps. Nodes reflecting the availability of this control power is included in reactor coolant pump trip trees, in conjunction with nodes representing failure of the breakers and failure of the PMS reactor coolant pump trip signal.

Table 26-4 provides a detailed list of the power supporting systems.

**Equipment Cooling**

Loss of all ventilation for a 24-hour scenario does not lead to the internal cabinet temperature exceeding the design limit of 120°F maximum allowable for proper card operation. In addition, loss of cooling to the PMS cabinets, which could eventually lead to elevated cabinet temperatures, would be detected by cabinet temperature sensors that are continuously monitored by the system. Upon detection of high cabinet temperature, the system assumes a predefined default state. That state is trip for reactor trip functions and actuate for ESF functions (exception: the fourth-stage ADS control signal default states are stay-as-is, as opposed to actuate). However, to conservatively model the possibility for failure of this mechanism, contribution for failure of the cabinet fan unit has been included in the modeling of each cabinet subsystem. Also, conditional probabilities given fan failure and coincident failure of the circuits that detect high temperature have been included as contributions to unavailability in the models.

### 26.1.2 Analysis of Instrumentation

Field signals are wired directly from the sensor, transmitter, switch, relay contact, or external systems to the PMS input/output (I/O) termination boards. Assignment of the sensors and input groups to each of the PMS fault tree models is performed on a function-by-function basis in the analyses. The assignment and logic used in developing the sensor group fault trees for a particular function are based on the information obtained for that function from the process block diagrams (References 26-10, 26-11, and 26-12), the input/output listings, and the success criteria for the calling system level trees in cases of the instrumentation and control subtrees. The process block diagrams show logic and input signals required to produce a particular ESF actuation, while input/output listings indicate which cabinet and train of equipment is connected to each sensor. Where redundancy is indicated in process block diagrams, that credit is developed into the trees. However, where multiple sensors are shown as inputs to a function and no redundancy or combinational logic is shown, all sensors are conservatively assumed to be able to fail the function independently. Table 26-11 shows sensor types that are used in the analyses.

### 26.1.3 Test and Maintenance Assumptions

Table 26-5 lists the testing frequency of PMS components. Table 26-6 describes the maintenance assumptions.

#### Automatic Testing

Automatic testing is used to test the IPC, ESFAC, and PLC subsystems. This analysis assumes that the autotester sequence will be initiated quarterly for each associated hardware train (as described in the SSAR). Note that the automatic test requires manual initiation to enable it to perform its automated testing sequence. This test frequency is used in analysis availability equations to define the mission time for systems under consideration.

For more details on automatic testing, see SSAR Section 7.1.

#### Self-Diagnostic Testing

Automatic self-diagnostic testing is performed during all modes of plant operation. This test is performed continuously to provide early detection of hardware malfunctions. This type of diagnostic testing includes tests such as processor checks, programmable read-only memory block check sums, read/write test of random access memory, check sums of static random access memory data, check sums of shared memory blocks, and data link transmission error detection. Extensive, detailed FMEA and functional block analyses (FBA), have been performed on the PMS modules to determine the effectiveness of these self-tests. In general, the results indicate that approximately 90 to 99 percent of faults that could occur will be detected by diagnostics and cause the system to assume a default state. These results are

incorporated into unavailability equations as percentages of faults that are detectable and/or fail-safe.

Additional test and maintenance assumptions for each of the PMS functions are described below.

**Reactor Trip**

Rod control cluster assemblies of the control rod drive mechanism are tested for movement every 2 weeks. In addition, rod cluster control assemblies are also tested at each refueling. Reactor trip system hardware is internally tested on a continuous basis through application of online diagnostics and is assumed to be functionally tested quarterly to demonstrate operability of all trip functions.

**ESF Actuation**

ESF system hardware is internally tested on a continuous basis through application of online diagnostics and is assumed to be functionally tested quarterly to demonstrate operability of all ESF functions. This includes testing of the ability to generate the reactor coolant pump trip signal.

**Indication**

By providing basic indication functions for the plant, effective testing of various indication paths is performed during each use of the indications available. Through comparison of the redundant displays, confirmation of correct processing and display may be assumed to be obtained on a continuous basis.

## 26.2 Performance during Accident Conditions

This section discusses success criteria for PMS assessments following different initiating events. The PMS provides automatic and manual actuation signals for various systems or functions, which have been listed earlier. Each of the initiating events either generates an appropriate trip demand and/or an ESF actuation. The reactor trip demand de-energizes the control rod drive mechanism and causes latch assemblies of the control rod drive mechanism to release the rod control clusters. Rod cluster control assemblies then fall into the reactor by gravity, causing a reactor shutdown. This control rod drive mechanism is indicated as MGSET in event tree models, and development of its failure probability is given in Section 26.1 of this report. Because the control rod drive mechanism is a passive safety-related system that does not rely on other systems for success, no other initiator would cause failure of the control rod drive mechanism to perform its intended safety function.

For ESF actuation, appropriate initiating events cause an associated ESF starting or controlling signal to ESF components to mitigate plant damage.

Table 26-1 lists fault tree names created in modeling the PMS instrumentation and control system. The success criteria for these fault trees are described in Tables 26-2a through 26-2e.

## 26.3 Initiating Event Review

This section addresses two issues: initiating events that impact availability of the PMS and initiating events that can be generated due to the failure of the PMS.

### 26.3.1 Initiating Event Impacting PMS

**Reactor Trip**

There are no initiating events that will impact availability of the reactor trip system.

**ESF Actuation Subsystem**

There are no initiating events that will impact availability of the ESF actuation system.

**Qualified Display Processing Subsystem**

There are no initiating events that will impact availability of the qualified display processing subsystem.

### 26.3.2 Initiating Event due to Loss of PMS

**Reactor Trip**

There are other ways to trip the reactor, even if both automatic and manual PMS fail: via automatic and manual diverse actuations (discussed in Chapter 27), local operator action to de-energize the MGSETs, and operator action to manually step in the rods. Hence, PMS failure does not necessarily lead to failure to trip the reactor. However, mechanical failure of the control rod drive mechanism to insert rod cluster control assemblies results in an anticipated trip without scram event. Additionally, failure of the PMS reactor trip can result in a spurious reactor trip.

**ESF Actuation Subsystem**

PMS failure could lead to failure to actuate ESF systems. This is possible if any of the following three sets of cabinets fail: integrated protection cabinets, engineering safety features actuation cabinets, and protection logic cabinets. In case of integrated protection cabinet or ESF actuation cabinet failure, manual actuation of safety systems and components are still possible. However, failure of protection logic cabinets will fail both automatic and manual actuation of safety components since manual signals pass through protection logic cabinets. Failure of PMS ESF can lead to spurious ESF actuations.

### Qualified Display Processing Subsystem

The qualified display processing subsystem has no direct control over plant component actuation and cannot cause an initiating event by itself. Only by failure to indicate correctly, coupled with failure of all other sources of display, failure of associated operator action, and failure of protection systems, is it possible to generate the condition for an initiating event originating from the qualified display processing subsystem.

## 26.4 System Logic Model Development

This section presents logic models used for quantification of system performance under various conditions. Each model depicts the system, given an initiating event. The top event logic for each model is defined by success criteria, which are directly related to the initiator.

### 26.4.1 Assumptions and Boundary Conditions

The following assumptions and boundary conditions apply to the assessment of the PMS.

a. The level of detail modeled for the PMS is limited to the circuit board or line replaceable unit level.

b. Wiring and cables are assumed to be available. Typically, failures of this equipment are experienced at termination junctions of transmitting and receiving boards, and failure rates for wiring are typically much lower than transmitting and receiving hardware. Effects of these failures are incorporated into the assessed performance of associated circuits boards. In addition, the level of complexity, coding, and dynamic signaling techniques used in transmission of data (such as deadman timers and on-line diagnostic) throughout the system forces any failures of this type to become uniquely detectable. Effects of these failures is bounded by the performance of transmitting and receiving circuitry.

c. The automatic tester subsystem is not analyzed in this evaluation. The communication subsystem is analyzed only for the part that is used for transmitting signals from the PMS to the plant control system.

d. The self-diagnostic test is conservatively assumed to be automatically completed every 5 minutes with an effectiveness in excess of 90 percent for all components that are monitored within the system. The actual effectiveness assigned is dependent on the module under consideration and the function that module is performing. Each value is used as input to availability equations to form basic event data base numbers.

e. A mean repair time for instrumentation and control components is assumed to be 4 hours for components located in accessible areas during normal plant operation.

f. No contribution due to random software failure is considered, as software failure falls solely under the category of common mode design failures. Appropriate nodes reflecting common mode software failure of individual software implementations and common mode failure of all software implementations within the system are included in the modeling. Development of software common mode models is discussed later in this chapter.

g. Cards connected directly to computer busses are assumed capable of causing busses to fail.

h. Pressure transmitters are used to measure pressure, level, or flow parameters.

The first type of pressure transmitters are those used to continuously interface with reactor pressure and high temperature. This type is a transmitter used to measure the following parameters:

- Pressurizer pressure
- Pressurizer water level
- Steam generator narrow range and wide range water level
- Steam generator steam line pressure
- Startup feedwater flow
- Reactor coolant pump flow

Common cause failures among these transmitters are named CCX-XMTR and/or CCX-XMTR195, as defined in Table 26-9.

The second type of pressure transmitters are those interfacing with high pressure and/or high temperature following an accident. These are the pressure transmitters used to measure containment pressure. Common cause failures among these transmitters are named CCX-XMTR1.

The third type of pressure transmitters are those sensing a system pressure (i.e., no stringent operating conditions). These transmitters (generally measuring pressure or flow) are used to start a standby loop (such as service water) on the failure of the normally operating one. Common cause failures among these transmitters are named CCX-TRNSM.

A fourth type of pressure transmitter is for the in-containment refueling water storage tank (IRWST) low water level. They sense very low pressure and normal temperature except during passive residual heat removal (PRHR) actuation. Common cause failures among these transmitters are named IWX-XMTR.

i. Automatic testing performed by the automatic tester subsystem comprehensively tests all boards every 3 months. A manual starting of the automatic tester subsystem is required.

A manual test is also performed to permit a complete test of the dynamic trip bus. During this test, the opening of the reactor trip breakers is also verified. This manual test is assumed to be performed every refueling.

j. One protection logic cabinet per engineered safety features actuation cabinets is present. Each protection logic cabinet contains power interface cards. Each power interface card actuates only one component. For the fourth stage of ADS, each Squibb valve is actuated by two power interface cards to preclude inadvertent actuation. Each card performs two-out-of-three voting.

k. The dynamic trip bus is composed of dynamic logic units. One dynamic logic unit per parameter is provided. For example, there is a dynamic logic unit for steam generator level and another for source range neutron flux. For each dynamic logic unit, there is a dedicated trip/normal/bypass switch that allows each individual partial trip function to be manually tripped or bypassed by plant personnel.

l. Sensors and field contacts are powered by the same bus as the PMS, i.e., by the Class 1E 120-vac uninterruptible power supply.

m. During testing, the two-out-of-four logic of one input becomes two-out-of-three logic. Subsequent channel bypass or failure results in one-out-of-two logic and upon an additional failure or bypass, the system trips.

n. Global trip is activated if any of three conditions, as reported in the subsystem description, are true for any trip functions. Conservatively, in this analysis only one condition leads to the global trip signal; i.e., two-out-of-three unbypassed partial trip from the other three channels.

o. Trip enable is activated if either of two conditions, as reported in the subsystem description, is true for any trip functions. Conservatively, in this analysis only one condition leads to the trip enable signal; i.e., one-out-of-three unbypassed partial trip from the other channels.

p. For the PMS, when a component can be manually actuated at system level as well as component level, failure of the common part of the chain (such as the protection logic cabinet) is modeled to reflect that singularity and integrated with the individual input and output circuits required.

q. Instrument line plugging during plant normal operation is not detectable until variations in plant conditions occur. Given a plugged line, the sensor/transmitters continue to

record the same value as before plugging occurred. The operator performs a channel check every 24 hours, which consists of reading and comparing values of the same parameter coming from four divisional sensor/transmitters.

If a large variation on the plant conditions (such as pressure and level) occurs, the sensor/transmitter connected with the plugged instrument line records a value different from the others. This alerts the operator to the degradation of the sensor/transmitter, which is put in a bypass state until the next refueling. This potential downtime is reflected in development of the sensor unavailabilities.

r. The power source of 120 vac is modeled in all trees with the exception of the reactor trip trees, since a power failure will automatically result in a reactor trip. The components actuated by the remainder of the instrumentation and control may require power for proper operation.

s. The implementation of the I&C subtrees is determined by combining success criteria (as described in the sections for which the subtrees are developed), the instrument lists, and information regarding the modeled function (as described in References 26-10, 26-11 and 26-12).

t. Loss of cooling assembly does not affect the board's performance, but failure of HVAC fan units have been conservatively included in modeling of the systems.

u. Failure of the pulse generator to produce the pulse signal is not accounted, because it leads to the reactor trip state.

v. In case of blackout, one-out-of-two subsystems of ESFAC and PLC is inoperable. The second subsystem works correctly because it is supplied by an uninterruptible power supply (UPS).

w. Loss of at least three 120-vac power sources leads to the fail-safe status for the de-energize to trip components. The loss of 120-vac power supply is conservatively modeled as possible failure for the engineered safety features for de-energize to trip components.

x. Where more than three independent, diverse sensor measurements are available as inputs for the processing of a particular functional operation, a conservative 1.0E-06 failures/demand rate is assigned to represent the unavailability contribution due to failure of all associated input sensors.

### 26.4.2 Fault Tree Models

The PMS fault tree models included in this section are:

- RTPMS: failure of the PMS to initiate a reactor trip, both automatic and manual (ATW-MAN03)
- RTPMS1: failure of the PMS to initiate a reactor trip, both automatic and manual (ATW-MAN05)
- RTSTP: failure of the operator to manually step in the control rods after the PMS (RTPMS) and the DAS (RTDAS) fail to trip the reactor
- RCL: failure to trip all four reactor coolant pumps following a small LOCA
- RCN: failure to trip all four reactor coolant pumps following an intermediate LOCA
- RCT: failure to trip all four reactor coolant pumps following transients
- SYS-IC: failure of the PMS to provide automatic and or manual actuation signals to plant equipment, incorporating the appropriate parts of the PMS ESF I&C. There are 258 PMS I&C subtrees, each of which are detailed in Table 26-2e. Note that for each of the 258 I&C subtrees, a list of subtrees is provided. These trees, when linked together according to batch-run files, form the individual I&C subs. This is described in detail below.

Fault trees for this system, RTPMS, RTPMS1, and RTSTP, are shown in Figures 26-4, 26-5, and 26-6 of Reference 26-1, respectively.

Fault trees for RCL, RCN and RCT, are shown in Figures 26-1 through 26-3 of Reference 26-1. A representative set of fault trees for the PMS I&C subtrees and their associated subtrees are shown in Figures 26-7 through 26-363 in Reference 26-1.

Fault tree analysis results provide quantitative values of total system unavailability and of the importance of specific components to that total. Table 26-1 provides a brief description for fault trees modeled. Tables 26-2a through 26-2e summarize success criteria for these fault trees. Event files for these trees are in Tables 26-10a and 26-10b.

### 26.4.3 Description of I&C Subtree Development

I&C subtrees are developed in a modular fashion, which facilitates construction, assembly, and review of the various I&C subtree functions that are required for analysis. To illustrate application of this method, the IC11A I&C subtree will be used as an example. Trees

required to construct the IC11A I&C subtree are listed in the first entry column of Table 26-2e. They are (with description):

- ADS-IC01: top tree of IC11A - fail to actuate V001A and V011A
- EPOADS01: failure of output driver modules
- MA1ADS01: failure of manual action (human error)
- S11ADS01: failure of PMS sensor group 1 (division 1)
- S12ADS01: failure of PMS sensor group 2 (division 2)
- S13ADS01: failure of PMS sensor group 3 (division 3)
- S14ADS01: failure of PMS sensor group 4 (division 4)
- S3DADS01: failure of DAS sensor group (CMF)
- SC1ADS01: failure of PMS sensor groups (CMF)
- SI1ADS01: failure of PMS sensors used for indication (CMF)
- AESIPC: failure of PMS input logic cabinets (automatic ESF)
- AESOUTA: failure of PMS actuation and output logic cabinets (automatic ESF - train A)
- MESOUTA: Failure of PMS multiplexing and output logic cabinets (manual ESF - train A)

Discussion of the assembly of these trees is presented below in detail. The following paragraphs describe naming conventions that are used for tree types; note that each tree name contains a three-character system name (e.g., ADS), and other unique identifiers. For the top tree, the naming convention is as follows:

SYS-ICXX

where:

SYS = three-character system name
XX = two-digit number representing a unique individual I&C sub number within each system

Exceptions to this convention are as follows:

The "-" is sometimes replaced by a B or P to signify a blackout or loss-of-offsite-power (LOOP) tree, respectively.

The XX is sometimes made up of characters and/or numbers (e.g., 01, A1, 99) to accommodate the organization of I&C subtrees.

System names addressed within the PMS are:

| | | |
|---|---|---|
| ADS | CIS | CMT |
| CVS | IRW | PCS |
| RHR | RNS | RPT |
| SGS | | |

For supporting trees, there are two general types: cabinet trees and I&C specific trees, the majority of which support cabinet trees. For PMS cabinet trees, the naming convention is as follows:

XESIPC(Y)

where:

X = A for automatic actuation, and S for spurious actuation
Y = B or P for blackout or LOOP operation, respectively

Note that ES stands for ESF, and IPC indicates input cabinetry. These cabinet trees are not used for manual actuation.

XESOUTY(Z)

where:

X = A for automatic actuation, M for manual actuation, and S for spurious actuation
Y = A, B, C, or D to indicate which train of ESF is being modeled
Z = B or P for blackout or LOOP operation, respectively

Note OUT indicates the output cabinetry.

The full list of PMS ESF cabinet trees, shown in Figures 26-320 through 26-330 of Reference 26-1, is as follows:

- Automatic ESF input cabinets (transient, blackout, and LOOP):

  AESIPC AESIPCB AESIPCP

- Automatic ESF output cabinets (transient, blackout, and LOOP):

  AESOUTA AESOUTAB AESOUTAP

  AESOUTB AESOUTBB AESOUTBP

  AESOUTC AESOUTCB AESOUTCP

  AESOUTD AESOUTDB AESOUTDP

- Manual ESF output cabinets (transient, blackout, and LOOP):

  MESOUTA MESOUTAB MESOUTAP

  MESOUTB MESOUTBB MESOUTBP

  MESOUTC MESOUTCB MESOUTCP

  MESOUTD MESOUTDB MESOUTDP

- Spurious ESF input cabinets:

  SESIPC

- Spurious ESF output cabinets:

  SESOUTA

  SESOUTB

  SESOUTC

  SESOUTD

For I&C-specific support trees, the following naming convention is applied:

XXXSYSNN

where:

XXX = tree type, where the types are as follows:

- EPO: failure of output driver modules
- MA1: failure of manual action (human error)
- S11: failure of PMS sensor group 1 (division 1)
- S12: failure of PMS sensor group 2 (division 2)
- S13: failure of PMS sensor group 3 (division 3)
- S14: failure of PMS sensor group 4 (division 4)
- S3D: failure of DAS sensor group (CMF)
- SC1: failure of PMS sensor groups (CMF)
- SI1: failure of PMS sensors used for indication (CMF)

SYS = the system name, where the systems are as follows:

| | | |
|---|---|---|
| ADS | CIS | CMT |
| CVS | IRW | PCS |
| RHR | RNS | RPT |
| SGS | | |

NN = the number of the I&C subtree within each system application, where NN is made up of characters and/or numbers (e.g., 01, A1, 99) to accommodate the organization of the I&C subtrees.

In order to construct an I&C subtree, a top tree is first generated. For this example, to generate the IC11A I&C subtree, the top tree, ADS-IC01, is developed. When fully developed, linked, and quantified, output of the ADS-IC01 top tree is named to correspond with the I&C subtree name IC11A and to support linking and quantification of calling system trees.

ADS-IC01 is shown in Figure 26-81 of Reference 26-1. Other I&C specific support trees for the IC11A I&C subtree are also shown in Figures 26-82 through 26-90 of Reference 26-1. As shown in Figure 26-81 of Reference 26-1, the ADS-IC01 top gate shows the name of the tree and the final I&C subtree name. Note that the final I&C subtree name is only shown for ADS cases where the final subtree name is sufficiently different from the I&C subtree top tree name. Most other subtrees have an equivalent or near-equivalent final I&C subtree name and I&C top tree name. Cross references of final I&C subtree names to the corresponding I&C top tree names are provided in Tables 26-2e, 26-3a, and 26-3b.

Logic of the ADS-IC01 top tree shows that both automatic and manual actuations must fail to cause total actuation failure. The automatic branch is comprised of two elements: failure of PMS auto logic - SUB-AESOUTA, and common mode software failure of all boards - CCX-SFTW. Failure of either element will cause failure of automatic actuation. The SUB prefix in SUB-AESOUTA indicates that the AESOUTA cabinet tree will be linked into this tree. From above, the AESOUTA cabinet tree represents failure of automatic ESF output actuation and logic cabinets for train A. Expansion of the AESOUTA tree is discussed below.

The manual branch of the ADS-IC01 shows that PMS and DAS manual actuation paths must fail to cause total failure of manual actuation. PMS manual actuation failure branch is the same as the PMS automatic branch, but calls SUB-MESOUTA instead of SUB-AESOUTA. From above, the MESOUTA cabinet tree represents failure of manual ESF output multiplexer and logic cabinets for train A. Expansion of the MESOUTA tree is discussed below.

The DAS manual actuation failure branch is comprised of five elements:

- Failure of DAS - MDAS
- Failure of DAS sensors - SUB-DASSIND
- Loss of DAS power bus EDS3EA1 non-1E 120-vac - SUB-ED3EA1
- Operator error - REC-MANDAS
- Failure of all indication - ALL-IND-FAIL

There are no cabinet tree developments for the modeling of DAS. Discussion of the DAS assessments are provided in Chapter 27. All support trees required for modeling of DAS in the I&C subtrees are integrated at this level. Two such trees are required in this situation: SUB-DASSIND and SUB-ED3EA1. SUB-ED3EA1 calls the supporting power trees, which are described under Chapter 22. SUB-DASSIND calls the I&C specific subtree required to model the sensor inputs used as indication to the operator for manual action. For this example, the S3DADS01 tree for failure of DAS sensor group (CMF) is developed to support the DASSIND call. Output of the S3DADS01 tree are named to match the generic DASSIND name and then linked into that branch of the ADS-IC01 tree. Simplified versions of files that perform the naming and linking of the trees are shown in Table 26-3a..

At this point in the discussion, we have addressed the top tree ADS-IC01 and its immediate subtrees that are called. This can be represented as follows where indentation indicates called subtrees, and <= indicates renaming of the application-specific output file for linking as a generic

name. (Called trees with no <= indicate that the called name is a specific, rather than a generic call. Therefore, the called name is exactly the same as the supporting tree name, and no renaming is required.):

```
IC11A    <=   ADS-IC01
              AESOUTA
              MESOUTA
              DASSIND  <=  S3DADS01
              ED3EA1
```

The AESOUTA tree, shown in Figure 26-323 of Reference 26-1, models logic of automatic ESF actuation and output logic cabinets. Using the same format as presented above, subtrees that are called from the AESOUTA tree are as follows (note that the AESOUTA tree always calls AESIPC, IDAEA1, and IDAEA2 in all cases, but the actual tree used for the EPO tree is dependent on the application, hence EPOADS01 is assigned to EPO in this case):

```
AESOUTA
          EPO          <=   EPOADS01
          AESIPC
          IDAEA1
          IDAEA2
```

The AESIPC tree, shown in Figure 26-320 of Reference 26-1, models the logic of the automatic ESF input cabinets. The subtrees, which are called from the AESIPC tree, are as follows (again, note that the AESIPC tree always calls IDAEA1, IDBEA1, IDCEA1, and ICDEA1, but the actual trees used for the CCXSNRS1, SENS1, SENS2, SENS3, and SENS4 trees are dependent on the application, hence SC1ADS01, S11ADS01, S12ADS01, S13ADS01, and S14ADS01 are assigned respectively in this case):

```
AESIPC
          CCXSNRS1     <=   SC1ADS01
          SENS1        <=   S11ADS01
          SENS2        <=   S12ADS01
          SENS3        <=   S13ADS01
          SENS4        <=   S14ADS01
          IDAEA1
          IDBEA1
          IDCEA1
          IDDEA1
```

The MESOUTA tree, shown in Figure 26-328 of Reference 26-1, models logic of the manual ESF multiplexer and output logic cabinets. Again, using the same format as presented above, subtrees, which are called from the MESOUTA tree, are as follows (again, note that MESOUTA tree always calls IDAEA1 and IDAEA2, but the EPO, ESFOPER, and CCXSNRS2 trees are depended

on the application, hence EPOADS01, MA1ADS01, and SI1ADS01 are assigned respectively for this case):

```
MESOUTA
        EPO          <=   EPOADS01
        ESFOPER      <=   MA1ADS01
        CCXSNRS2     <=   SI1ADS01
        IDAEA1
        IDAEA2
```

Combining the information shown above, the full IC11A tree is then expanded as follows:

```
IC11A   <=   ADS-IC01
             AESOUTA
             EPO          <=      EPOADS01
             AESIPC
             CCXSNRS1     <=      SC1ADS01
             SENS1        <=      S11ADS01
             SENS2        <=      S12ADS01
             SENS3        <=      S13ADS01
             SENS4        <=      S14ADS01
             IDAEA1
             IDBEA1
             IDCEA1
             IDDEA1
             IDAEA1
             IDAEA2
             MESOUTA
             EPO          <=      EPOADS01
             ESFOPER      <=      MA1ADS01
             CCXSNRS2     <=      SI1ADS01
             IDAEA1
             IDAEA2
             DASSIND      <=      S3DADS01
             ED3EA1
```

By using the above modular fault tree linking methodology, trees that are called by many I&C subtrees functions (such as the cabinet trees) can be created and reviewed once, and then be configured in the overall I&C subtree linking along with appropriate supporting input trees as many times as is required. Thus, the same tree does not have to be modeled repeatedly in multiple trees.

Linking of I&C subtrees is performed automatically using a set of batch-run files to execute the running, renaming, and linking of the trees. Simplified versions of those files are shown in

Table 26-3a to facilitate review of I&C subtrees. Additionally, a list of all representative I&C subtrees that have been plotted is included as Table 26-3b. Note that while only plots of representative I&C subtrees are included in Reference 26-1, Table 26-3b shows the application and differences from representative subtrees, for those subtrees that are not plotted. Typically, subtrees that are not plotted are nearly identical to a representative plotted subtree, with the only difference being related to a redundant train of equipment being actuated, or LOOP or blackout operation, where only support power trees that are called differ. Note that entries of Table 26-3a match I&C subtrees that have been plotted.

### 26.4.4 Human Interactions

Generally, human interactions are modeled in the PMS fault trees where operator action is needed to initiate a manual reactor trip, manually step in the rods, and initiate ESF actuation. Note that for I&C subtrees where only manual action and no automatic action is credited, the human interactions are generally modeled in the calling system level trees and not in I&C subtrees. This facilitates correct development of logic in those system level trees. Table 26-8 lists a summary of human errors included as basic events in two reactor trip system fault trees. Note that details on the calculation of human errors are discussed in Chapter 30.

## 26.5 Discussion of Methodology

The following sections present methods that have been applied in this analysis. These are fault tree analyses (FTA) by which system level results are calculated; data manipulation, where individual part failure rates are obtained and processed for use in the FTAs as unavailabilities and failure probabilities; and common mode failure analysis, in which the contributions of common faults across redundant portions of the design are calculated.

### 26.5.1 Fault Tree Analysis

Availability and reliability of PMS I&C systems are demonstrated using fault tree analysis (FTA) methodology. The FTA method uses a quantified logic diagram showing various paths of failures and combinations of failures that can lead to an undesired event for the system being studied. The FTA determines the probability of occurrence of each part as well as the logical sum of the probabilities, which is the probability of failure of the undesired event of the system as a whole. The FTA methodology applied is consistent with the specification for reliability assessments in ANSI/IEEE-352-1987.

The following paragraphs discuss key FTA modeling and quantification methods used in analyses. The first portion of the discussion is applicable to the spurious failure rate per year calculations, and the latter portion of the discussion applies to FTAs that produce unavailability or failure upon demand results.

### 26.5.2 Unavailability

For all but one of the PMS I&C analyses, application of the FTAs for failure-upon-demand cases are performed using standard FTA unavailability application, where ORed events effectively sum event unavailabilities, while ANDed events have their respective unavailabilities multiplied. The result from FTAs directly produces final unavailabilities and no further processing is performed. This is the standard method used for evaluation of FTAs to give system level unavailabilities.

### 26.5.3 Spurious Failure Rate Per Year

As part of the evaluation of ADS, one I&C subtree was developed to determine the expected number of spurious ADS actuations per year. That I&C subtree is titled ICS. Results from that evaluation are entered into the database as a basic event node data point. The evaluated rate is equal to 5.4E-5 events / year for spurious ADS actuation. The following text describes the method used to evaluate this rate using FTA methodology.

In modeling system spurious failure rates per year, individual component probabilities of failure are entered into the tree as:

$$P(f) = 1\text{-}e^{-\lambda T}$$

This formula can be conservatively approximated as:

$$P(f) = \lambda T$$

where T is the mission time for the component, and $\lambda$ is the failure rate of the component. The above formulas yield the probability of a component failing in mission time T. However, modeling repairable redundant systems such as the PMS I&C systems, modeling probability of failure as $\lambda$ times T does not correctly model system failure scenarios in which multiple failures are required for spurious system events to occur. To correctly model multiple order events, second and higher order events must occur within the repair time (R) of the first failure. A solution to correctly model repairable redundant systems is to use a failure exposure time of two times repair time (2R) in place of the mission time when computing component probabilities of failure, and then using a multiplicative factor of mission time divided by failure exposure time (T/2R) on the final quantified system probability of failure in order to adjust the results to the desired mission time. The following discussion explains this approach.

Consider a repairable redundant system in which multiple failures are required to cause a system spurious actuation. For these cases, the first failure can occur any time during full system mission time. However, in order for a spurious actuation at system level to occur, the second failure must occur within two times the repair time of the first failure.

Consider three cases: Case 1, where both component 1 and component 2 fail during the system mission time (but at different times) and do not cause a system failure due to repair; and Cases 2

and 3, where they are two examples of failure scenarios that do cause a system spurious failure. In Case 2, component 2 fails first, and within the repair time of component 2, component 1 fails. Case 3 is the converse of this, with component 1 failing first. Case 2 and Case 3 examples show the need to model for twice the repair time.

The following discussion gives two examples of application and the effects for OR gates and AND gates in the fault tree model.

For all OR gates in the tree, resultant output effectively equals results that would have been obtained by using component input values based on $P(f) = \lambda T$. This is due to the distributive law that can be applied to OR gate logic. For an example two-part system, the OR relationship can be conservatively approximated as follows:

$$P(f:system) = P(f:part\ 1) + P(f:part\ 2)$$

Substituting values per the method presented above:

$$P(f:system) = ((\lambda_1 * 2R) + (\lambda_2 * 2R)) * T/2R$$

which reduces to:

$$P(f:system) = (\lambda_1 * T) + (\lambda_2 * T)$$

Thus, for any intermediate single-point failure nodes of the tree, this modeling method implies that any failure of these parts at any time during the full mission time T will cause loss of the intermediate function being assessed. Therefore, application of this method correctly models single point failures that can lead to the undesired system event.

For AND gates in the tree, the same method is applied. For combinations of failures, resultant output effectively equals results that would have been obtained by using component input values based on $P(f) = \lambda T$ for initial part detectable failures and $P(f) = \lambda * 2R$ for subsequent redundant part detectable failures. For an example two-part redundant system, the AND relationship where both failures are detectable can be expressed as follows:

$$P(f:system) = P(f:Part\ 1) * P(f:Part\ 2)$$

Substituting the values per the method presented above:

$$P(f:system) = ((\lambda_1 * 2R) * (\lambda_2 * 2R)) * T/2R$$

the resulting equation is:

$$P(f:system) = (\lambda_1 * T) * (\lambda_2 * 2R)$$

This method implies that a loss of function requires two failures: failure of part 1 during full mission time T, and the subsequent failure of part 2 during twice the repair time of part 1. This result is consistent with the discussion of modeling repairable redundant systems presented above. For the spurious ADS model, T = 8760 hours, and R = 4 hours. Thus, all input failure rates used in the tree are multiplied by 8 hours (2R where R = 4 hours), and the final tree result is multiplied by 1095 hours (T/2R where T = 8760 hours, and 2R = 8 hours). This produces the probability of a spurious event over mission time T, which is then converted to a failure rate per mission time T, giving the number of spurious ADS events per year that could cause a large LOCA as 5.4E-05 events/year. The number of spurious ADS events that could lead to an intermediate LOCA and a medium LOCA are 1.8E-09 events/year and 1.1E-08 events/year, respectively.

### 26.5.4 Common Cause Failures

Several common cause failures within the PMS are considered credible and accounted for explicitly during construction of fault trees. Mainly two common cause failures are identified: hardware common cause failures due to the use of the same type of boards for many subsystems, and software common cause failures.

The hardware common cause failure evaluations are based on the multiple greek letter method, which uses beta, gamma, and delta factors to represent the conditional probabilities of second-, third-, and fourth-order failures, respectively, due to common cause. These factors are then applied to random hardware failure probabilities to produce common cause failure probabilities. Both common cause failures of components within a system and common cause failures of components across systems are addressed. It should noted that the method used in calculating MGL factors for the hardware CMF include a substantial contribution due to the inclusion of software in the design. This inclusion is deliberately left in the analysis as an added measure of conservatism when considering potential impacts of software failures on the system, in addition to contributions for software common mode failure described below.

The software common cause failure evaluations are based on a model that incorporates a number of factors that can affect the development and implementation of software modules. This model yields a resultant software common mode unavailability of 1.1E-05 failures/demand for any particular software module, and a software common mode unavailability of 1.2E-06 failures/demand for software failures that would manifest themselves across all types of software modules derived from the same basic design program in all applications.

The supporting common cause failures used in analyses are presented in Table 26-9. Data files used for quantification are included in Chapter 32.

### 26.5.5 Data Manipulation

This section discusses how individual component unavailabilities and probabilities of failure are computed for input into logic in fault trees.

Data used in this analysis are computed based upon the following generic formulas for computing component probability of failure and unavailability:

Probability of failure: $P(f) = 1 - e^{-\lambda T} \approx \lambda T$

T = mission time

$\lambda$ = component failure rate

Unavailability: $\bar{A} = (MTTR)/(MTTF+MTTR)$

MTTF = mean time to failure

MTTR = mean time to repair

The above simple formulas are enhanced to correctly model board utilization for multiple channel boards and fault tolerance of the component using the following factors:

ADJ: The adjust factor is used to adjust component failure rate based upon the percentage of the components' hardware needed to perform the function modeled. For example, the failure rate for a four-channel input module that utilizes only one channel to perform the required function is adjusted appropriately with the ADJ factor to account for the fact that only failures of the channel utilized and any hardware that is common to all of the channels can affect the required function performed by the module.

FD: The fail-danger factor is used to apportion failures that are undetectable or result in the non-default or undesired state. This factor is derived from the results of the failure modes and effects analyses and functional block analyses.

The following discussion explains data manipulations performed for data sets used in quantifying failure upon demand and spurious rate of failure for PMS configurations. First, two spurious data sets are discussed, then unavailability data set are presented.

There are two data sets utilized in modeling spurious failure of PMS redundant configurations. The first of these is used to model functions in which the default state upon detection of a failure is to initiate or perform the intended function. For this model, no credit is taken for fault tolerance upon detectable failures. This yields the following equation for spurious probability of failure:

$$P(f) = \lambda * ADJ * (2 * MTTR)$$

The adjust factor is still used to credit the system for unused channels on multiple channel boards. Note also that the (2 * MTTR) term is used for mission time of the component per the discussion on fault tree modeling of spurious failure presented above.

The second data set used in modeling system spurious failure models functions in which the default state upon detection of failure is to take action other than that which could place the system at risk of giving spurious action (e.g., default state = stay as is). The formula for computing

spurious probability of failure is similar to the previous case, but factors in the fail-danger number. This formula becomes:

$$P(f) = \lambda * ADJ * FD * (2 * MTTR)$$

For modeling component unavailability, only one data set is needed for the fully redundant system configuration. The component unavailability is computed as follows:

$$\bar{A}_T = 1-(MTTF/ADJ)/((MTTF/ADJ)+FD*T/2+MTTR)$$

In this case, the MTTF is only adjusted by the adjust term, since both fail-safe and fail-danger terms are being considered. The fail-danger term is used in adding additional down time experienced by the system due to undetected failures. In this case, the average amount of down time experience due to undetected failures is computed by apportioning the mission time (T) divided by two term by the percentage of failures that can result in the nonsafe and undetectable state.

Failure probabilities calculated in this section are shown in Table 26-7.

## 26.6 References

1. *AP600 Probabilistic Risk Assessment Fault Trees*, WCAP-13275 (Proprietary) and WCAP-13404 (Nonproprietary), Revision 2.

2. *AP600 Instrumentation and Control Hardware Description (Protection and Safety Monitoring System)*, WCAP-13382, Rev. 0.

3. *AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report (Protection and Safety Monitoring System)*, WCAP-13383, Rev.0.

4. *AP600 Instrumentation and Control Defense-in Depth and Diversity Report (Protection and Safety Monitoring System, Diverse Actuation System)*, WCAP-13633, Rev. 0.

5. *Bypass Logic for the Westinghouse Integrated Protection System Addendum 2 AP600 Bypass Logic Implementation Description (Protection and Safety Monitoring System)*, WCAP-8897, Rev. 0.

6. *AP600 Instrumentation and Control Software Architecture and Operational Description (Protection and Safety Monitoring System)*, WCAP-14080, Rev. 0.

7. *Advanced Passive Plant Protection System FMEA (Protection and Safety Monitoring System)*, WCAP-13594, Rev. 0.

8. *AP600 System/Event Matrix*, WCAP-13793, Rev. 0.

9. *Joint Westinghouse Owners Group / Westinghouse Program: ATWS Rule Administration Process*, WCAP-11992, December 1988.

10. AP600 DWG. PMS-J3J-001, Process Block Diagram Index, Rev. 3., February 2, 1993.

11. AP600 DWG. PLS-J3J-001, Process Block Diagrams, Rev. 3., February 3, 1993.

12. AP600 DWG. PMS-J3J-021, Process Block Diagram Index, Rev. 2., March 2, 1993.

Table 26-1

LIST OF SYSTEM FAULT TREES

| Fault Tree Name | Description |
|---|---|
| RTPMS, RTPMS1 | Automatic and manual failure of the PMS to trip the reactor |
| RTSTP | Operator fails to manually step in the control rods after the PMS and the DAS have failed to trip the reactor |
| RCL | Failure to trip all four RCPs following a small LOCA |
| RCT | Failure to trip all four RCPs |
| RCN | Failure to trip all four RCPs following an intermediate LOCA |
| SYS-IC | Failure of the I&C systems to provide automatic and or manual actuation signals to plant equipment, incorporating the appropriate parts of the PMS and DAS |

Table 32-1 (Sheet 9 of 13)

## GENERIC DATA BASE

| Component | Failure Mode | Mean [1] (d = demand hr= hour) | Error [2] Factor | I. D. Code | Simon File Line # | Remarks |
|---|---|---|---|---|---|---|
| **ELECTRICAL COMPONENTS (cont.)** | | | | | | |
| 37. Circuit Breaker (<600 V) | Failure to close | 1.0E-3 /d | 10 | ---CR---VC | # 491 | To be added to pumps, fans, etc. powered by 480-vac substation |
| | Failure to close (standby rate) | 2.8E-6 /hr | 10 | ---CR---GC | # 492 | |
| | Failure to open | 1.0E-3 /d | 10 | ---CR---VO | # 493 | Derived from failure rate per demand (See note 29) |
| | Failure to open (standby rate) | 1.0E-7 /hr | 10 | ---CR---GO | # 494 | |
| | Spurious open | 5.0E-7 /hr | 3 | ---CR---RQ | # 495 | |
| 38. Reactor Trip Breaker (PWR) | Failure to operate | 3.54E-6/hr | 10 | ---RB---FA | --- | (See note 30) |
| 39. Relay (electromechanical) | Contacts fail to operate (open or close) | 1.0E-4 /d | 10 | ---RE---CA | # 561 | Error factor from Reference 2. (See note 16) |
| | Contacts fail to operate (open or close - standby rate) | 5.0E-7 /hr | 10 | ---RE---GA | # 562 | (See notes 16, 25) |
| | Operate spuriously to deenergize state | 1.0E-6 /hr | 10 | ---RE---DQ | # 563 | (See notes 17, 25) |
| | Operates spuriously to energized state | 5.0E-7 /hr | 10 | ---RE---EQ | # 565 | (See notes 18, 25) |
| | Static transfer switch fails to transfer | 2.5E-6 /hr | 10 | ---RE---TA | # 566 | The failure rate was assumed 5 times higher than that for relay due to more complexity of the component. |
| 40. Time-delay Relay (electromechanical) | Failure to operate (standby rate) | 5.0E-6 /hr | 3 | ---TD---TA | # 571 | (See note 25) |
| | Premature operation | 3.0E-4 /hr | 10 | ---TD---TQ | # 572 | From Reference 2 |

Table 32-1 (Sheet 10 of 13)

## GENERIC DATA BASE

| Component | Failure Mode | Mean [1] (d = demand hr= hour) | Error [1] Factor | I. D. Code | Simon File Line # | Remarks |
|---|---|---|---|---|---|---|
| **ELECTRICAL COMPONENTS (cont.)** | | | | | | |
| 41. Electrical Buswork | Failure during operation | 2.0E-7 /hr | 5 | ---BS---LP | # 531 | Also applied for distribution panels and 120-vdc switchboards |
| 42. Transformer | High voltage: failure to continue operating | 1.2E-6 /hr | 3 | ---TR---HF | # 541 | Error factor from Reference 2 |
| | 4.16 kv to 480v: failure to continue operating | 7.0E-7 /hr | 3 | ---TR---MF | # 542 | Error factor from Reference 2 |
| | Low voltage: failure to continue operating | 8.0E-7 /hr | 3 | ---TR---LP | # 543 | Error factor from Reference 2 |
| 43. Diesel Generator | | | | | | Includes engine frame and associated moving parts, generator, coupling, governor, output breaker, static exciter, lube oil system, fuel oil, intake and exhaust air, starting system; excludes starting air compressor and accumulator, fueling storage and transfer, load sequences, and synchronizers. (See note 19) |
| | Failure to start and load | 1.4E-2 /d | 3 | ---DG---DS | # 551 | This is the failure to start, accept load, and run for 1/2 hour. |
| | Failure to start and load (standby rate) | 3.0E-5 /hr | 3 | ---DG---FS | # 552 | |
| | Failure to run, given start | 2.4E-3 /hr | 10 | ---DG---DR | # 553 | This is the failure to run for more than 1/2 hour, given start. |
| 44. Standby Combustion Turbine - Generator | Failure to start | 2.5E-2 /d | 10 | ---CT---ES | # 555 | This is the failure to start, accept load, and run for 1/2 hour. (See note 25) |
| | Failure to start (standby rate) | 9.0E-5 /hr | 10 | ---CT---FS | # 556 | (See note 25) |
| | Fails to run after starting | 1.0E-5 /hr | 10 | ---CT---DR | # 557 | This is the failure to run for more than 1/2 hour, given start. (See note 25) |

15. Leakage from the tubes in a passive residual heat removal (PRHR) heat exchanger can lead to the need to isolate the heat exchanger (automatically or manually, depending on the plant design), thereby rendering it unavailable. Because of the quality of water in these heat exchangers and the very low rate of plugging of heat exchangers in general, the plugging failure mode has a negligible rate of occurrence.
16. The failure to operate includes both failure of the relay coil and failure of the contacts to open or close on demand.
17. The failure rate for spurious operation to the energized state includes failure of the relay coil by opening or shorting to ground and spurious opening or closing of the relay contacts (whichever is applicable for the deenergized position of the relay).
18. The failure rate for spurious operation to the energized state includes shorting of the relay coil to power and spurious opening or closing of the relay contacts (as appropriate).
19. The nonsafety diesel generators have a slow load pick up and, therefore, a lower stress during starting sequence. Similar standby and operating failure rate obtained for the safety diesel generators can be considered applicable also to nonsafety ones.
    This consideration is supported by the results of the survey performed for 17 diesel generators of six ENEL fossil electric plants (Reference 6).
20. The open circuit failure rate is used for the cables which are not in conduit or closed tray.
    The short to ground failure rate is used for 150 KVAC or 380 KVAC cables.
    The short to power is used for 4.16 KVAC, 480 VAC, 125 VAC, 120 VAC because they are isolated from the ground, and the short to ground is supposed to be alarmed and does not cause a direct failure.
21. Reference 1 lists different failure rates for pressure, level and flow transmitters.
    Although these failures account for sensor and transmitter, the major failure contribution comes from the transmitter. Pressure, level, and flow transmitters are practically the same, due to the fact that they sense always a differential pressure. Therefore, there are no reasons for which these transmitters should have different failure rates.
    To accommodate that, a geometric average among the failure rates reported in Reference 1 are evaluated and assigned to those components.
    Summarizing, we have:
    - failure to response to change in process:
      $(4.8E\text{-}7 \times 1.0E\text{-}6 \times 4.6E\text{-}7)^{1/3} = 6.0E\text{-}7/hr$
    - failure maximum or zero:
      $(2.7E\text{-}7 \times 6.4E\text{-}7 \times 2.1E\text{-}6)^{1/3} = 7.1E\text{-}7/hr$
    - drift high or zero:
      $(3.3E\text{-}7 \times 5.1E\text{-}7 \times 1.7E\text{-}6)^{1/3} = 6.6E\text{-}7/hr$
22. These failures are generally detected by the channel check performed every 12 hours or 24 hours or by gross failure alarm.
23. There is no data for motor-operated valve (MOV) reverse leakage in Reference 1; therefore, the ratio of check valve to MOV reverse leakage failure rates from Reference 6 is used to derive the reverse leakage failure rate for MOV: 1.0E-6 /hr * 0.2 = 2.0E-7 /hr.
24. This data is originally provided by ENEL. However, there is no documentation available for the data source; therefore, it will be treated as "expert judgment."
25. No error factor is available; an engineering assessment is made.
26. If the water chemistry is controlled and there are devices to prevent the drop of plugging material (e.g., screen), the failure rate of orifice plugging in a system with normally stagnant water is assumed to be 0.1 of the failure rate for continuously flushed lines.
27. The AP600 design includes explosive valves because of their high reliability and suitability to a function where there is a one-time need for the valve to actuate. This reputation is supported by the use of explosive valves in many designs where the valve cannot fail to perform its function. Examples of these designs include

weapons systems and space systems. The explosive valve design is simple and there are few ways for the valve to fail to actuate. This type of design contrasts with the designs of air-operated or motor-operated valves, which have more moving parts that can fail and prevent the valve from actuating.

The ALWR URD (Reference 32-1) indicates a failure probability (failure to operate) for explosive valves of 3E-03 per demand. This failure rate does not indicate a valve design with extremely high reliability, as would be expected. This may be because the basis for the URD value is a small population of valves and extrapolation from older, less relevant data.

Sandia Laboratories have worked on designs of weapons systems and space systems where explosive valves are commonly used. They were consulted to verify the URD failure probability. Two sources at Sandia produced failure data based on a large population of explosive valves. The data produced failure probabilities of 2.0E-04 per demand and 3.2E-04 per demand.

Each of these values is relevant to the AP600 explosive valve failures. A geometric mean of the URD value and the Sandia values produces a failure probability of 5.8E-04 per demand $[\{(3.0E-03) * (2.0E-04) * (3.2E-04)\}^{1/3}]$.

28. These breakers (>4 kv) are similar to those used in Westinghouse operating nuclear power plants. The ALWR URD indicates the failure probability (fail to open) for such breakers is 5E-04 per demand. From this an hourly failure rate was derived, 1.4E-06 /hr. This failure rate does not agree with experience, and a search through the NPRDS database was performed to verify the URD value. The search produced a large population from which a failure rate of 4.8E-07 /hr was calculated (Reference 32-8). This is the value used in the AP600 PRA models.

29. These breakers (<600 v) are similar to those used in Westinghouse operating nuclear power plants. The ALWR URD indicates the failure probability (fail to open) for such breakers is 1E-07 per demand. From this an hourly failure rate was derived, 2.8E-06 /hr. This failure rate does not agree with experience, and a search through the NPRDS database was performed to verify the URD value. The search produced a large population from which a failure rate of 1E-03 /hr was calculated (Reference 32-8). This is the value used in the AP600 PRA models.

30. The failure rate for the reactor trip breakers is determined using a proprietary calculation. This calculation is based on IEEE-STD-500 and is supported by plant data for Westinghouse plants.

For steam generator tube rupture sequences, the majority of the core damage frequency includes successful operation of the passive residual heat removal system. This depressurizes the reactor coolant system and stops the leak through the ruptured tube to the secondary side. Core damage is conservatively assumed because the automatic depressurization system was not actuated to depressurize the reactor coolant system to the containment pressure, or the lost reactor coolant system inventory was not replaced.

In these cases, the operators have several hours (which are not credited in the Level 1 analysis) to determine the problem and act to fully depressurize the reactor coolant system as instructed by FR.C-1 ERG. Depressurization of the primary side will ensure the steam generator tubes are covered with water. The water will provide decontamination of any leakage from the primary side should that occur.

The post-core-damage depressurization is dominated by the failure of the operators to diagnose the problem and act accordingly. The hardware failure is significantly less than the potential for the operators to fail.

In the steam generator tube rupture case where the passive residual heat removal system is successful, followed by successful automatic depressurization system actuation and in-containment refueling water storage tank injection, and the failure of recirculation, core damage is assumed in the level 1 analysis. With these circumstances, the loss of reactor coolant system fluid to the secondary side would be stopped due to the low primary-side pressure and the high water level in the faulted steam generator. This scenario assumes that the faulted steam generator would be kept filled, and the tubes would be covered.

Other accident classes are marked by depressurization below 150 psi by virtue of the accident progression and are guaranteed success at this top event.

The equipment used to diagnose the high-pressure condition and depressurize the reactor coolant system for success at node DP is safety-related and covered under the design-basis equipment qualification program. The operator action is credited within the conditions of ERG FR.C-1.

### 35.7.2 Top Event IS - Containment Isolation

Nodal Question: Is the containment isolated prior to core damage?

Success Criterion: One isolation valve closed in each penetration line prior to core damage subject to the screening action discussed in Chapter 24

Severe Accident Phenomenon Addressed: Initial containment integrity

Actuation: Automatic through protection and safety monitoring system (PMS) or manual

Post-Core-Uncovery Cue for Operator Action: ERG E-0 entered at reactor trip or safety injection signal

Successful containment isolation determines initial containment integrity. If the containment is not isolated, the result is a fission-product release to the environment from the initial stages of core damage. The containment is isolated by the protection and safety monitoring system or by the operator at step 5 in the E-0 ERG. Containment isolation is required before the accident conditions exceed the design basis after core uncovery. The time available prior to significant fission-product release for the operator to isolate the containment is approximately 1 hour (Reference 35-4), except in the 3A, 3BR, and 3C accident classes, in which core damage occurs relatively quickly due to inability to reflood the vessel. In accident classes 3A, 3BR, and 3C, only automatic containment isolation is credited.

Equipment survivability of the containment isolation system is covered under the design-basis equipment qualification program. A fault tree evaluating hardware and operator success is linked to top event IS to quantify success of containment isolation.

### 35.7.3 Top Event IR - Reactor Cavity Flooding

Nodal Question: Is the in-containment refueling water storage tank water level in the reactor cavity sufficient to submerge the reactor vessel above the elevation of the in-vessel core debris?

Success Criteria: 2 of 2 valves open in 1 of 2 recirculation lines from the in-containment refueling water storage tank to containment sump or in-containment refueling water storage tank injection through the progression of the accident

Severe Accident Phenomena Addressed: Reactor vessel integrity

Actuation: Automatic or manual

Post-Core-Uncovery Cue for Operator Action: ERG FR.C-1, very high containment radiation

The basis for in-vessel retention (IVR) of molten core debris in the AP600 is the DOE/ARSAP report (Reference 35-1) on IVR. Success of IVR is demonstrated if the outside of the reactor vessel is submerged in water at least to an equivalent elevation as the in-vessel molten debris pool. The cavity water level must be at least to the 83' elevation within 45 minutes and at least to the 86' elevation within 75 minutes after core damage. The operator determines that the cavity needs to be flooded in ERG FR.C-1 based on inability to recover RCS injection or very high radiation in the containment. The required elevations for successful flooding are based on covering the entire hemispherical portion of the lower head before the earliest time of debris relocation to the lower head (Appendix P of Reference 35-1) and covering the maximum estimated depth of molten core debris before the failure of the support plate into the lower head. Failure at node IR is conservatively assumed to result in

Table 35-6

**SUMMARY OF OPERATOR ACTIONS CREDITED ON CONTAINMENT EVENT TREE**

| Top Event | Description of Operator Error | Event ID | Cue(s) | Time Window |
|---|---|---|---|---|
| DP | Failure to recognize need for post-core uncovery RCS depress during small LOCA or transient with loss of PRHR | LPM-REC01 | core-exit T/C > 1200°F (ERG FR.C-1) | 20 minutes |
| | Failure to complete ADS as recovery from failure of automatic actuation or manual actuation after core damage | ADN-REC01 | core-exit T/C > 1200°F (ERG FR.C-1) | 20 minutes |
| IS | Failure to recognize need and failure to isolate the containment, given core damage following an accident | CIC-MAN01 | high containment pressure, high containment temperature, high containment radiation (ERG E-0) | 60 minutes |
| PC | Failure to recognize need and failure to open PCS water valves to drain cooling water on containment shell | PCN-MAN01 | high containment pressure (ERG E-0) | 60 minutes |
| IR | Failure to recognize need and failure to open recirculation valves to flood reactor cavity after core damage | REN-MAN03 | high containment radiation, core-exit temperature > 1200°F (ERG FR.C-1) | 20 minutes |
| IG | Failure to recognize need and failure to actuate hydrogen control system, given core damage following an accident | VLN-MAN01 | core-exit T/C > 1200°F (ERG FR.C-1) | 15 minutes |

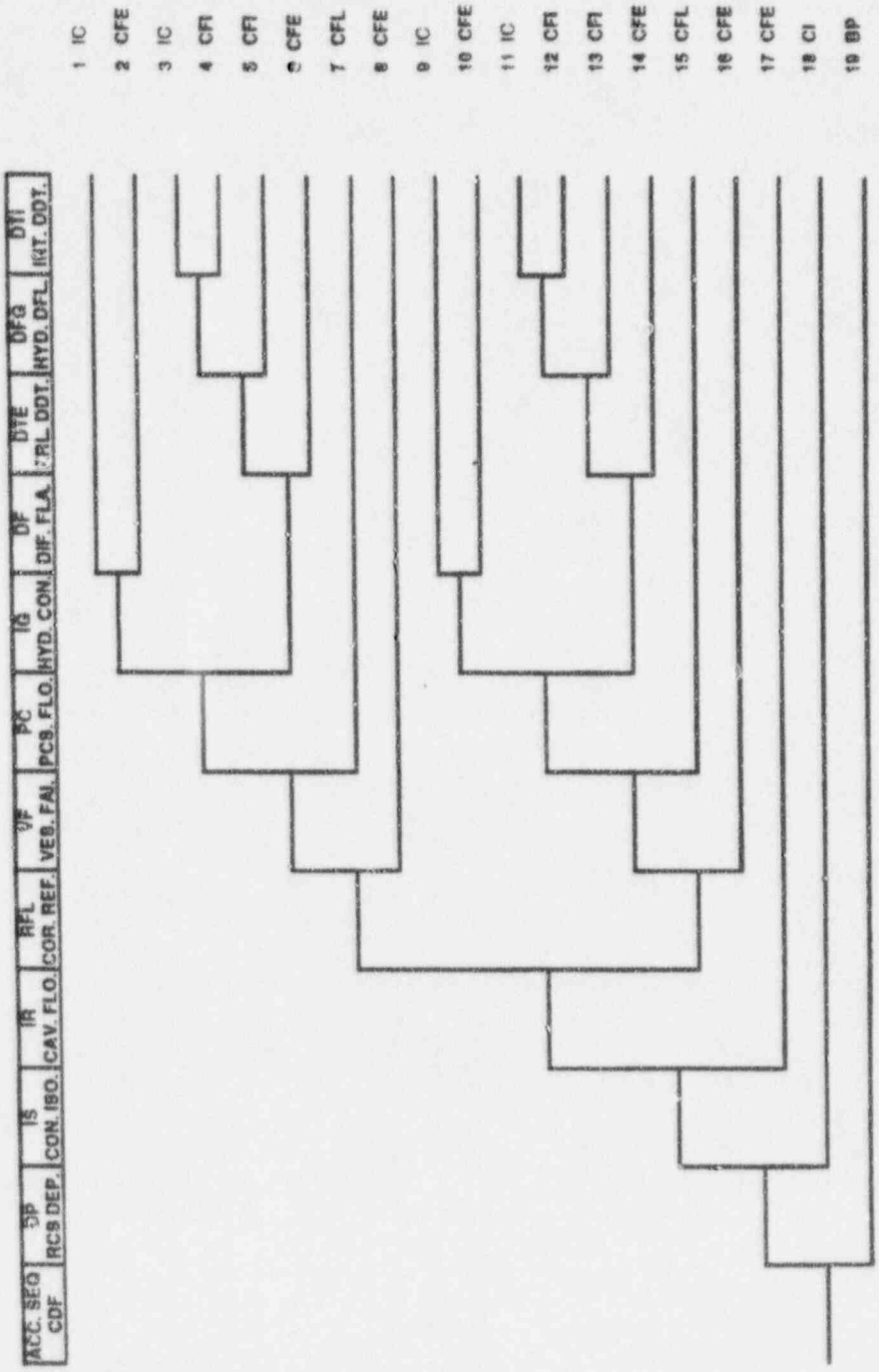



Figure 35-1

Containment Event Tree

Table 36-1

**SUMMARY TABLE FOR RCS DEPRESSURIZATION (CET NODE DP)**

| Accident Class | Failure Probability |
|---|---|
| 1A | ADTLT |
| 1AP | ADTLT |
| 1D | 0 |
| 3A | ADALT* |
| 3BR | 0 |
| 3BE | 0 |
| 3BL | 0 |
| 3C | 0 |
| 3D | 0 |
| 6 | Failure of operator to actuate ADS |

*ADALT = CM2NL + RCN + PRTA + OTH-SGTR
Fault trees CM2NL, RCN, and PRTA are discussed in Chapter 6.
OTH-SGTR is a scalar value, SGTR, defined in Chapter 31.

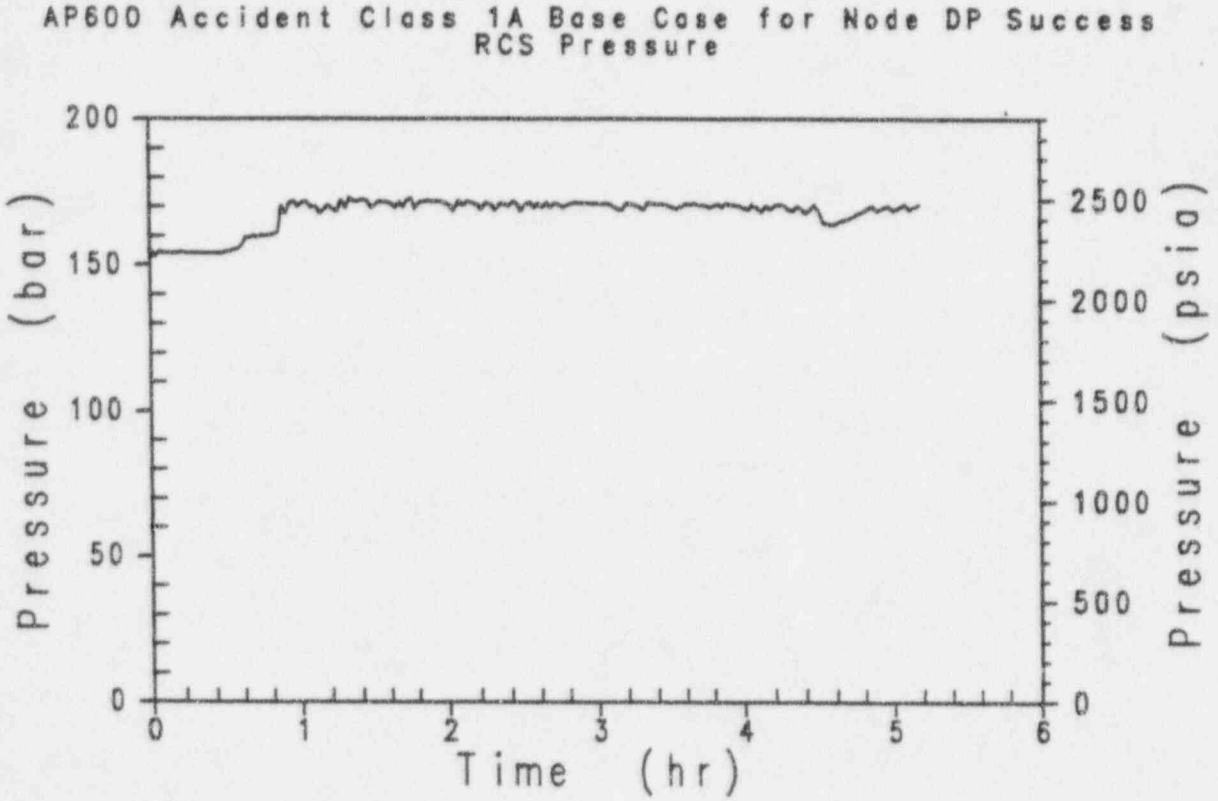



Figure 36-1

**AP600 Accident Class 1A Base Case for Node DP Success -- RCS Pressure**

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

successfully. Core damage occurs later as a result of failure of water recirculation to the pressure vessel. The time to core damage for sequences in this accident class will be significantly greater than 1 hour. Fault tree CIC is linked to node IS for this accident class. For this conservative accident class, the time to core damage will be significantly greater than 1 hour, but the fault tree assumes only 1 hour is available.

### 37.3.6 Accident Class 3C

Accident class 3C consists of sequences with vessel rupture resulting in core damage. For these sequences, there is a probability that the vessel rupture could result in containment damage, which would render containment isolation impossible. This probability is represented by the scalar value OTH-CNB, discussed in Chapter 31.

If containment isolation has not failed as a result of the vessel rupture, then containment isolation can be achieved through the protection and safety monitoring system; no credit is taken for the operator to isolate containment given the relatively short time before core damage. The failure probability for containment isolation for this case is represented by fault tree CID. This fault tree and the scalar OTH-CNB are linked to node IS for this accident class.

### 37.3.7 Accident Class 3D/1D

Accident classes 3D and 1D consist of fault sequences for which partial depressurization only occurs. Core uncovery for these sequences would occur later than the bounding accident sequence used to arrive at the fastest time to core uncovery in Reference 37-1. Therefore, fault tree CIC (automatic and manual actuation credited) is linked to node IS for this accident class.

### 37.3.8 Accident Class 6

Accident class 6 contains fault sequences for steam generator tube ruptures (SGTRs). For those sequences where passive residual heat removal (PRHR) is successful but the automatic depressurization system (ADS) has not been actuated, the operators have a significant amount of time to actuate the automatic depressurization system and fully depressurize the primary side of the reactor coolant system. The operation of the passive residual heat removal system and the actuation of the automatic depressurization system will ensure that the leak flow will be stopped and the steam generator tubes will be covered. The water covering the steam generator tubes ensures that the release from the primary side is decontaminated before it enters the environment.

For those steam generator tube rupture sequences with successful actuation of the passive residual heat removal system and automatic depressurization system, but failure of recirculation, the primary side is depressurized and the steam generator tubes are covered. Actuation of the automatic depressurization system opens a pathway from the reactor coolant system to the containment, and containment isolation is necessary to mitigate a release through any containment penetrations. After the automatic depressurization system is actuated, the

accident is bounded by the accident in Reference 37-1, and the fault tree CIC (automatic and manual actuation of containment isolation) is linked to node IS for this accident.

## 37.4 Summary

Success at node IS in the containment event tree is defined as the closure of one isolation valve in each of the containment penetrations prior to the onset of core damage. The fault tree/scalar values used to determine the failure probability for each accident class are summarized in Table 37-1.

## 37.5 References

37-1 Position Paper on AP600 Specific Time Delay in the Physically Based Source Term, Westinghouse Letter Number NTD-NRC-94-4335, November 1994.

Table 37-1

**SUMMARY TABLE FOR CONTAINMENT ISOLATION (CET NODE IS)**

| Accident Class | Failure Probability* |
|---|---|
| 1A | CIC |
| 1AP | CIC |
| 3A | CID |
| 3BR | CID |
| 3BE | CIC |
| 3BL | CIC |
| 3C | OTH-CNB + CID |
| 3D/1D | CIC |
| 6 | CIC |

Notes:

* Fault tree CIC is discussed in Chapter 24.
Fault tree CID is the same as CIC, but with the operator action failure probability set to 1.0.
OTH-CNB is a scalar value discussed in Chapter 31.
+ represents an OR in Boolean logic.

slow and the level in the valve vault will rise. A plot of the water level in valve vault and reactor cavity is provided in Figure 38-1.

The dominant Level 1 PRA sequences, as presented in Table 33-4, were examined (accounting for more than 99 percent of the total core damage frequency) to find the proportion of accident class 3BE sequences that had a direct vessel injection line break as their initiating event. PRA sequences number 1, 3, 4, 10, 27, 28, 31, 37, and 41 (total sequence probability 7.8E-08) are 3BE sequences. Of these, only sequence 1 (sequence probability 3.4E-08) was initiated by a direct vessel injection line break. Therefore, 0.44 of the 3BE sequence's probability results from direct vessel injection line breaks.

To determine if the valve vault is flooded by the in-containment refueling water storage tank water, the failure probability of the gravity injection line valves opening must be calculated. Given that the squib valves in the intact direct vessel injection line have failed to open (a pre-condition of core damage), it is necessary to find the proportion of in-containment refueling water storage tank line failures that result in both lines failing. In those cases, valve vault flooding is not possible. Failure of one line of the in-containment refueling water storage tank is modeled using fault tree IW1A (failure probability 3.3E-04). Failure of both lines is modeled by IW2AB (failure probability 6.9E-05). The conditional probability of both lines failing, given that one has failed, is 6.9E-05/3.3E-04 = 0.21.

Therefore, reflooding will NOT occur if the initiating event is a direct vessel injection line break (probability = 0.44) AND the in-containment refueling water storage tank failure affects both injection lines (probability = 0.21). Therefore, the total RFL failure probability for accident class 3BE is 0.44 x 0.21 = 0.09.

A similar argument to that presented above is used to calculate the scalar RFL for the focused PRA. However, because the focused PRA assumes all nonsafety-related systems fail, the relative importance of sequences that include nonsafety systems (such as sequences with a small LOCA as an initiating event) will increase. The conditional probability of both in-containment refueling water storage tank injection lines failing given that one has failed will also change, as some electrical systems and diverse activation system (DAS) functions are not claimed in the focused PRA. Examination of the results of the focused PRA shows that 0.208 of the 3BE sequence's probability results from direct vessel injection line break (compared to 0.441 for the baseline PRA). For the focused PRA, the probability of fault tree IW1A is 5.04E-04, and the probability of fault tree IW2AB is 1.61E-04. Therefore, for the focused PRA, the conditional probability of both lines failing, given that one has failed, is 1.61E-04/5.04E-04 = 0.32. The failure probability for the focused PRA for node RFL is 0.208 x 0.32 = 0.07. The difference between the baseline and the focused PRA sensitivity is not significant.

### 38.3.4 Accident Class 3BL

Accident class 3BL bins accident sequences in which gravity recirculation fails. Gravity injection is successful for accident class 3BL. However, the ability to recirculate water from

the containment sump to the reactor vessel fails, and the core is eventually uncovered. By definition of accident class 3B, water is not available to reflood the core, so a failure probability of 1 is applied for scalar RFL for accident class 3BL.

### 38.3.5 Accident Class 3D/1D

Accident classes 3D and 1D bin accident sequences that are partially depressurized such that sufficient gravity injection fails. For success at node RFL, full depressurization must be achieved. Therefore, the core debris cannot be reflooded and a failure probability of 1 is applied for RFL in accident class 3D/1D.

It is noted that no reflooding of the core is optimistic from the point of view of hydrogen generation, as some limited water injection may occur given that partial depressurization has occurred. For this reason, the hydrogen generation analysis (Chapter 41) for accident class 3D assumes that limited water injection is available to react with unoxidized zircaloy molten core debris.

### 38.3.6 Accident Class 6

Accident class 6 contains fault sequences for steam generator tube ruptures (SGTR). The steam generator tube rupture sequences that do not represent a containment bypass contain the successful operation of the passive residual heat removal system, the automatic depressurization system, and injection from the in-containment refueling water storage tank. Some of these sequences contain a failure of recirculation. The failure of recirculation precludes the success of reflooding the core through the recirculation lines. A failure probability of 1 is applied for scalar RFL for accident class 6.

### 38.3.7 Accident Class 3C

Accident class 3C bins sequences that are initiated by a large failure of the reactor vessel below the top of the core. Core damage is a single failure cutset and occurs due to the inability to fully reflood the core before the reactor cavity fills with water above the level of the failure. The vessel failure depressurizes the RCS and the ADS is actuated providing a flowpath into the vessel and a vent pathway for the steam from the vessel. Therefore, as the cavity fills with water, the vessel and the damaged core are reflooded by the progression of the accident. Therefore, a failure probability of 0 is assigned to accident class 3C.

### 38.3.8 Accident Class 3A

Accident class 3A bins ATWS sequences which produce core damage. The failure of the RCS piping due to overpressure in the 3A sequences is assessed at node DP, and failure is assigned to the bypass release category BP. Therefore, at node RFL for accident class 3A, the RCS piping is intact and the coolant inventory losses are mitigated. The core is covered and cooled. Node RFL is assigned a failure probability of 0 for accident class 3A.

## 38.4 Summary

The scalar failure probabilities applied to containment event tree node RFL have been developed for each accident class and are summarized in Table 38-1. Success for node RFL is defined as core debris reflooding. The success criteria require full system depressurization and a flowpath for water injection into the reactor coolant system.

Table 38-1

SUMMARY TABLE FOR REFLOODING (CET NODE RFL)

| Accident Class | Failure Probability |
|---|---|
| 1A | 0 |
| 1AP | 0 |
| 3BR | 0 |
| 3BE | 0.09 baseline PRA<br>0.07 focused PRA |
| 3BL | 1 |
| 3D/1D | 1 |
| 3C | 0 |
| 3A | 0 |
| 6 | 1 |

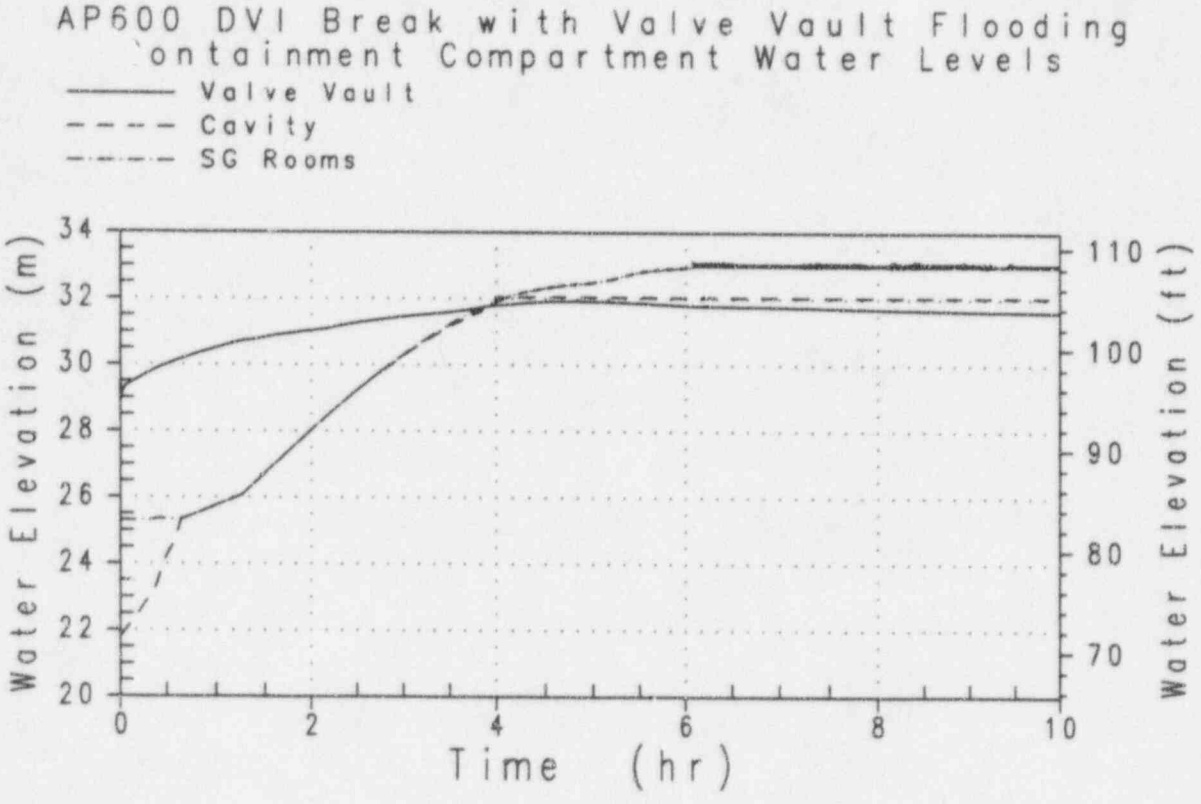



Figure 38-1

**AP600 DVI Break with Valve Vault Flooding Containment Compartment Water Levels**

head is greater than 45 minutes after initiation of rapid oxidation in the core. The top of the reactor vessel hemisphere is at the 83' elevation in the containment (reactor cavity floor elevation is 71' 6"). Therefore, to meet the first criterion, the water level must be greater than the 83' elevation within 45 minutes of the rapid core oxidation.

Full relocation of core debris after core support plate slump occurs more than 75 minutes after initiation of rapid core oxidation. The height of the core debris and the uncertainties in height are discussed in Chapter 7 of Reference 39-1. Maximum debris pool depth is 2.8 meters in the lower head. This depth corresponds to a containment elevation of approximately 86'. Therefore, to meet the second criterion, the water level must be greater than the 86' elevation within 75 minutes of rapid core oxidation. Based on this elevation, core makeup tank (CMT) water and accumulator water alone are not sufficient to prevent vessel failure, and the in-containment refueling water storage tank water must be drained into the floodable region of the containment to achieve water cooling of the reactor vessel.

The success criteria are summarized as follows:

- Cavity water elevation greater than 83' within 45 minutes of rapid cladding oxidation
- Cavity water elevation greater than 86' within 75 minutes of rapid cladding oxidation

### 39.4.1.2 Manual Action Success Criteria

The operator action to flood the cavity is determined in Emergency Response Guideline (ERG) FR.C-1, which instructs the operator to flood the reactor cavity if injection to the RCS cannot be recovered or containment radiation reaches levels that indicate fission-product releases as determined by a core damage assessment guideline. The high core-exit temperature and containment radiation levels coincide with rapid core oxidation.

Flooding rates for one and two cavity flooding lines open are presented in Figure 39-7. With one flooding line open, the 83' elevation is reached within 20 minutes of opening the valves and the 86' elevation is reached within 40 minutes. At least 25 minutes are available for the operator to open the cavity flooding valves after rapid core oxidation signals the need for cavity flooding. Water in the cavity prior to the operator action is conservatively neglected.

The criterion used for operator action to flood the cavity is the manual opening of at least 1 of 2 cavity flooding lines within 20 minutes of rapid core oxidation as evidenced by very high core-exit thermocouple readings or very high containment radiation readings.

### 39.4.1.3 Limited In-Vessel Debris Relocation

In accident classes 3A, recovered anticipated transient without scram (ATWS) sequences with success at node DP, and depressurized 1A and 1AP, core damage is limited, no significant debris relocation to the lower vessel is predicted, and the reactor vessel remains water filled. In these cases, success is credited at node IR since there is no molten core debris in the lower head.

### 39.4.2 Cavity Flooding Scenario Dependencies

#### 39.4.2.1 Accident Class 3BE

Accident class 3BE contains core damage sequences in which the reactor coolant system is fully depressurized but gravity injection is failed. Since the in-containment refueling water storage tank water injection fails, an operator action is required to flood the reactor cavity. Fault tree IWF (see Chapter 12) is linked to node IR in accident class 3BE to evaluate the probability of hardware and human action failure in cavity flooding.

In a significant fraction of the 3BE frequency, a direct vessel injection (DVI) line is failed and the intact injection line is plugged or the valves fail to open. In these sequences, the in-containment refueling water storage tank water can drain from the broken side of the direct vessel injection line, through the drain from the valve vault to the floodable region of the containment, as discussed in Chapter 38 for containment event tree node RFL. The manual action to flood is not required in this case. Conservatively, only the operator action to flood the cavity is credited at node IR for accident class 3BE.

#### 39.4.2.2 Accident Class 3BL

Accident class 3BL contains severe accident sequences in which long-term recirculation of the in-containment refueling water storage tank water fails. In these cases, the in-containment refueling water storage tank water has successfully injected into the cavity before core damage, but is unable to recirculate. Cavity flooding to cool the reactor vessel is guaranteed by progression of the accident sequence. A failure probability of zero is assigned to node IR for accident class 3BL.

#### 39.4.2.3 Accident Class 3A

Accident class 3A contains anticipated transient without scram sequences that damage the core. At the IR node in the containment event tree, node DP is successful for accident class 3A, which means that the reactor coolant system is intact throughout the pressure transient, and the passive residual heat removal system is providing long-term heat removal. Core damage is assumed, although it would be very limited, and no core debris is accumulated in the lower head. Although there is no cavity flooding, success is achieved by the lack of debris in the lower head. A failure probability of zero is assigned to node IR for accident class 3A.

#### 39.4.2.4 Accident Class 3C

Accident class 3C contains core damage sequences initiated by rupture of the reactor vessel below the elevation of the core. Safety injection is successful, but unable to reflood the core before filling the floodable region of the containment. Cavity flooding is achieved through progression of the accident sequence. A failure probability of zero is assigned to node IR for accident class 3C.

The results of the analyses showed that the insulation was able to meet each of the defined functional requirements. The design of the reactor vessel insulation provides an engineered pathway for water-cooling the vessel and for venting steam from the reactor cavity. Design changes to the insulation were completed to ensure that the stress and deflection requirements were met to provide adequate pathways for ingress of water and venting of steam.

## 39.6 Reactor Vessel External Surface Treatment

Based on the reactor vessel system design specification, the only treatment of the external surface of the reactor vessel is a protective paint applied by the manufacturer prior to shipping. The paint protects the vessel carbon steel surface during shipping and storage. Removal of external surface paint, or any other treatment of the external reactor vessel surface, is not expected to occur.

The ULPU testing includes tests using prototypical steel with paint applied according to Westinghouse paint application specifications. The aged paint surface actually increased the wetability of the vessel external surface and increased the critical heat flux. In the PRA, it is assumed that no external surface treatment of the reactor vessel impairs heat removal from the vessel external surface.

## 39.7 Reactor Vessel Failure (Node VF)

### 39.7.1 Node VF Success Criteria

The question considered at node VF to determine success or failure of reactor vessel integrity is:

Is the core debris maintained inside the reactor vessel?

Success is credited at node VF if debris is maintained in the reactor vessel and relocation to the containment is prevented. Based on the ROAAM analysis of in-vessel retention, an intact reactor vessel remains intact if the reactor coolant system is depressurized (success at node DP) and the reactor vessel is adequately submerged (success at node IR). However, in accident class 3C, the vessel rupture initiating event, the vessel is failed prior to core damage and relocation. In this case, success is credited if vessel failure does not allow debris relocation to the cavity.

Success criteria are as follows:

- For all accident classes except 3C, success of node DP and node IR results in success at node VF.
- For accident class 3C, success at node DP and node IR, and maintaining the debris inside the faulted reactor vessel, result in success at node VF.

For all accident classes except 3C (vessel rupture initiating event), maintaining the debris in the vessel is ensured by vessel integrity (success at nodes IR and DP). In accident class 3C, the vessel is failed below the intact core as a result of the initiating event. Since vessel rupture produces core damage, regardless of system availability, the failure of ADS and gravity injection has negligible frequency in accident class 3C. Core damage is caused by the inability to reflood the core until the reactor cavity is filled. AP600 has the unique cavity flooding feature that, once the cavity is filled up to the break, water can reflood back into the vessel as the containment compartments fill to arrest core damage before full core relocation. Only a limited amount of debris is likely to relocate to the lower head. The most likely failure for the reactor vessel initiating event is a local failure above the top of the lower head hemisphere at the beltline of the vessel. This location has the highest fluence and brittleness from exposure. Debris relocated into the lower head is guaranteed to be water cooled in the vessel. Therefore, for accident class 3C, a scalar failure probability value of 0.1 for debris relocation is assigned to node VF. A sensitivity to this value is investigated and discussed in Chapter 43.

## 39.8 Summary

The fault trees and scalar values linked for nodes IR and VF are summarized in Tables 39-2 and 39-3, respectively.

## 39.9 References

39-1 Theofanous, T.G., et al., "In-Vessel Coolability and Retention of a Core Melt," DOE/ID-10460, July 1995.

39-2 Theofanous, T.G., et al., "Lower Head Integrity Under In-Vessel Steam Explosion Loads," DOE/ID-10541, released for peer review, July 1995.

39-3 Theofanous, T.G., "On the Proper Formulation of Safety Goals and Assessment of Safety Margins for Rare and High-Consequence Hazards," Reliability Engineering & Systems Safety, Summer 1996.

39-4 Theofanous, T.G., et al., "The Probability of Mark-I Containment Failure by Melt Attack on the Liner," NUREG/CR-6025, November 1993.

39-5 Theofanous, T.G., et al., "The Probability of Containment Failure by Direct Containment Heating in Zion," NUREG/CR-6075, December 1994.

detonation by sufficiently high-energy sources from any objects in the containment during accident conditions does not exist (Reference 41-2). Deflagration-to-detonation transition is considered, and the method of NUREG/CR-4803 (Reference 41-6) is used to evaluate the potential for flame acceleration. This method is summarized in Section 41.8.

Since the lowest hydrogen concentration for which deflagration-to-detonation transition has been observed in the intermediate-scale FLAME facility at Sandia is 15 percent (Reference 41-7), and 10 CFR 50.34(f) limits hydrogen concentration to less than 10 percent, the likelihood of deflagration-to-detonation transition is assumed to be zero if the hydrogen concentration is less than 10 percent. Containment failure is assumed if a detonation is predicted.

### 41.3.5 Igniter System

The availability of the igniter system for each accident sequence is evaluated by fault tree VLH (Chapter 16) and linked to the containment event tree node IG for all accident sequences. The AP600 igniter system, if operational during a severe accident, will burn hydrogen as soon as the lean upward flammability limits are met. Thus, the concentration of hydrogen is maintained, on average, at the lean upward flammability limits. However, depending on the hydrogen release rate, location and oxygen availability, locally high concentrations may exist in the in-containment refueling water storage tank or in the subcompartment where the pipe break occurs. According to the MAAP4 analysis to demonstrate the AP600 compliance with 10 CFR 50.34(f) presented in this chapter, hydrogen combustion due to the operation of the igniter system results in uniformly distributed hydrogen concentrations less than 10 percent and hydrogen releases to confined compartments are oxygen starved during the transient release even with the artificially high hydrogen generation rates and 100 percent active cladding reaction assumed in the analyses. Therefore, for accident scenarios in which the igniter system is operational from the onset of core damage, a zero conditional probability of global burn or detonation is assumed.

The hydrogen igniters are actuated by manual action when core-exit temperature exceeds 1200°F as directed by the emergency response guideline (ERG) FR.C-1. The indication and actuation are done with containment conditions within the equipment qualification limits of the systems used, within the design basis of the plant and systems, and before fission-product releases to the containment, so equipment survivability of the monitoring and actuation systems during the time frame that they are required to perform is assured.

The time available for the operator to actuate the hydrogen igniters is assumed to be 15 minutes from the time the core-exit thermocouples exceed 1200°F. Sensitivities concerning the reliability of the operator action and the hydrogen control system reliability are presented in Chapter 50.

### 41.3.6 Other Ignition Sources

A flammable mixture will not burn without an ignition source unless the temperature of the mixture is so high (~1000 K) that auto-ignition becomes possible. Hot surfaces or random sparks from equipment or static electricity may be postulated ignition sources. High-temperature gas jets exiting from the reactor coolant system (RCS) may become an ignition source. However, the gas stream may not have enough momentum to entrain the surrounding flammable mixture, especially in the depressurized cases.

For decomposition event tree quantification, with igniter failure, the likelihood of a random ignition source is assumed to be 0.5 during the in-vessel phase with hydrogen generation to the containment. In the long term, the probability of an ignition source is assumed to be 1.

### 41.3.7 Severe Accident Management Actions

The only severe accident management guidance that is considered in the AP600 PRA is the operator action to flood the reactor cavity in the event of core damage. This action often results in the late reflooding of a damaged core. Some sequences lead to core reflooding through the natural progression of the accident. No recovery of pumped injection reflooding the core is considered in these analyses. (Pumped injection to refill the cavity or reflood the core is possible as an accident management strategy.)

## 41.4 MAAP4 Hydrogen Cases

The MAAP4 code (Reference 41-8) was used to investigate the hydrogen generation rate in the core and releases from the reactor coolant system into the containment. The accident progression and containment response such as break location, sequence timing and rate of containment flooding can have a significant effect on hydrogen generation. The MAAP4 code was used to provide insights into the accident progression, degree of hydrogen generation, containment response, and hydrogen concentrations in compartments during the release from the reactor coolant system to the containment.

### 41.4.1 Modeling Assumptions and Limitations

#### 41.4.1.1 In-Vessel Hydrogen Generation

In these analyses, the hydrogen generation is limited to the in-vessel metal-water reaction that occurs during the core heatup and relocation after core uncovery. Ex-vessel debris phenomena that produce hydrogen, such as core-concrete interaction, are conservatively assumed to fail the containment, so their contribution to hydrogen generation is not required. To model the core heatup and in-vessel hydrogen generation, the AP600 core model is nodalized into 17 axial nodes and 7 radial nodes with axial and radial peaking factors as presented in Figures 41-4 and 41-5. Decay heat is calculated using the American Nuclear Society (ANS) 1979 correlation with best-estimate assumptions. Within each node, the mass and energy of the uranium-dioxide, zirconium, zirconium-dioxide, water/steam/hydrogen, and control rod

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

## TABLE OF CONTENTS (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF TABLES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

## LIST OF FIGURES (Cont.)

value as mean-centered, with the design damping values representing the 84 percentile damping value. Therefore, the margin factor, $MF_d$, is defined as:

$$MF_d = Sa_d/Sa_m$$

where,

$Sa_d$ = spectral acceleration value associated with the design damping value
$Sa_m$ = spectral acceleration value associated with median-centered damping
Variability, $(\beta_c)_d$, for damping is defined by:
$(\beta_c)_d = \ln [Sa_d/Sa_m]$

**Inelastic Energy Absorption, Ductility**

A large amount of energy is absorbed by inelastic structural response. The structure or system is capable of performing its function even though it is responding in an inelastic range. The following statements are made in Reference 55-6, page 34, concerning this phenomenon:

"Numerous observations of the actual performance of structures subjected to seismic motions have demonstrated the capacity of structures to absorb and dissipate much energy when strained in inelastic response. The energy absorption obtained from a linear elastic analysis performed to the design or yield level is only a fraction of the total energy absorption capability of a structure. Unless corrected for inelastic-response capability, a linear elastic-response analysis can not account for the inelastic energy absorption capacity of a structure."

For those structures whose HCLPF values were determined by probabilistic fragility methods, only the inner containment structures and IRWST modules considered ductility. These structures are of shear-wall-type construction. The associated ductility margin factor and variability used are given in Reference 55-7: median margin factor equal to 2.25; composite standard deviation equal to 0.25. Local inelastic energy absorption was not considered.

**Analysis and Modeling Error**

Reference 55-7, pages 143 to 145, discusses modeling errors and how they relate to analysis results. It is stated, "assuming that the analyst does his best job of modeling, modeling accuracy could be median-centered, with variability in each of the modeling parameters amounting to variability in calculated mode shapes and frequencies." The recommendations given in this reference are used to reflect modeling errors.

**Mode Shapes**

To reflect modeling errors in the dynamic model where mode shapes are used in the analytical method to calculate seismic loads, the following standard deviations are used:

| | |
|---|---|
| Multi-degree of freedom system model: | $(\beta_c)_m = 0.15$ |
| System that responds predominantly in one mode: | $(\beta_c)_m = 0.10$ |

**Modal Frequency Variability**

Shifts in the frequency affect spectral acceleration levels and introduce error. This is reflected in the seismic margin analysis by using a log-normal standard deviation calculated as the ratio of the spectral acceleration value associated with a one-sigma variation in frequency, and the spectral acceleration value at the median-centered frequency.

$$(\beta_c)_f = \ln\{S_\beta/S_f\}$$

where,

$S_\beta$ = spectral acceleration value at the 84 percent exceedance probability frequency estimate, $f_\beta$

$S_f$ = spectral acceleration value at median-centered frequency

$f$ = median-centered frequency

$f_\beta$ = 84-percent exceedance probability frequency estimate = $f \times e^{[(+/-0.3]}$

**Imperfection**

Imperfections in the containment vessel affect buckling capacity. This is discussed in Reference 55-8. The critical buckling load is a function of the square of the wavelength. The standard deviation associated with the wavelength is equal to 0.32 per Reference 55-8. Therefore, the standard deviation for imperfection as it relates to critical buckling load is equal to 0.64.

**Soil Structure Interaction**

In the design of the AP600 plant, envelope spectra are used of the different soil conditions. No credit is taken in the development of the HCLPF values that recognizes that the specific site seismic requirements can be much smaller. Variability, $(\beta_c)_{ssi}$, is estimated to be 0.1.

**Conservative Deterministic Failure Margin Method**

The HCLPF value for the Shield Building roof was calculated using the conservative deterministic failure margin approach. A finite-element analysis performed on this structure considered cracking of the concrete and redistribution of the loads. Deterministic margin

Table 55-1 (Sheet 2 of 5)

SEISMIC MARGIN HCLPF VALUES

| Description | Median pga [8] | $\beta_c$ | HCLPF Value [8] | Basis |
|---|---|---|---|---|
| Tank PXS-MT 1A/B (Accumulator) | 2.2g | 0.46 | 0.76g | [1] |
| Tank PXS 2A/B (CMT) | - | - | 0.63g | [4] |
| **Valves** | | | | |
| Room Number 11202 | - | - | 0.96g | [4] |
| Room Number 11206 | - | - | 0.96g | [4] |
| Room Number 11207 | - | - | 0.96g | [4] |
| Room Number 11208 | - | - | 0.96g | [4] |
| Room Number 11300 | - | - | 0.96g | [4] |
| Room Number 11301 | - | - | 0.83g | [4] |
| Room Number 11302 | - | - | 0.96g | [4] |
| Room Number 11304 | - | - | 0.83g | [4] |
| Room Number 11400 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 11403 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 11500 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 11601 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 11603 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 11703 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12244 | - | - | 0.92g | [4] |
| Room Number 12254 | - | - | 0.92g | [4] |
| Room Number 12255 | - | - | 0.92g | [4] |
| Room Number 12256 | - | - | 0.92g | [4] |
| Room Number 12306 | - | - | 0.86g | [4] |
| Room Number 12362 | 3.3g | 0.61 | 0.81g | [1] |

Table 55-1 (Sheet 3 of 5)

SEISMIC MARGIN HCLPF VALUES

| Description | Median pga [8] | $\beta_c$ | HCLPF Value [8] | Basis |
|---|---|---|---|---|
| Room Number 12401 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12404 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12405 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12406 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12452 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12454 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12555 | 3.3g | 0.61 | 0.81g | [1] |
| Room Number 12701 | 3.3g | 0.61 | 0.81g | [1] |
| **Electrical Equipment** | - | - | | |
| Battery | - | - | 1.04g | [6] |
| Battery Racks | 3.3g | 0.46 | 1.14g | [1] |
| Battery Chargers | - | - | 0.98g | [6] |
| 125 VDC Distribution Panel | - | - | 0.51g | [6] |
| 120 VAC Distribution Panel | - | - | 0.51g | [6] |
| Transfer Switches | - | - | 0.51g | [6] |
| 125 VDC MCC | - | - | 0.93g | [6] |
| 125 VDC Switchboard | - | - | 0.51g | [6] |
| Regulating Transformer | - | - | 1.03g | [6] |
| Inverter | - | - | 0.65g | [6] |
| 4.16 kV Switchgear | - | - | 0.86g | [6] |
| Reactor Trip Switchgear | - | - | 0.81g | [6] |

Table 55-1 (Sheet 4 of 5)

SEISMIC MARGIN HCLPF VALUES

| Description | Median pga [8] | $\beta_c$ | HCLPF Value [8] | Basis |
|---|---|---|---|---|
| Hydrogen Monitor | - | - | 1.19g | [6] |
| CMT Level Switch | - | - | 1.09g | [6] |
| Neutron Detector | - | - | 0.51g | [6] |
| Radiation Monitor | - | - | 0.64g | [6] |
| RTD | - | - | 3.75g | [6] |
| Speed Sensors | - | - | 2. 17g | [6] |
| Incore Thermocouple | - | - | 3 .94g | [6] |
| RCP Bearing Water Temp Thermocouple | - | - | 3 .94g | [6] |
| PCS Water Flow Transmitter (el. 135.3') | - | - | 0.93g | [6] |
| PCS Water Flow Transmitter (el. 261') | - | - | 0.61g | [6] |
| PRHR HX Flow Transmitter | - | - | 1.55g | [6] |
| RCS Flow Transmitter | - | - | 1.55g | [6] |
| SG Feed Transmitter | - | - | 1.16g | [6] |
| IRWST Level Transmitter | - | - | 1.27g | [6] |
| PZR Level Transmitter | - | - | 1.27g | [6] |
| SG Narrow-Range Transmitter | - | - | 0.85g | [6] |
| SG Wide-Range Transmitter | - | - | 0.85g | [6] |
| Air Storage Tank Pressurizer Transmitter | - | - | 0.99g | [6] |
| Containment Pressurizer Sensor & Transmitter | - | - | 1. 27g | [6] |
| RCS Wide-Range Pressure Transmitter | - | - | 1. 27g | [6] |
| PRZ Pressure Sensor | - | - | 1. 27g | [6] |

Table 55-1 (Sheet 5 of 5)

**SEISMIC MARGIN HCLPF VALUES**

| Description | Median pga [8] | $\beta_c$ | HCLPF Value [8] | Basis |
|---|---|---|---|---|
| Main Steam Line Pressure Transmitter | - | - | 0.99g | [6] |
| ESFAC Cabinet | - | - | 0.74g | [6] |
| Protection Logic Cabinet | - | - | 0.74g | [6] |
| Integrated Protection Cabinet SWGR | - | - | 0.74g | [6] |
| Multiplex Cabinet | - | - | 0.74g | [6] |
| Qualified Data Processing System (QDPS) Cabinet | - | - | 1.94g | [6] |
| MCR SUPR OPER Station | 2.8g | 0.46 | 0.97g | [1] |
| MCR Switch Station | 2.8g | 0.46 | 0.97g | [1] |
| QDPS and MCR Display | - | - | 1.98g | [6] |
| MCR Isolation Dampers | - | - | 0.80g | [6] |
| Power and Control Panels | - | - | 1. 14g | [6] |
| Ceramic Insulators | 0.2g | 0.35 | 0.09g | [2] |

**Table Notes:**

[1] HCLPF based on Utility Requirements Document recommended generic fragility data
[2] HCLPF based on recognized generic fragility data
[3] HCLPF based probabilistic fragility analysis
[4] HCLPF based on deterministic approach
[5] HCLPF based on conservative deterministic fragility margin approach
[6] HCLPF based on design margin as defined from test data
[7] Component support will control HCLPF value
[8] pga is the free-field peak ground acceleration level for the seismic event

Table 59-29 (Sheet 1 of 18)

**AP600 PRA-BASED INSIGHTS**

| | INSIGHT | DISPOSITION |
|---|---|---|
| 1. | The passive core cooling system (PXS) is composed of the following:<br>- Accumulator subsystem<br>- Core makeup tank (CMT) subsystem<br>- In-containment refueling water storage tank (IRWST) subsystem<br>- Passive residual heat removal (PRHR) subsystem.<br><br>The automatic depressurization system (ADS), which is part of the reactor coolant system (RCS), also supports passive core cooling functions. | |
| 1a. | The accumulators provide a safety-related means of safety injection of borated water to the RCS.<br><br>The following are some important aspects of the accumulator subsystem as represented in the PRA: | SSAR 6.3.2 |
| | - There are two accumulators, each with an injection line to the reactor vessel/direct vessel injection (DVI) nozzle. Each injection line has two check valves in series. | Certified Design Material |
| | - The reliability of the accumulator subsystem is important. The COL will maintain the reliability of the accumulator subsystem. | SSAR 16.2 |
| | - Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failures. | SSAR 6.3.2 |

Table 59-29 (Sheet 2 of 18)

**AP600 PRA-BASED INSIGHTS**

| | INSIGHT | DISPOSITION |
|---|---|---|
| 1b. | ADS provides a safety-related means of depressurizing the RCS. | Certified Design Material |
| | The following are some important aspects of ADS as represented in the PRA: | |
| | ADS has four stages. Each stage is arranged into two separate groups of valves and lines.<br>- Stages 1, 2, and 3 discharge from the top of the pressurizer to the IRWST<br>- Stage 4 discharges from the hot leg to the RCS loop compartment. | Certified Design Material |
| | Each stage 1, 2, and 3 line contains two motor-operated valves (MOVs). | Certified Design Material |
| | Each stage 4 line contains an MOV valve and a squib valve. | Certified Design Material |
| | The valve arrangement and positioning for each stage is designed to reduce spurious actuation of ADS.<br>- Stage 1, 2, and 3 MOVs are normally closed and have separate controls.<br>- Each stage 4 squib valve has redundant, series controllers.<br>- Stage 4 is blocked from opening at high RCS pressures. | SSAR 6.3.2 |
| | The ADS valves are automatically and manually actuated via the protection and safety monitoring system (PMS), and manually actuated via the diverse actuation system (DAS). | Certified Design Material |
| | The ADS valves are powered from Class 1E dc power. | Certified Design Material |
| | The ADS valve positions are indicated and alarmed in the control room. | SSAR 6.3.7 |
| | Stage 1, 2, and 3 valves are stroke-tested every 6 months. Stage 4 squib valve actuators are tested every 2 years for 20% of the valves. | SSAR 3.9.6 |
| | The reliability of the ADS is important. The COL will maintain the reliability of the ADS. | SSAR 16.2 |
| | ADS is required by the Technical Specifications to be available from power conditions down through refueling without the cavity flooded. | SSAR 16.1 |
| | Depressurization of the RCS through ADS minimizes the potential for high-pressure melt ejection events.<br>- Procedures will be provided for use of the ADS for depressurization of the RCS after core uncovery. | Emergency Response Guidelines |

Table 59-29 (Sheet 3 of 18)

**AP600 PRA-BASED INSIGHTS**

| INSIGHT | DISPOSITION |
|---|---|
| 1.b (cont.)<br>The ADS mitigates high pressure core damage events which can produce large uncertainties in containment integrity due to the following severe accident phenomena:<br>- High pressure melt ejection<br>- Direct containment heating<br>- Induced steam generator tube rupture<br>- Induced RCS piping rupture and rapid hydrogen release to containment | PRA Chapter 36 |
| 1c. The CMTs provide safety-related means of high-pressure safety injection of borated water to the RCS. | SSAR 6.3.1 |
| The following are some important aspects of CMT subsystem as represented in the PRA: | |
| There are two CMTs, each with an injection line to the reactor vessel/DVI nozzle.<br>- Each CMT has a normally open pressure balance line from an RCS cold leg.<br>- Each injection line is isolated with a parallel set of air-operated valves (AOVs).<br>- These AOVs open on loss of Class 1E dc power, loss of air, or loss of the signal from the PMS.<br>- The injection line for each CMT also has two normally open check valves in series. | SSAR 6.3.2 |
| The CMT AOVs are automatically and manually actuated from PMS and DAS. | Certified Design Material |
| CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open. | SSAR 6.3.1 & 7.3.1 |
| The CMT AOV positions are indicated and alarmed in the control room. | SSAR 6.3.7 |
| CMT AOVs are stroke-tested quarterly. | SSAR 3.9.6 |
| The CMTs are risk-important for power conditions because the level indicators in the CMTs provide an open signal to ADS and to the IRWST squib valves as the CMTs empty.<br>- The COL will maintain the reliability of the CMT subsystem. | SSAR 16.2 |
| CMT is required by the Technical Specifications to be available from power conditions down through cold shutdown with RCS pressure boundary intact. | SSAR 16.1 |

Table 59-29 (Sheet 4 of 16)

**AP600 PRA-BASED INSIGHTS**

| | INSIGHT | DISPOSITION |
|---|---|---|
| 1d. | IRWST subsystem provides a safety-related means of performing the following functions:<br>- Low-pressure safety injection following ADS actuation<br>- Long-term core cooling via containment recirculation<br>- Reactor vessel cooling through the flooding of the reactor cavity by draining the IRWST into the containment. | SSAR 6.3 |
| | The following are some important aspects of the IRWST subsystem as represented in the PRA: | |
| | IRWST subsystem has the following flowpaths:<br>- Two (redundant) injection lines from IRWST to reactor vessel/DVI nozzle. Each line is isolated with a parallel set of valves; each set with a check valve in series with a squib valve.<br>- Two (redundant) recirculation lines from the containment to the IRWST injection line. Each recirculation line has two paths: one path contains a squib valve and a MOV, the other path contains a squib valve and a check valve.<br>- The two MOV/squib valve lines also provide the capability to flood the reactor cavity. | Certified Design Material |
| | There are screens for each IRWST injection line and recirculation line. | Certified Design Material |
| | Squib valves provide the pressure boundary and prevent the check valves from normally seeing a high delta-P. | SSAR 6.3.3 |
| | Squib valves and MOVs are powered by Class 1E dc power. | Certified Design Material |
| | The squib valves and MOVs for injection and recirculation are automatically and manually actuated via PMS, and manually actuated via DAS. | Certified Design Material |
| | The squib valves and MOVs for reactor cavity flooding are manually actuated via PMS and DAS from the control room. | Certified Design Material |
| | Diversity of the squib valves in the injection lines and recirculation lines minimizes the potential for common cause failure between injection and recirculation/reactor cavity flooding. | SSAR 6.3.2 |
| | Automatic IRWST injection at shutdown conditions is provided using PMS low hot leg level logic. | SSAR 7.3.1 |
| | The positions of the squib valves and MOVs are indicated and alarmed in the control room. | SSAR 6.3.7 |

Table 59-29 (Sheet 17 of 18)

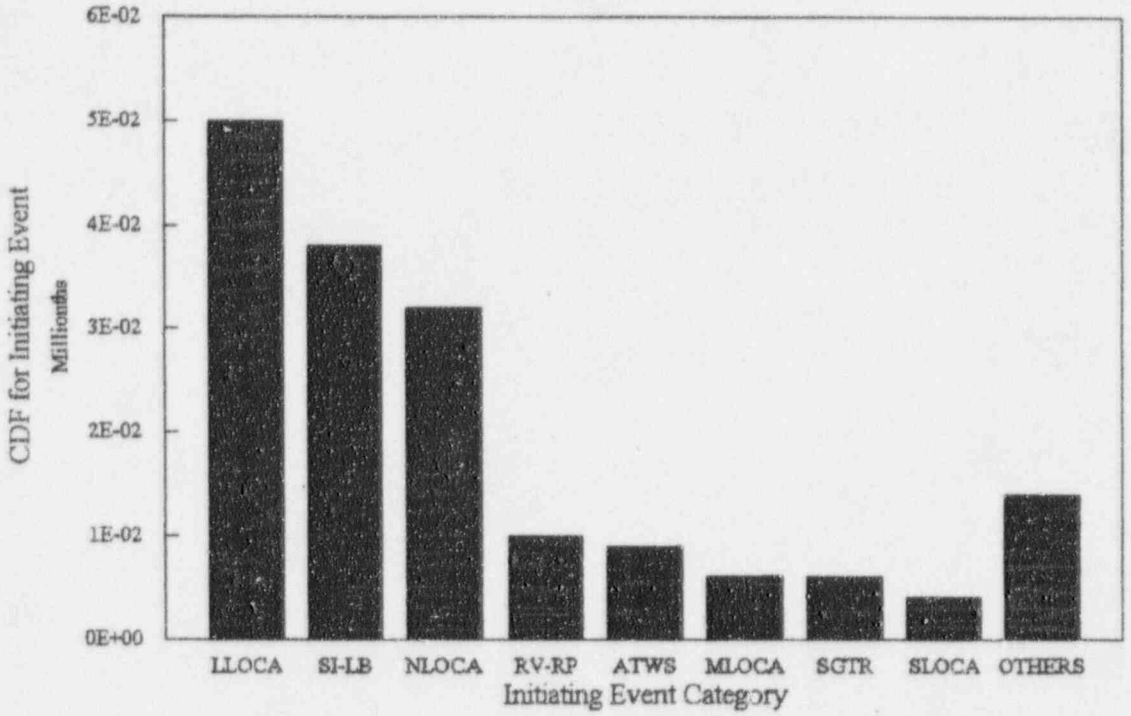
**AP600 PRA-BASED INSIGHTS**

| | INSIGHT | DISPOSITION |
|---|---|---|
| 25. | The depressurization of the reactor coolant system below 150 psi facilitates in-vessel retention of molten core debris. | PRA Chapter 36 |
| 26. | The reflective reactor vessel insulation provides an engineered flow path to allow the ingression of water and venting of steam for externally cooling the vessel in the event of a severe accident involving core relocation to the lower plenum.<br><br>The reflective insulation can withstand pressure differential loading due to the IVR boiling phenomena.<br><br>No coatings are applied to the outside surface of the reactor vessel which will inhibit the wettability of the surface. | PRA Chapter 39 |
| 27. | The reactor cavity design provides a reasonable balance between the regulatory requirements for sufficient ex-vessel debris spreading area and the need to quickly submerge the reactor vessel for the in-vessel retention of core debris. | PRA Chapter 39 and Appendix B |
| 28. | The design can withstand a best-estimate ex-vessel steam explosion without failing the containment integrity. | PRA Appendix B |
| 29. | The containment design incorporates defense-in-depth for mitigating direct containment heating by providing no significant direct flow path for the transport of particulated molten debris from the reactor cavity to the upper containment regions. | PRA Appendix B |
| 30. | The hydrogen control system is comprised of passive autocatalytic recombiners (PARs) and hydrogen igniters to limit the concentration of hydrogen in the containment during accidents and beyond design basis accidents, respectively.<br><br>The operator action to activate the igniters is the first step in ERG FR.C-1 to ensure that the igniter activation occurs prior to rapid cladding oxidation. | Certified Design Material<br><br>Emergency Response Guidelines |
| 31. | The containment layout prevents the formation of diffusion flames that can challenge the integrity of the containment shell.<br><br>Vents from compartments where hydrogen releases can be postulated area away from the containment wall and penetrations or are hatched and locked closed.<br><br>IRWST vents near the containment wall are turned to direct releases away from the containment shell. | SSAR 1.2, General Arrangement Drawings |

Table 59-29 (Sheet 18 of 18)

**AP600 PRA-BASED INSIGHTS**

| | INSIGHT | DISPOSITION |
|---|---|---|
| 32. | The containment structure can withstand the pressurization from a LOCA and the global combustion of hydrogen released in-vessel (10 CFR 50.34(f)). | PRA Chapter 41 |
| 33. | The steam generator should not be depressurized to cool down the RCS if water is not available to the secondary side. This action protects the tubes from large pressure differential and minimizes the potential for creep rupture. | Severe Accident Management Guidance Framework |
| 34. | Depressurizing the RCS and maintaining a water level covering the SG tubes on the secondary side can mitigate fission product releases from a steam generator tube rupture accident. | Severe Accident Management Guidance Framework |




Legend:

| | |
|---|---|
| LLOCA | Large Loss of Coolant Accident |
| SI-LB | Safety Injection Line Break |
| NLOCA | Intermediate Loss of Coolant Accident |
| RV-RP | Reactor Vessel Rupture |
| ATWS | Anticipated Transients Without Scram |
| MLOCA | Medium Loss of Coolant Accident |
| SGTR | Steam Generator Tube Rupture |
| SLOCA | Small LOCA |
| OTHERS | All other initiating events at power |

Scale is core damage events per million reactor years ("millionths"); multiply scale reading by $1 \times 10^{-6}$ to obtain frequency.

Figure 59-1

**Contribution of Initiating Events to Core Damage**

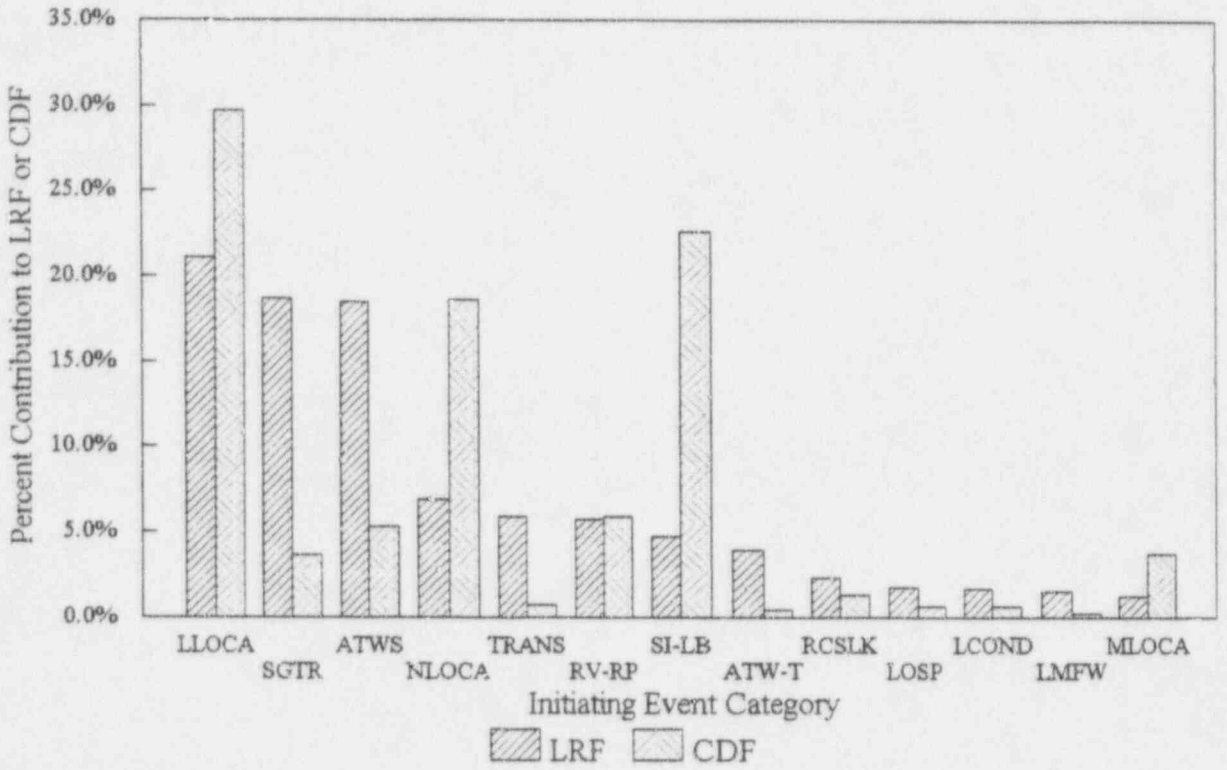
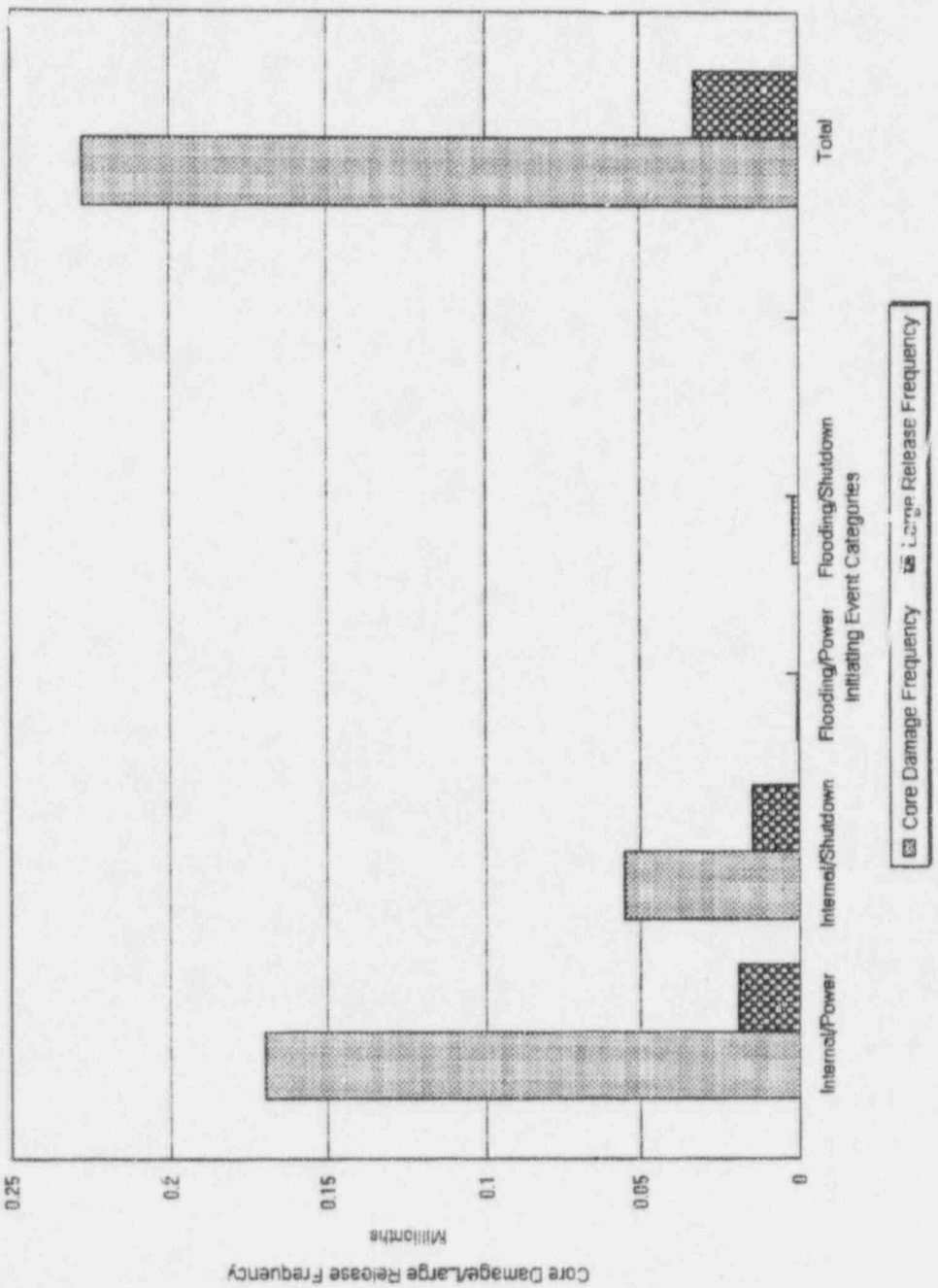



Figure 59-2

**Contribution of Initiating Events to Large Release Frequency and Core Damage Frequency**




Note

1) The bound free assessment performed did not include a release frequency analysis. The results of the fire assessment are not included here.

2) The flood assessment is a bounding analysis - a comparison of the results from it to those from at-power or shutdown is not instructive other than to note that the risk from flooding is very small.

Figure 59-3

**Total Plant CDF/LRF**

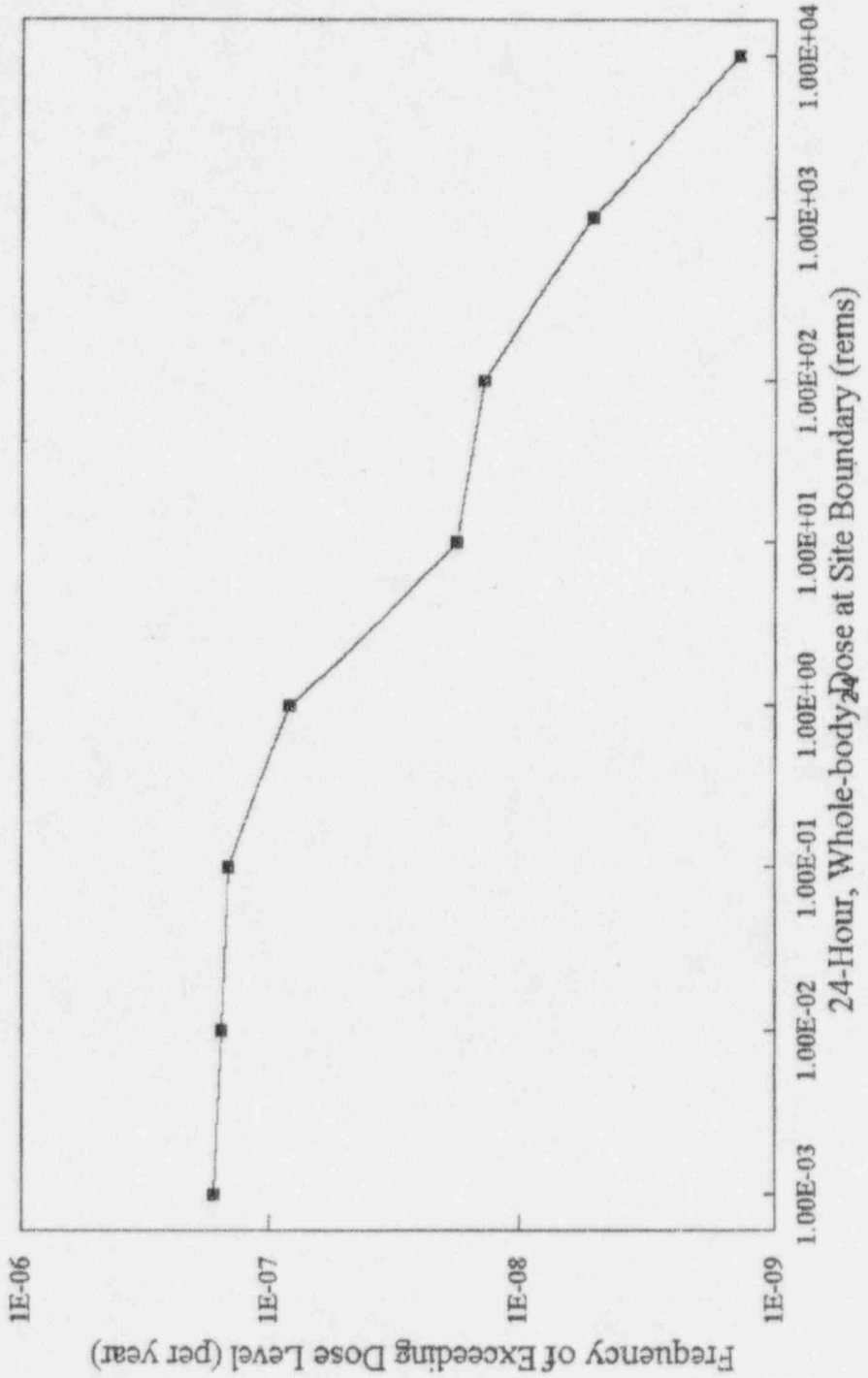



Figure 59-4

**24-Hour Site Boundary Dose Cumulative Frequency Distribution**

# APPENDIX D

# EQUIPMENT SURVIVABILITY ASSESSMENT

## D.1 Introduction

The purpose of the equipment survivability assessment is to evaluate the availability of equipment and instrumentation used during a severe accident to achieve a controlled, stable state after core damage under the unique containment environments. Severe accident phenomena may create harsh, high temperature and pressure containment environments with a significant concentration of combustible gases. Local or global burning of the gases may occur, presenting additional challenges to the equipment. Analyses demonstrate that there is reasonable assurance that equipment used to mitigate and monitor severe accident progression is available at the time it is called upon to perform.

The methodology used to demonstrate equipment survivability is:

- Identify the high level actions used to achieve a controlled, stable state
- Define the accident time frames for each high level action
- Determine the equipment and instruments used to diagnose, perform and verify high level actions in each time frame
- Determine the bounding environment within each time frame
- Demonstrate reasonable assurance that the equipment will survive to perform its function within t.. severe environment.

## D.2 Applicable Regulations and Criteria

Equipment that is classified as safety-related must perform its function within the environmental conditions associated with design-bases accidents. The level of assurance provided by equipment required for design-bases events is "equipment qualification."

The environmental conditions resulting from beyond design basis events may be more limiting than conditions from design-bases events. The NRC has established criteria to provide a reasonable level of assurance that necessary equipment will function in the severe accident environment within the time span it is required. This criterion is referred to as "equipment survivability."

The applicable criteria for equipment, both mechanical and electrical, required for recovery from in-vessel severe accidents are provided in 10 CFR 50.34(f):

- Part 50.34(f)(2)(ix)(c) states that equipment necessary for achieving and maintaining safe shutdown of the plant and maintaining containment integrity will perform its safety function during and after being exposed to the environmental conditions attendant with the release of hydrogen generated by the equivalent of a 100 percent fuel-clad metal-water reaction including the environmental conditions created by activation of the hydrogen control system.

- Part 50.34(f)(2)(xvii) requires instrumentation to measure containment pressure, containment water level, containment hydrogen concentration, containment radiation intensity, and noble gas effluent at all potential accident release points.

- Part 50.34(f)(2)(xix) requires instrumentation adequate for monitoring plant conditions following an accident that includes core damage.

- Part 50.34(f)(3)(v) states that systems necessary to ensure containment integrity shall be demonstrated to perform their function under conditions associated with an accident that releases hydrogen generated from 100 percent fuel-clad metal-water reaction.

The applicable criteria for equipment, both electrical and mechanical, required to mitigate the consequences of ex-vessel severe accidents is discussed in Section III.F, "Equipment Survivability" of SECY-90-016. The NRC recommends in SECY-93-087 that equipment provided only for severe accident protection need not be subject to 10 CFR 50.49 equipment qualification requirements, the 10 CFR 50 Appendix B quality assurance requirements, or 10 CFR 50 Appendix A redundancy/diversity requirements. However, mitigation features must be designed to provide reasonable assurance they will operate in the severe accident environment for which they are intended and over the time span for which they are needed.

## D.3 Definition of Controlled, Stable State

The goal of accident management is to achieve a controlled, stable state following a beyond design basis accident. Establishment of a controlled, stable state protects the integrity of the containment pressure boundary. The conditions for a controlled, stable state are defined by WCAP-13914, the Framework for AP600 Severe Accident Management Guidance (SAMG) (Reference D-1).

For a controlled, stable core state:

- A process must be in place for transferring the energy being generated in the core to a long-term heat sink

- The core temperature must be well below the point where chemical or physical changes might occur

For a controlled, stable containment state:

- A process must be in place for transferring the energy that is released to the containment to a long-term heat sink
- The containment boundary must be protected
- The containment and reactor coolant system conditions must be well below the point where chemical or physical processes (severe accident phenomena) might result in a dynamic change in containment conditions or a failure of the containment boundary.

## D.4 Definition of Equipment Survivability Time Frames

The purpose of the equipment survivability time frames is to identify the time span in the severe accident in which specific equipment is required to perform its function. The phenomena and environment associated with that phase of the severe accident defines the environment which challenges the equipment survivability. The equipment survivability time frame definitions are summarized in Table D.4-1.

### D.4.1 Time Frame 0 - Pre-Core Uncovery

Time Frame 0 is defined as the period of time in the accident sequence after the accident initiation and prior to core uncovery. The fuel rods are cooled by the water/steam mixture in the reactor vessel. The accident has not yet progressed beyond the design basis of the plant and hydrogen generation and the release of fission products from the core is negligible. Emergency response guidelines (ERGs) are designed to maintain or recover the borated water inventory and heat removal in the reactor coolant system to prevent core uncovery and establish a safe, stable state. Recovery within Time Frame 0 prevents the accident from becoming a severe accident. Equipment survivability in Time Frame 0 is covered under the design basis equipment qualification program.

### D.4.2 Time Frame 1 - Core Heatup

Time Frame 1 is defined as the period of time after core uncovery and prior to the onset of significant core damage as evidenced by the rapid oxidation of the core. This is the transition period from design basis to severe accident environment. The overall core geometry is intact and the uncovered portion of the core is overheating due to the lack of decay heat removal. Hydrogen releases are limited to relatively minor cladding oxidation and some noble gas and volatile fission products may be released from the fuel-clad gap. As the core-exit gas temperature increases, the ERGs transition to a red path indicating inadequate core cooling. The operators attempt to reduce the core temperature by depressurizing the RCS and re-establish the borated water inventory in the reactor coolant system. If these actions do not result in a decrease in core-exit temperature, the control room staff initiate actions to mitigate a severe accident by turning on the hydrogen igniters for hydrogen control and flooding the

reactor cavity to prevent reactor pressure vessel failure. Recovery in Time Frame 1 prevents the accident from becoming a core melt. Equipment survivability in Time Frame 1 is evaluated to demonstrate it is within the equipment qualification envelope.

### D.4.3 Time Frame 2 - In-Vessel Severe Accident Phase

Time Frame 2 is the period of time in the severe accident after the accident progresses beyond the design basis of the plant and prior to the establishment of a controlled, stable state (end of in-vessel core relocation), or prior to reactor vessel failure. The onset of rapid oxidation of the fuel rod cladding and hydrogen generation defines the beginning of Time Frame 2. The heat of the exothermic reaction accelerates the degradation, melting and relocation of the core. Fission products are released from the fuel-clad gap as the cladding bursts and from the fuel matrix as the $UO_2$ pellets melt. Over the period of Time Frame 2, the initial, intact geometry of the core is lost as it melts and relocates downward inside the core reflector. The molten corium pool eventually melts through the reflector and relocates to the lower head. Severe accident management strategies exercised during Time Frame 2 are designed to recover reactor coolant system inventory and heat removal, to maintain reactor vessel integrity and to maintain containment integrity. Recovery actions in Time Frame 2 may create environmental challenges by increasing the rate of hydrogen and steam generation.

### D.4.4 Time Frame 3 - Ex-Vessel Severe Accident Phase

Time Frame 3 is defined as the period of time after the reactor vessel fails until the establishment of a controlled, stable state. The AP600 reliably provides the capability to flood the reactor vessel and prevent the vessel failure in a severe accident, and, as quantified in the PRA, this severe accident time phase 3 is of such low frequency, it is considered to be remote and speculative. Molten core debris is relocated from the reactor vessel onto the containment cavity floor which creates the potential for rapid steam generation, core-concrete interaction and non-condensible gas generation. Severe accident management strategies implemented in Time Frame 3 are designed to monitor the accident progression, maintain containment integrity and mitigate fission product releases to the environment.

Table D.4-1

DEFINITION OF EQUIPMENT SURVIVABILITY TIME FRAMES

| Time Frame | Beginning Time | Ending Time | Comments |
|---|---|---|---|
| 0 | Accident initiation | safe, stable state or core uncovery | • Bounded by design basis equipment qualification environment |
| 1 | Core uncovery | controlled, stable state or rapid cladding oxidation | • Core uncovery and heatup<br>• Bounded by design basis equipment qualification environment |
| 2 | Rapid cladding oxidation | controlled, stable state or vessel failure | • In-vessel core melting and relocation<br>• Entry into SAMG |
| 3 | Vessel failure | controlled, stable state or containment failure | • Ex-vessel core relocation |

## D.5 Definition of Active Operation Time

Equipment only needs to survive long enough to perform its function to protect the containment fission product boundary. In the case of some items, such as valves or motor-operators, once the equipment performs its function, it changes state and the function is completed. For other items, such as pumps, the equipment must operate continuously to perform its function. The time of active operation is the time during which the equipment must change state or receive power to perform its function.

## D.6 Equipment and Instrumentation for Severe Accident Management

The AP600 emergency response guidelines (Reference D-2) and severe accident management guidance (SAMG) framework (Reference D-1) define actions that accomplish the goals for achieving a controlled, stable state and terminating fission product releases in a severe accident. The high level actions from the accident management framework are summarized in Table D.6-1 and provide the basis for the actions considered for identifying equipment. The purpose of this section is to review ERG and SAMG actions within each of the time frames of the severe accident to determine the equipment and instrumentation and the active operation time in which they are needed to provide reasonable assurance of achieving a

controlled, stable state. The AP600-specific accident management framework is used to identify the equipment for performing the high level actions.

The Westinghouse Owners Group (WOG) SAMG (Reference D-3) provides the primary input to the selection of the instrumentation used for monitoring the actions. The instrument used to diagnose the need for the action and monitor the response are listed. Instruments to evaluate potential negative impacts are covered under other high level actions in the framework and therefore are also considered for survivability.

The equipment and instrumentation used in each time frame are summarized in Tables D.6-2 through D.6-4.

### D.6.1 Time Frames 0 and 1 - Accident Initiation, Core Uncovery and Heatup

Time Frame 0 represents the accident time prior to core uncovery. Time Frame 1 represents the time following core uncovery, prior to the rapid oxidation of the core. Aside from potential ballooning of the cladding, the core has not lost its initial intact geometry and is coolable.

During Time Frames 0 and 1, most of the equipment that is automatically actuated will receive a signal to start. However, given a severe accident sequence, some critical equipment does not actuate. From accident initiation until the time of core uncovery (Time Frame 0) the conditions are bounded by the design basis and covered under equipment qualification. During Time Frame 1, the environment is still within the design basis of the plant and the control room is operating within the Emergency Response Guidelines (ERGs), but the conditions have the potential to degrade. To achieve a controlled, stable state, accident management, via the ERGs, is geared toward recovering the core cooling before the coolable geometry is lost. Failing that, the plant is configured to keep the core debris in the vessel, and mitigate the containment hydrogen that will be generated in Time Frame 2.

#### D.6.1.1 Injection into the RCS

Failure of RCS injection is likely to be the reason the accident has proceeded to core uncovery. Successful injection into the RCS removes the sensible and decay heat from the core. Prior to the rapid oxidation of the cladding, successful RCS injection essentially recovers the accident before it progresses to substantial core melting and relocation and establishes a controlled, stable state. Failure to inject into the RCS at a sufficient rate allows the accident to proceed into Time Frame 2 and the SAMG.

The equipment and systems used to inject into the RCS are the core makeup tanks, accumulators and IRWST (which are part of the passive core cooling system (PXS)), the chemical and volume control system (CVS) pumps, and the normal residual heat removal (RNS) pumps. For non-LOCA and small LOCA sequences, depressurization of the RCS is required for successful injection.

Injection into the RCS in Time Frame 1 is covered in a number of ERG procedures. The FR.C-1 procedure is entered from the Critical Safety Function Status Tree based on high core-exit temperature, and provides a final attempt to recover the core with water. The plant response is monitored using the system flowrates, RCS pressure, core exit temperature, or RCS piping temperature.

### D.6.1.2 Injection into Containment

In ERG FR.C-1, the operator is instructed to inject water into the containment to submerge the reactor vessel and cool the external surface if injection to the RCS cannot be established. This action is performed at the end of Time Frame 1, immediately prior to entry into the SAMG. Successful cavity flooding prevents vessel failure in the event of molten core relocation to the vessel lower head. Failure of cavity flooding may allow the accident to proceed to vessel failure and molten core relocation into the containment (Time Frame 3) if timely injection into the reactor vessel cannot be established to cool the core and prevent substantial core relocation to the lower head.

The PXS motor-operated and squib recirculation valves are opened manually to drain the IRWST water into the containment.

ERG FR.C-1 is entered from the Critical Safety Function Status Tree based on high core exit temperature. The plant response is monitored by containment water level or IRWST water level indication.

### D.6.1.3 Injection into the Steam Generators

In the event of non-LOCA or small LOCA sequences, the RCS pressure is elevated above the secondary pressure. Failure of feedwater to the steam generators may be the initiating event for such sequences and recovery of injection to the steam generators may be required. If the steam generators remain dry and the core is uncovered, the tube integrity or hot leg nozzle integrity will be threatened by creep rupture failure at the onset on rapid oxidation (entry into Time Frame 2). Injecting to the steam generators provides a heat sink to the RCS by boiling water on the secondary side, and protects the tubes by cooling them. Successful steam generator injection can establish a controlled, stable state if the losses from the RCS can be recovered and mitigated. Failure to inject to the steam generator requires depressurization of the RCS to prevent creep rupture failure of the tubes and loss of the containment integrity at the onset of rapid oxidation in Time Frame 2.

For accident sequences initiated by steam generator tube rupture, the procedures instruct the control room to isolate injection to the faulted steam generator, and to use injection to the intact steam generator in conjunction with steam generator depressurization to cooldown the reactor coolant system and isolate the break. In Time Frame 1, within the FR.C-1, injection to the intact steam generators may be used to re-establish a primary heat sink to cooldown the RCS and a controlled, stable state if the losses from the RCS can be recovered and mitigated.

Failure to inject to the steam generator may lead to a continued loss of coolant to the faulted steam generator and progression to Time Frame 2.

The main feedwater and startup feedwater pumps are used to inject into a pressurized secondary system. If the secondary system can be depressurized sufficiently, condensate, fire water or service water can also be used to inject into the secondary side.

Injection into the steam generators is covered in the ERG in FR-H.1. The guidelines are entered from the Critical Safety Function Status Tree based on low steam generator level, either wide range or narrow range. ERG FR.C-1 is entered based on high core-exit temperature. The plant response is monitored with the steam generator level and steamline pressure.

### D.6.1.4 Depressurize Reactor Coolant System

#### D.6.1.4.1 Non-LOCA and Small LOCA Sequences

In the event of non-LOCA or a small LOCA sequences, the RCS pressure is above the secondary pressure. If the steam generators are dry and the core is uncovered, the hot leg nozzle or tube integrity is threatened by creep rupture failure at the onset of rapid cladding oxidation (beginning of Time Frame 2). Timely depressurization (prior to significant cladding oxidation) of the RCS mitigates the threat to the tubes, allows injection of the accumulators and IRWST water, and provides a long-term heat sink to establish a controlled, stable state. Failure to depressurize can result in the failure of the tubes and a loss of containment integrity when oxidation begins.

For steam generator tube rupture (SGTR) initiated sequences, depressurization of the RCS can be used to isolate the faulted steam generator, and re-establish core cooling via injection.

The automatic depressurization system (ADS) is required to fully depressurize the RCS to allow the PXS systems to inject. However, the recovery of passive residual heat removal (PRHR) or injection to the steam generators will provide a substantial heat sink to depressurize the RCS and mitigate the threat to the tubes. The CVS can be aligned to the auxiliary pressurizer sprays to depressurize the RCS and mitigate the threat to the tubes.

Depressurization of the RCS within Time Frame 1 is outlined in ERG FR.C-1 which is entered based on high core-exit temperature. The RCS pressure, core-exit temperature and RCS temperature can be used to monitor the plant response to the RCS depressurization.

#### D.6.1.4.2 LOCA Sequences

LOCA sequences (other than small LOCA sequences) by definition are depressurized below the secondary system pressure by the initiating event and therefore, are not a threat to steam generator tube integrity upon the onset of rapid oxidation. Depressurization may be required for injection to establish a long-term heat sink. Intermediate LOCAs require additional

depressurization to allow the injection of RNS or PXS. Medium LOCAs require additional depressurization to allow the injection of PXS. Large LOCAs are fully depressurized by the initiating event.

In LOCA sequences, only the ADS is effective in providing depressurization capability to allow injection to the RCS. Steam generator cooldown and auxiliary pressurizer sprays are not effective.

Depressurization of the RCS is outlined in ERG FR.C-1 which is entered based on high core-exit temperature. The RCS pressure, core-exit temperature and RCS temperature can be used to monitor the plant response to the RCS depressurization.

#### D.6.1.4.3 Prevent Reactor Vessel Failure

Depressurization of the RCS, along with injecting into the containment is an accident management strategy to prevent vessel failure. The depressurization of the RCS reduces the stresses on the damaged vessel wall facilitating the in-vessel retention of core debris.

The ADS is used to depressurize the RCS to prevent reactor vessel failure.

Depressurization of the RCS is outlined in ERG FR.C-1. FR.C-1 is entered based on the core-exit temperature. The RCS pressure, core-exit temperature and RCS temperature can be used to monitor the plant response to the RCS depressurization.

### D.6.1.5 Depressurize Steam Generators

The steam generators are depressurized to facilitate low-pressure injection into the secondary system and to depressurize the RCS in non-LOCA and small LOCA sequences. Injection to the steam generator must be available to depressurize the secondary system to prevent creep rupture failure of the tubes.

The steam generator PORV and steam dump valves are used for depressurizing the steam generators.

Depressurization of the steam generators is outlined in ERG FR.H-1 as a means to facilitate low-pressure injection into the steam generators.

The steamline pressure and RCS pressure can be used to monitor the plant response.

### D.6.1.6 Containment Heat Removal

Containment heat removal is not explicitly listed as a high level action in the AP600 SAMG Framework, but it is implicit in the high level action "Depressurize Containment." Containment heat removal is provided by the passive containment cooling system (PCS). The PCS heat removal through a dry containment shell is sufficient to prevent containment failure;

however, water cooling of the shell is needed to establish a controlled, stable state with the containment depressurized. The actuation of PCS water is typically automatic in Time Frame 0.

PCS water is supplied to the external surface of the containment shell from the PCS water storage tank or the post-72 hour water tank. Alternative water sources can be provided via separate connections outside containment.

The containment heat removal can be monitored with the containment pressure and the PCS water flowrate or PCS water storage tank level.

### D.6.1.7 Containment Isolation

Containment isolation is not explicitly listed as a high level action in the AP600 SAMG Framework, but it is implicit as a requirement to protect the fission product barrier.

Containment isolation is provided by an intact containment shell and the containment isolation system (CIS) which closes the isolation valve in lines penetrating the containment shell.

The containment isolation can be monitored by the containment pressure and the CIS valve positions.

### D.6.1.8 Hydrogen Control

Maintaining the containment hydrogen concentration below a globally flammable limit is a requirement for a controlled, stable state. The containment can withstand the pressurization from a global deflagration, but potential flame acceleration can produce impulsive loads for which containment integrity is uncertain. While hydrogen is not generated in a significant quantity until Time Frame 2, provisions are provided in the ERGs within Time Frame 1 to turn on the igniters before hydrogen generation begins so that hydrogen can be burned as it is produced.

Severe accident hydrogen control in the AP600 is provided by hydrogen igniters. The containment has passive auto-catalytic recombiners (PARs) as well, but they are not credited for severe accidents.

The igniters are manually actuated from the control room as the first step in ERG FR.C-1 on high core-exit temperature. The intention of this timing is to actuate the igniters prior to the cladding oxidation (Time Frame 1). The containment hydrogen concentration is monitored prior to actuation so that a globally flammable mixture is not unintentionally ignited.

The plant response to the igniter actuation can be monitored by containment hydrogen concentration using the hydrogen monitors or the post-accident sampling function, which is part of the primary sampling system. The containment pressure response can also be used to observe hydrogen burning.

### D.6.1.9 Accident Monitoring

Accident monitoring is a post-TMI requirement as outlined in 10 CFR 50.34(f). Aside from the accident management purposes outlined above, monitoring the progression of the accident and radioactive releases provides input to emergency response and emergency action levels.

Accident monitoring is provided by the in-containment monitors for pressure, hydrogen concentration, water levels, and radiation, as well as the post-accident sampling system.

## D.6.2 Time Frame 2 - In-Vessel Core Melting and Relocation

Time Frame 2 represents the period of core melting and relocation and the entry into the SAMG. The intact and coolable in-vessel core geometry is lost, and relocation of core debris into the lower head is likely. The in-vessel hydrogen generation and fission product releases from the fuel matrix occur during this time frame.

### D.6.2.1 Injection into the RCS

In Time Frame 2, the in-vessel core configuration loses its coolable geometry and it is likely that at least some of the core debris will migrate to the reactor vessel lower head. If the RCS is depressurized and the reactor vessel is submerged, the core debris will be retained in the reactor vessel. However, injection into the RCS to cover and cool the core debris is required to achieve a controlled, stable state. RCS injection is not required to protect the containment fission product boundary. Injection is successful if it is sufficient to quench the sensible heat from the core debris and maintained to remove decay heat.

RCS injection is outlined from SAMG SAG-3 (Reference D-3) and entered from the Diagnostic Flow Chart. Water can be injected into the RCS using the PXS, the CVS or the RNS systems. Post-core damage, the actions may be monitored with RCS pressure or temperature or containment pressure.

### D.6.2.2 Injection into Containment

The objective of injection to the containment prior to reactor vessel failure (Time Frame 3) is to cool the external surface of the vessel to maintain the core debris in the vessel. Reasonable assurance of injecting to the containment for in-vessel retention is achieved by instructing the operator to drain the IRWST in the ERGs within Time Frame 1. After relocation of core debris to the lower head in Time Frame 2, the success of this action becomes uncertain. If the vessel fails, the accident progresses to Time Frame 3. Active operation for injection to containment is completed prior to Time Frame 2.

### D.6.2.3 Injection into the Steam Generators

In transients and small LOCAs, injection into the steam generators is required to be recovered in Time Frame 1 to be successful. Steam generator tubes or the hot leg nozzles will fail when

the cladding oxidation begins at the onset of Time Frame 2. Steam generator injection is not required for LOCAs which depressurize the RCS below the secondary system pressure.

Within Time Frame 2 SAMG, injection can be utilized in unisolated SGTR sequences to maintain the water level on the secondary side for mitigation of fission product releases. Injecting into the steam generators, along with depressurization of the RCS, is an accident management action to isolate containment or scrub fission products. Failure to inject to the faulted steam generator in Time Frame 2 can lead to continued breech of the containment fission product boundary and large offsite doses.

The main feedwater and startup feedwater pumps are used to inject into a pressurized secondary system. If the secondary system can be depressurized sufficiently, condensate, fire water or service water can also be used to inject into the secondary side.

Injection into the steam generators is covered in the WOG SAMG (Reference D-3) in SAG-1. The guideline is entered from the Diagnostic Flow Chart based on low steam generator level, either wide range or narrow range. The plant response is monitored with the steam generator level and steamline pressure.

#### D.6.2.4 Depressurize RCS

RCS depressurization is required within Time Frame 1 for facilitating in-vessel retention of core debris and for successfully preventing steam generator tube failure in high pressure severe accident sequences. The steam generator tubes or hot leg nozzles will fail due to creep rupture after the onset of rapid oxidation at the beginning of Time Frame 2. This action facilitates in-vessel retention of core debris in conjunction with injection into the containment to give time to recover pumped injection sources to establish a controlled, stable state. Reasonable assurance of successful RCS depressurization is provided by instructing the operator to depressurize the system in the ERGs in Time Frame 1. Active operation of RCS depressurization is completed prior to Time Frame 2.

#### D.6.2.5 Depressurize Steam Generators

Active operation to depressurize the steam generators is used to cooldown the RCS prior to Time Frame 2. After the onset of core melting and relocation, depressurizing steam generators could threaten steam generator tube integrity. Depressurizing the steam generator in Time Frame 2 does not facilitate the establishment of a controlled, stable state.

#### D.6.2.6 Containment Heat Removal

Reasonable assurance of successful containment heat removal is provided since automatic actuation of PCS water occurs in Time Frame 0 and passive air cooling of dry shell prevents containment overpressurization, providing time for operator to recover a water source. Alternate water sources can be provided by connections to the external PCS water tank which is outside the containment pressure boundary and not subjected to the harsh environment.

### D.6.2.7 Containment Isolation

Active operation of containment isolation valves is required in Time Frame 0 or 1 to establish the containment fission product barrier. Therefore, only the survivability of the containment pressure boundary, including penetrations, is required to maintain containment isolation after Time Frame 1.

### D.6.2.8 Hydrogen Control

The operator action to actuate the igniters occurs prior to the hydrogen generation at the onset of Time Frame 2. The igniters need to survive and receive power throughout the hydrogen release to maintain the hydrogen concentration below the lower flammability limit during the hydrogen generation in Time Frame 2.

### D.6.2.9 Accident Monitoring

During the initial core melting and relocation, containment hydrogen and radiation monitors are used for core damage assessment and verification of the hydrogen igniter operation. Steam generator radiation monitoring is used to determine steam generator tube integrity. In the longer term, the post-accident sampling function can be used to monitor hydrogen and radiation. Containment pressure needs to be monitored throughout Time Frame 2.

## D.6.3 Time Frame 3 - Ex-Vessel Core Relocation

Time Frame 3 represents the phase of the accident after vessel failure. The core debris is in the reactor cavity, and the IRWST water is not injected into the containment.

### D.6.3.1 Injection into the RCS

The RCS is failed. Injection to the RCS is no longer needed in Time Frame 3.

### D.6.3.2 Injection into Containment

Reasonable assurance of sufficient water coverage to the ex-vessel debris bed is passively provided by the containment design to drain water from the RCS, CMTs, and accumulators to the lower containment. Water condensing on the PCS shell is returned to the reactor cavity after filling the IRWST and a small volume in the refueling canal to the overflow. Without draining the IRWST water to the cavity, the CMT, accumulator and RCS water provides sufficient water return to the cavity to maintain water coverage over the ex-vessel debris bed.

### D.6.3.3 Injection into the Steam Generators

The RCS is failed. Injection into the steam generators is no longer needed in Time Frame 3. Injection to the steam generator for SGTR fission product scrubbing is not required to maintain the water level as the water cannot drain against the containment backpressure.

### D.6.3.4 Depressurize RCS

The RCS is depressurized by the vessel failure in Time Frame 3.

### D.6.3.5 Depressurize Steam Generators

The RCS is failed. Steam generator depressurization is not needed in Time Frame 3.

### D.6.3.6 Containment Heat Removal

Active operation of PCS water is completed prior to Time Frame 3.

### D.6.3.7 Containment Isolation

Continued operation of the containment shell as a pressure boundary is needed to maintain containment isolation in Time Frame 3.

### D.6.3.8 Combustible Gas Control

The hydrogen igniters are used to control combustible gases. Active operation of igniters continues to control the release of combustible gases from the degradation of concrete in the reactor cavity.

### D.6.3.9 Accident Monitoring

Containment pressure and the post-accident sampling function are sufficient to monitor the accident in the long-term.

## D.6.4 Summary of Equipment and Instrumentation

The equipment and instrumentation used in achieving a controlled, stable state following a severe accident, and the time it operates are summarized in Tables D.6-2 through D.6-4.

Table D.6-1

**AP600 HIGH LEVEL ACTIONS RELATIVE TO ACCIDENT MANAGEMENT GOALS**
(taken from Table 5-1, reference D-1)

| Goal | Element | High Level Action |
|---|---|---|
| Controlled, stable core | water inventory in RCS | • inject into RCS<br>• depressurize RCS |
| | water inventory in containment | • inject into containment |
| | heat transfer to SGs | • inject into RCS<br>• inject into SGs<br>• depressurize SGs |
| | heat transfer to containment | • inject into RCS<br>• inject into containment<br>• depressurize RCS |
| Controlled, stable containment | heat transfer from containment | • depressurize containment<br>• vent containment |
| | isolation of containment | • inject into SGs<br>• depressurize RCS |
| | hydrogen prevention/control | • burn hydrogen<br>• pressurize containment<br>• depressurize RCS<br>• inject into containment<br>• vent containment |
| | CCI prevention | • inject into containment |
| | HPME prevention | • inject into containment<br>• depressurize RCS |
| | creep rupture prevention | • depressurize RCS<br>• inject into SGs |
| | containment vacuum prevention | • pressurize containment |
| Terminate fission product release | isolation of containment | • inject into SGs<br>• depressurize RCS |
| | reduce fission product inventory | • inject into containment<br>• depressurize RCS |
| | reduce fission product driving force | • depressurize containment |

Table D.6-2

**EQUIPMENT AND INSTRUMENTATION OPERATION PRIOR TO END OF TIME FRAME 1 - CORE UNCOVERY AND HEATUP**

| Action | Equipment | Instrumentation | Purpose | Comment |
|---|---|---|---|---|
| Inject into RCS | • PXS<br>• CVS<br>• RNS | • core exit t/c's<br>• RCS pressure<br>• RCS RTDs | • restore core cooling | • injection must often be recovered to be successful in severe accident |
| Inject Into Containment | • PXS recirc<br>• SFS injection to refueling cavity | • core-exit t/c's<br>• containment water level<br>• IRWST water level | • prevent vessel failure | • manual cavity flooding action in ERG FR.C-1 entered when CET/C > 1200°F |
| Inject into SGs | • High Pressure<br>- MFW<br>- SFW<br>• Low Pressure<br>- condensate<br>- fire water<br>- service water | • SG WR water level<br>• steamline pressure | • establish heat sink<br>• make SGs available to depressurize RCS<br>• prevent creep rupture | • injection source must often be recovered to be successful in severe accident |
| Depressurize RCS | • ADS<br>• PRHR HX<br>• via SGs<br>• Aux Pzr Spray (CVS) | • RCS pressure<br>• core-exit t/c's<br>• RCS RTDs | • facilitate injection to RCS<br>• long-term heat transfer path | • ADS often automatic |
| | | | • prevent creep rupture<br>• containment integrity | • RCS depressurization required prior to cladding oxidation to prevent creep rupture |
| | | | • isolate break in SGTR | • uses intact SG or PRHR |
| | | | • prevent vessel failure | • requires injection to containment to be successful |

Table D.6-2 (Cont.)

**EQUIPMENT AND INSTRUMENTATION OPERATION PRIOR TO END OF TIME FRAME 1 - CORE UNCOVERY AND HEATUP**

| Action | Equipment | Instrumentation | Purpose | Comment |
|---|---|---|---|---|
| Depressurize SGs | • SG PORV<br>• Steam dump | • steamline pressure<br>• RCS pressure | • facilitate injection to SGs<br>• depressurize RCS | • requires injection into SGs to prevent creep rupture |
| Containment Heat Removal | • PCS water<br>• external fire water | • containment pressure<br>• PCS flowrate<br>• PCS tank level | • containment integrity<br>• alleviate environmental challenge to equipment<br>• long-term heat transfer path | • PCS water often automatic |
| Containment Isolation | • CIS<br>• containment shell | • CIS valve position<br>• containment pressure | • containment integrity | • CIS often automatic<br>• manual action in ERG E-0 |
| Control Hydrogen | • igniters | • containment hydrogen monitors<br>• containment pressure | • containment integrity | • manual igniter action in ERG FR.C-1 entered when CET/C > 1200°F |
| Accident Monitoring | | • SG radiation<br>• containment pressure<br>• containment hydrogen<br>• containment water level<br>• containment radiation | • accident management<br>• emergency response<br>• emergency action levels | • required by 10 CFR 50.34(f) |

Table D.6-3

**EQUIPMENT AND INSTRUMENTATION OPERATION DURING TIME FRAME 2 - IN-VESSEL CORE MELTING AND RELOCATION**

| Action | Equipment | Instrumentation | Purpose | Comment |
|---|---|---|---|---|
| Inject into RCS | • PXS<br>• CVS<br>• RNS | • RCS pressure<br>• containment pressure | • cool core debris | • RCS injection needed to cool in-vessel debris for reasonable assurance of controlled, stable state |
| Inject Into Containment | | | | • active operation completed in Time Frame 1 |
| Inject into SGs | • High Pressure<br>- MFW<br>- SFW<br>• Low Pressure<br>- Condensate<br>- Fire Water<br>- Service Water | • SG WR water level | • isolate containment in SGTR<br>• scrub fission products | • also requires RCS depressurization for success |
| Depressurize RCS | | | | • active operation completed in Time Frame 1 |
| Depressurize SGs | | | | • active operation completed in Time Frame 1 |
| Containment Heat Removal | | | | • active operation completed in Time Frame 1 |
| Containment Isolation | • containment shell | • containment pressure | • containment integrity | • CIS active operation completed in Time Frame 1 |
| Control Hydrogen | • igniters | • containment hydrogen monitors<br>• post-accident sampling function | • containment integrity | • active operation continues in Time Frame 2<br>• monitors only required initially to verify hydrogen igniter operation |
| Accident Monitoring | | • containment pressure<br>• post-accident sampling function | • accident management<br>• emergency response<br>• emergency action levels | • active operation continues in Time Frame 2 |

Table D.6-4

**EQUIPMENT AND INSTRUMENTATION OPERATION DURING TIME FRAME 3 - EX-VESSEL CORE RELOCATION**

| Action | Equipment | Instrumentation | Purpose | Comment |
|---|---|---|---|---|
| Inject into RCS | | | | • not needed in Time Frame 3 |
| Inject Into Containment | | | | • injection of CMTs and accumulators in Time Frame 1 provides reasonable assurance of water coverage to ex-vessel core debris |
| Inject into SGs | | | | • not needed in Time Frame 3 |
| Depressurize RCS | | | | • not needed in Time Frame 3 |
| Depressurize SGs | | | | • not needed in Time Frame 3 |
| Containment Heat Removal | | | | • active operation completed in Time Frame 1 |
| Containment Isolation | • containment shell | • containment pressure | • containment integrity | • active operation of CIS completed in Time Frame 1 |
| Control Hydrogen | • igniters | • post-accident sampling function | • containment integrity | • active operation continues in Time Frame 3 |
| Accident Monitoring | | • containment pressure<br>• post-accident sampling function | • accident management<br>• emergency response<br>• emergency action levels | • active operation continues in Time Frame 3 |

## D.7 Radiation Environment - Severe Accident

The radiation exposure inside the containment for a severe accident is conservatively estimated by considering the dose in the middle of the AP600 containment with no credit for the shielding provided by internal structures.

Sources are based on the emergency safeguards system core thermal power rating and the following analytical assumptions:

- Power Level ..... 1,972 MWt

- Fraction of total core inventory released to the containment atmosphere:

| | |
|---|---|
| Noble Gases (Xe, Kr) | 1.0 |
| Halogens (I, Br) | 0.75 |
| Alkali Metals (Cs, Rb) | 0.75 |
| Tellurium Group (Te, Sb, Se) | 0.305 |
| Barium, Strontium (Ba, Sr) | 0.104 |
| Noble Metals (Ru, Rh, Pd, Mo, Tc, Co) | 0.005 |
| Lanthanides (La, Zr, Nd, Eu, Nb, Pr, Sm, Y, Cm, Am) | 0.0051 |
| Cerium Group (Ce, Pu, Np) | 0.0051 |

The radionuclide groups and elemental release fractions listed above are consistent with the accident source term information presented in NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants - Final Report," with the exception of the early in-vessel release fractions for barium and strontium, lanthanides, and cerium groups. For barium and strontium, the value of 0.004 is used in place of the NUREG-1465 value of 0.02. For the lanthanide and cerium groups, the release fraction of 0.0001 is considered in place of the NUREG-1465 values of 0.0002 for lanthanides and 0.0005 for the cerium group. These exceptions are based on the recommendations of the Department of Energy's Advanced Reactor Severe Accident Program (ARSAP) in support of the ALWR program (Ref. D-4).

The timing of the releases are based on NUREG-1465 assumptions as well as AP600-specific activity release projections. The release scenario assumed in the calculations is described below.

An initial release of activity from the gaps of a small number of failed fuel rods at 30 seconds into the accident is considered. The instantaneous release of 0.15 percent of the core inventory of the volatile species (defined as noble gases, halogens, and alkali metals) is assumed. At 50 minutes after the accident, an additional 2.85 percent of the core activity inventory is assumed to be instantaneously released from the gaps of failed fuel rods and is added to the previously released inventory associated with 0.15 percent of the gap activity. Thus, the total release of volatile species at 50 minutes after the accident is 3 percent of the total core inventory.

At 30 minutes following the instantaneous gap activity releases, that is, 80 minutes into the accident, an additional 2 percent of the core inventory is added to the inventory that exists based on the previous gap activity releases. At this point, 5 percent of the total core inventory of volatile species has been assumed to be released.

Over the next 1.3 hours, releases associated with an early in-vessel release period are assumed to occur, that is, from 1.33 hours (or 80 minutes) to 2.63 hours into the accident. This source term is a time-varying release in which the release rate is assumed to be constant during the duration time, consistent with the assumptions in NUREG-1465. Additional releases during the early in-vessel release period include 95 percent of the noble gases, 35 percent of the halogens, and 25 percent of the alkali metals, as well as the fractions of the tellurium group, barium and strontium, noble metals, lanthanides, and cerium group as listed above.

The duration of the ex-vessel release is two hours and the late in-vessel release is ten hours. These releases occur simultaneously after the early in-vessel release. The additional releases include 35 percent of the halogens, 45 percent of the alkali metals, over 25 percent of the tellurium group, ten percent barium and strontium and fractions of the noble metals, lanthanides and cesium group, consistent with the assumptions of NUREG-1465.

The resulting instantaneous gamma and beta dose rates are provided in Figures D.7.0-1 and D.7.0-2, respectively.

### D.7.1 Bounding Severe Accident Environments

The bounding severe accident environments for each of the equipment survivability time frames defined in Section D.4 are provided in this section. These bounding environments for the reactor coolant system and containment are used in the assessments described in Section D.8.

The MAAP4 computer code (version 4.0.2) was used to support the quantification of the equipment survivability time frames and the bounding environment within each time frame. Two basic sequences and five sensitivity cases were quantified to establish the bounding environments including hydrogen combustion in the containment. Each sequence input data were adjusted to assure that a 100% fuel-clad metal-water reaction occurred so that the required bounding hydrogen source was considered.

The two base sequences were a large (2.2 $ft^2$) hot leg break into a steam generator compartment and a 4-inch direct vessel injection (DVI) line break in a valve vault room. For each of these LOCA sequences, four sensitivity cases were run to determine the effects of cavity flooding, core-concrete interaction, igniters (local burn versus global burn) and jet burning of the heated hydrogen-rich RCS gas discharge. A total of ten sequences were quantified. The designator and description for each of the ten sequences are summarized in Table D.7-1.

The key event timing for each of the sequences is summarized in Table D.7-2. These key events in the severe accident progression directly relate to the equipment survivability time frames. Time Frame 1 is the interval between core uncovery and a core exit gas temperature exceeding 2000°F (1367 K). Time Frame 2 is the interval between the core exit gas temperature exceeding 1367 K and either the end of core material relocation into the lower head or vessel failure. Time frame 3 is the interval between vessel failure and the end of the sequence.

The MAAP4 results provide the bounding containment environment associated with the combustion of hydrogen resulting from the equivalent of 100% oxidation of the active fuel cladding where: 1) igniters are functioning (local burning scenario), 2) igniters were artificially defeated (global burning scenario), and 3) jet burning and igniters were defeated (global burning scenario). To calculate more severe bounding containment environments, the cavity flooding was defeated in some sequences resulting in ex-vessel hydrogen generation due to core-concrete interaction.

The results of 4-inch DVI line break sequences are very similar to the hot leg large LOCA results because the ADS 4th stage valves are opened in both sequences. The RCS response for these low pressure sequences is very similar. The peak temperature calculated in the upper plenum gas was about 2780°F (1800 K). Since these sequences are low pressure sequences with the ADS 4th stage valves open, the gas temperature in the pressurizer stayed below the nominal temperature (665°F, 625 K) for most of the transient in all of these sequences. The gas temperatures in both steam generators stayed below 566°F (570 K) for all of these sequences because water was present in both steam generator secondary sides.

Figures D.7.1-1 through D.7.1-6 show gas temperatures in the containment compartments, the containment pressure and the RPV temperature. Since this sequence has cavity flooding, resulting in no vessel failure and no core-concrete interaction, all hydrogen burns occurred before 11,000 seconds. However, the hydrogen burned was not due to igniter induced burns. Some of the hydrogen coming out from the primary system through the ADS 4th stage valves were burned as they came out because the primary system gas temperature was higher than the jet burn temperature (1448°F, 1060 K). To see the effect of the jet burn, the jet burn model was turned off in the A3BE-GJ and APLHL-GJ sequences. For cases without the jet burn, it was observed that a large amount of hydrogen was burned in the upper compartment and much less hydrogen was burned in the steam generator compartments. The containment gas temperatures after 11,000 seconds reached stable conditions because of the availability of PCS.

In general, results with and without igniters were very similar because of the jet burn of the gas flow coming out from the primary system. For cases without cavity flooding, more hydrogen was generated due to the core-concrete interaction such that late hydrogen burns were observed.

For the hot leg LOCA sequences with the cavity flooding available, the water level in the containment eventually reached the hot leg break elevation and the whole core became submerged by water in the later transient. The reverse water flow through the break did not occur in the DVI line break sequences because of the high floor elevation of the valve vault.

The families of curves for the other base case (large LOCA) and all the sensitivity cases are provided in Figures D.7.1-7 through D.7.1-60.

Table D.7-1

**SEQUENCE DESIGNATOR**

Hot leg LOCA with a break area of 2.2 $ft^2$ with no reflood: 2 ADS Stage 1-3 and 4 ADS Stage 4, 1 accumulator, 1 CMT, and PCS available.

- APLHL — Large hot leg with cavity flooding, similar to the A3BE, except the break location and the area. The break location is in S/G compartment 1, rather than valve vault.
- APLHL-N — APLHL + no cavity flooding + no ex-vessel cooling
- APLHL-G — APLHL + no igniters
- APLHL-GN — APLHL + no igniters + no cavity flooding + no ex-vessel cooling
- APLHL-GJ — APLHL + no igniters + no jet burn

4-inch DVI line break with no reflood and no PRHR: 2 ADS Stage 1-3 and 4 ADS Stage 4, 1 accumulator, 1 CMT, and PCS available.

- A3BE — AP600 3BE sequence with cavity flooding, ex-vessel cooling, igniters, and jet burning
- A3BE-N — A3BE + no cavity flooding + no ex-vessel cooling
- A3BE-G — A3BE + no igniters
- A3BE-GN — A3BE + no igniters + no cavity flooding + no ex-vessel cooling
- A3BE-GJ — A3BE + no igniters + no jet burn

Table D.7-2

**SUMMARY OF MAAP4 ANALYSES: EQUIPMENT SURVIVABILITY TIME FRAMES**

| Key Quantity or Timing | SEQUENCES | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 4-inch DVI Line Break | | | | | Hot Leg Large LOCA | | | | |
| | A3BE | A3BE-N | A3BE-G | A3BE-GN | A3BE-GJ | APLHL | APLHL-N | APLHL-G | APLHL-GN | APLHL-GJ |
| Clad Oxidation (%) | 100.41 | 98.36 | 100.4 | 100.43 | 100.47 | 100.42 | 100.4 | 100.43 | 100.49 | 100.44 |
| Time of Core Uncovery (s) | 2767 | 2766 | 2767 | 2766 | 2767 | 2086 | 2082 | 2086 | 2082 | 2086 |
| Time of Core Exit Gas Temp. > 1367 K | 4262 | 4256 | 4262 | 4256 | 4262 | 3456 | 3453 | 3456 | 3453 | 3456 |
| Time of Initial Core Material Relocation Into Lower Head | 5662 | 5692 | 5700 | 5651 | 5700 | 4949 | 4924 | 4949 | 4925 | 4949 |
| Time of Vessel Failure | N/A | 20589 | N/A | 17652 | N/A | N/A | 18120 | N/A | 19119 | N/A |
| Time core Material Relocation Into Lower Head Ends | 16800 | 20100 | 20700 | 16300 | 18500 | 14000 | 38500 | 14000 | 15000 | 14000 |

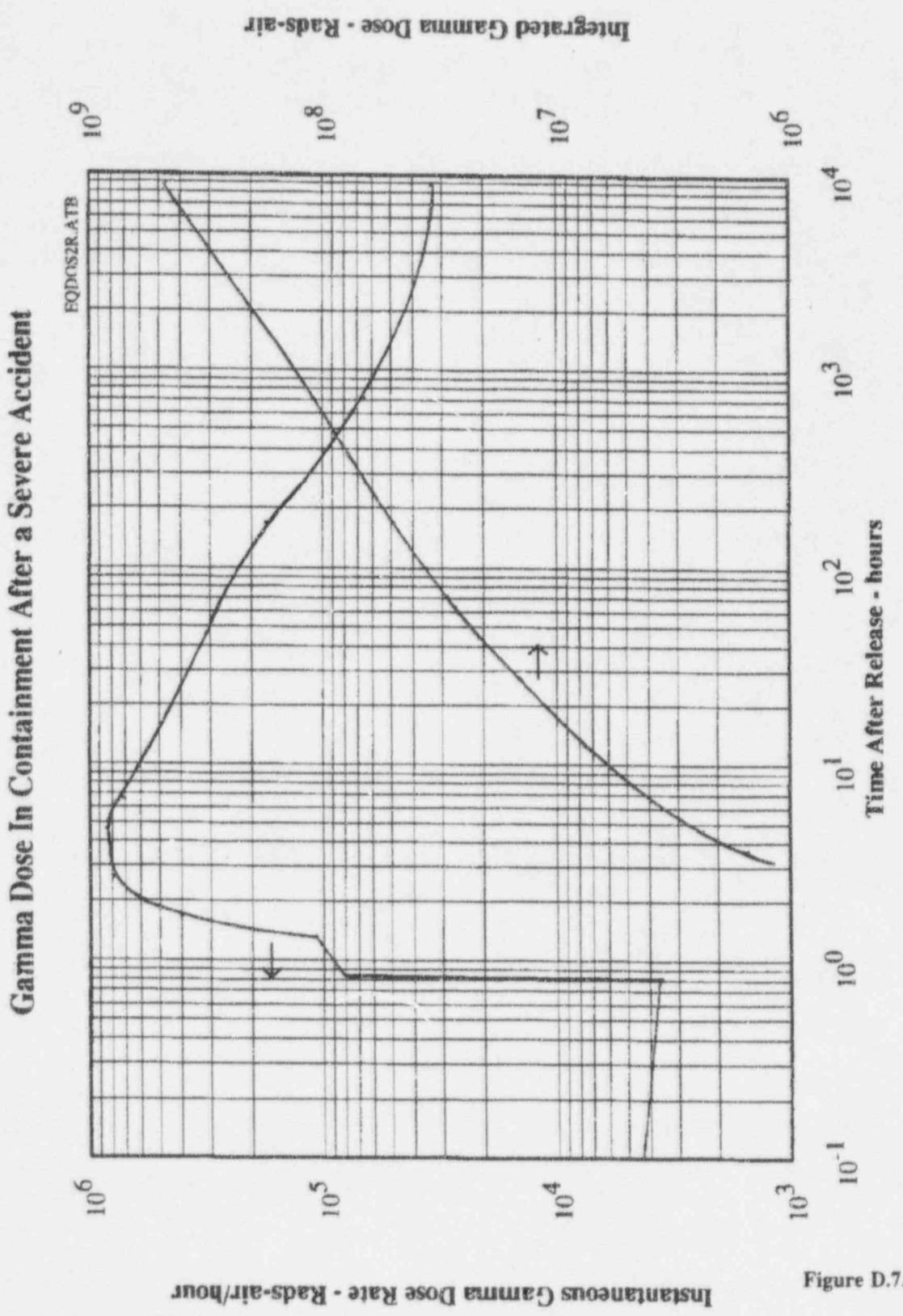

Gamma Dose In Containment After a Severe Accident
EQDOS2R.ATB
Integrated Gamma Dose - Rads-air
Instantaneous Gamma Dose Rate - Rads-air/hour
Time After Release - hours
$10^9$
$10^8$
$10^7$
$10^6$
$10^6$
$10^5$
$10^4$
$10^3$
$10^4$
$10^3$
$10^2$
$10^1$
$10^0$
$10^{-1}$

Figure D.7.0-1

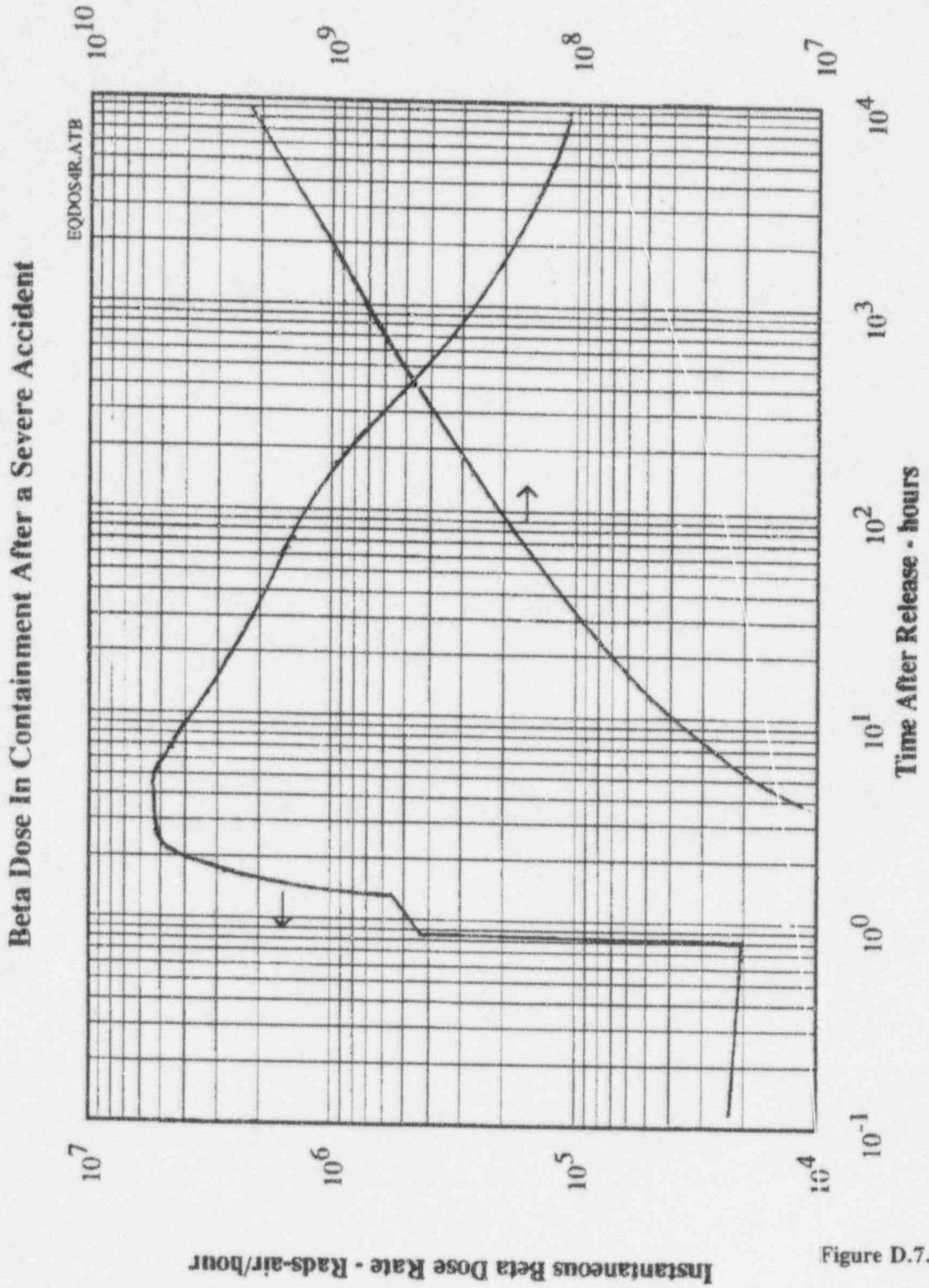

Beta Dose In Containment After a Severe Accident
EQDOS4R.ATB
Integrated Beta Dose - Rads-air
Instantaneous Beta Dose Rate - Rads-air/hour
Time After Release - hours
$10^{10}$
$10^{9}$
$10^{8}$
$10^{7}$
$10^{4}$
$10^{3}$
$10^{2}$
$10^{1}$
$10^{0}$
$10^{-1}$
$10^{7}$
$10^{6}$
$10^{5}$
$10^{4}$

Figure D.7.0-2

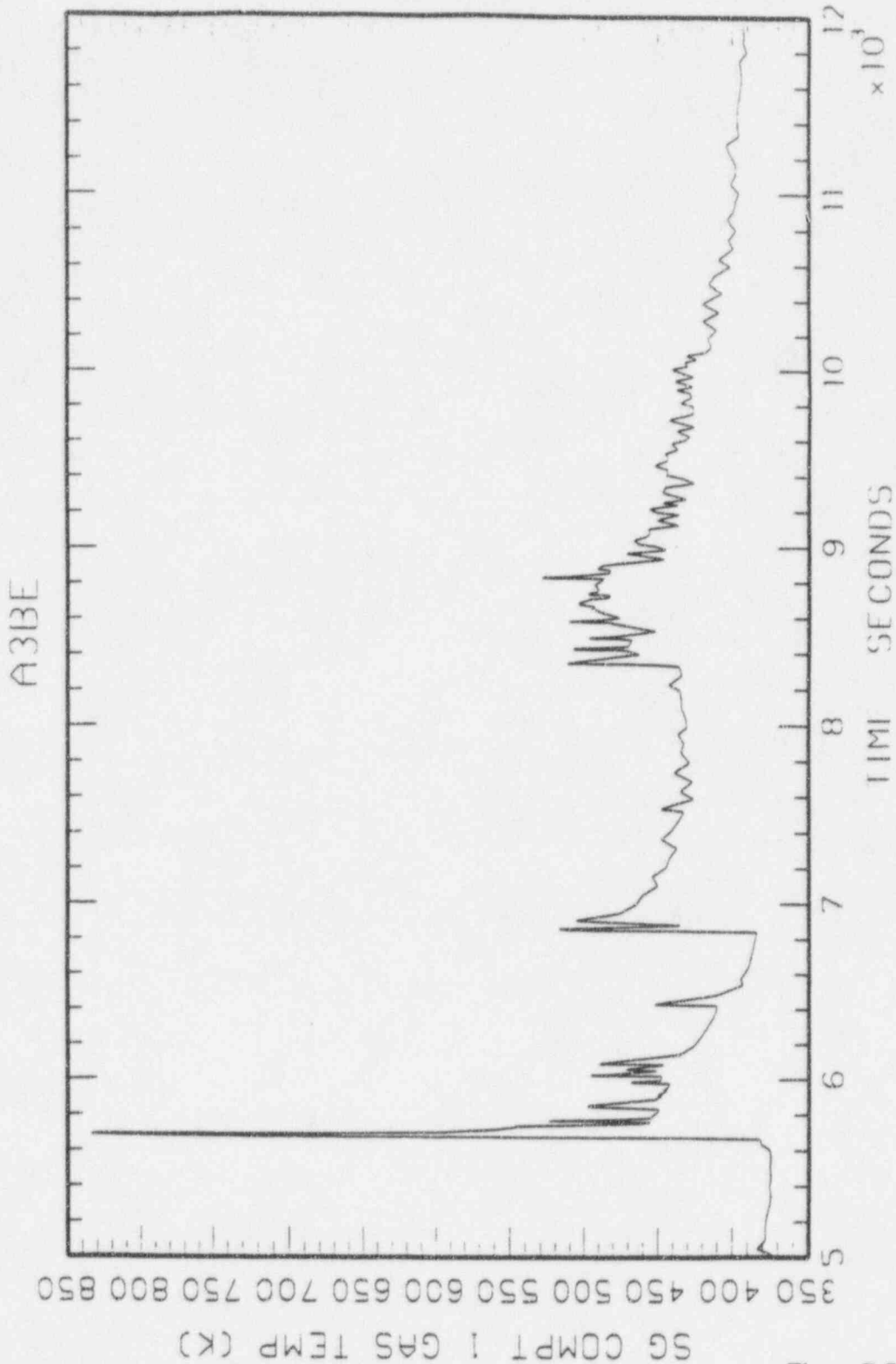

A3BE
SG COMPT 1 GAS TEMP (K)
350 400 450 500 550 600 650 700 750 800 850
5 6 7 8 9 10 11 12
TIME SECONDS
x 10³

Figure D.7.1-1

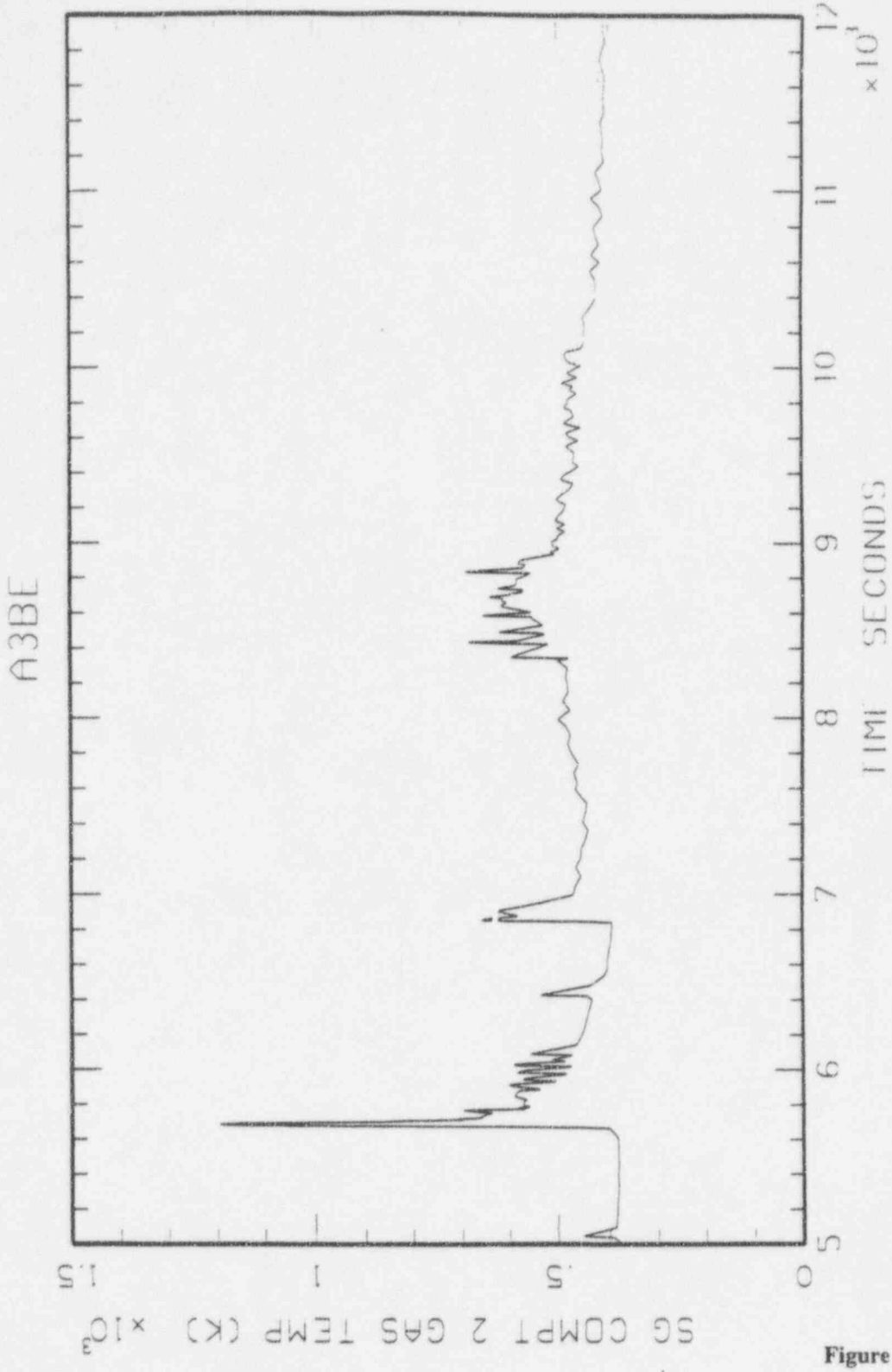

A3BE
SG COMPT 2 GAS TEMP (K) x10³
0
.5
1
1.5
5
6
7
8
9
10
11
12
x10³
TIME SECONDS

**Figure D.7.1-2**

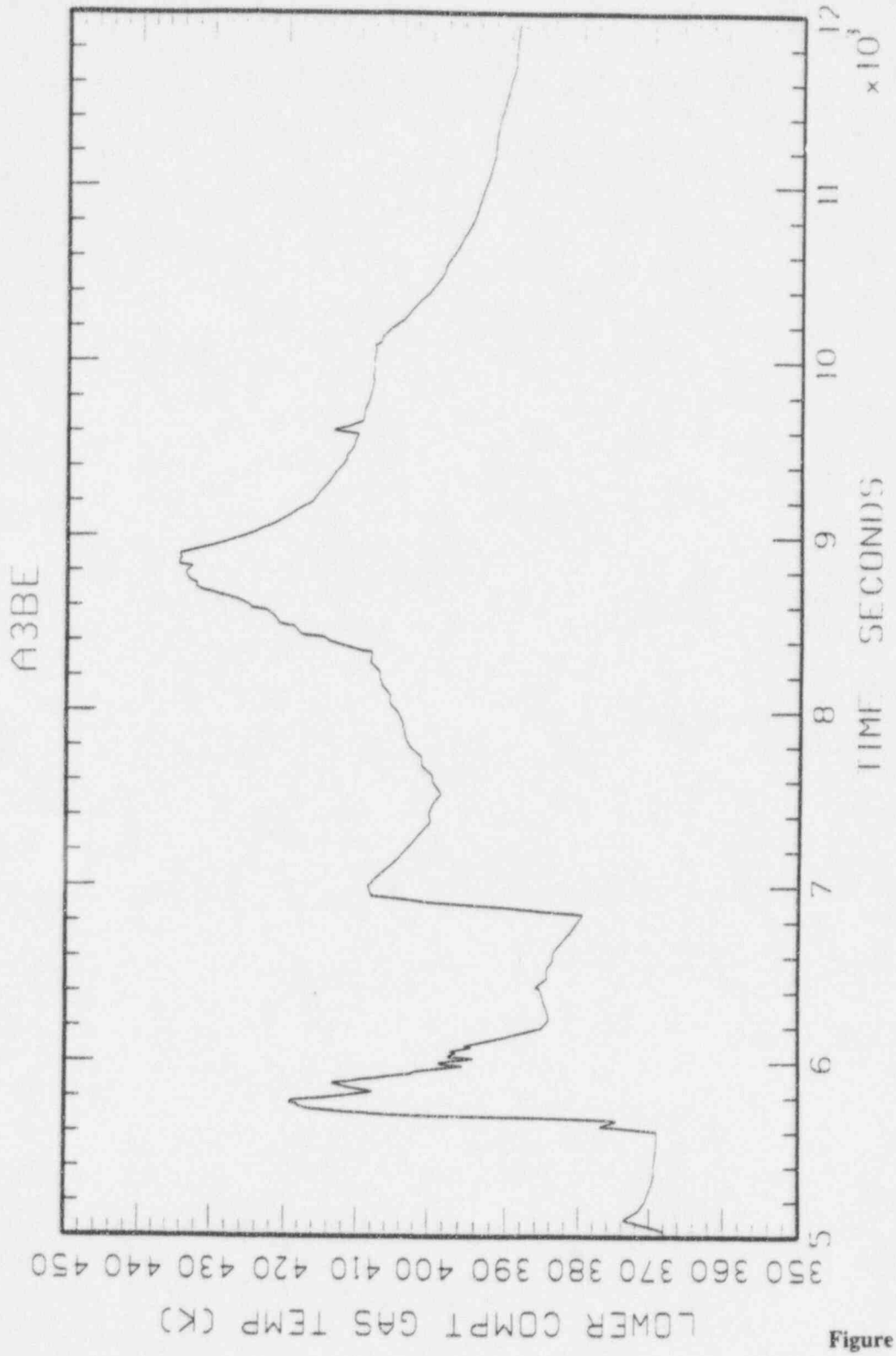

A3BE
LOWER COMPT GAS TEMP (K)
350 360 370 380 390 400 410 420 430 440 450
5 6 7 8 9 10 11 12
x 10³
TIME SECONDS

Figure D.7.1-3

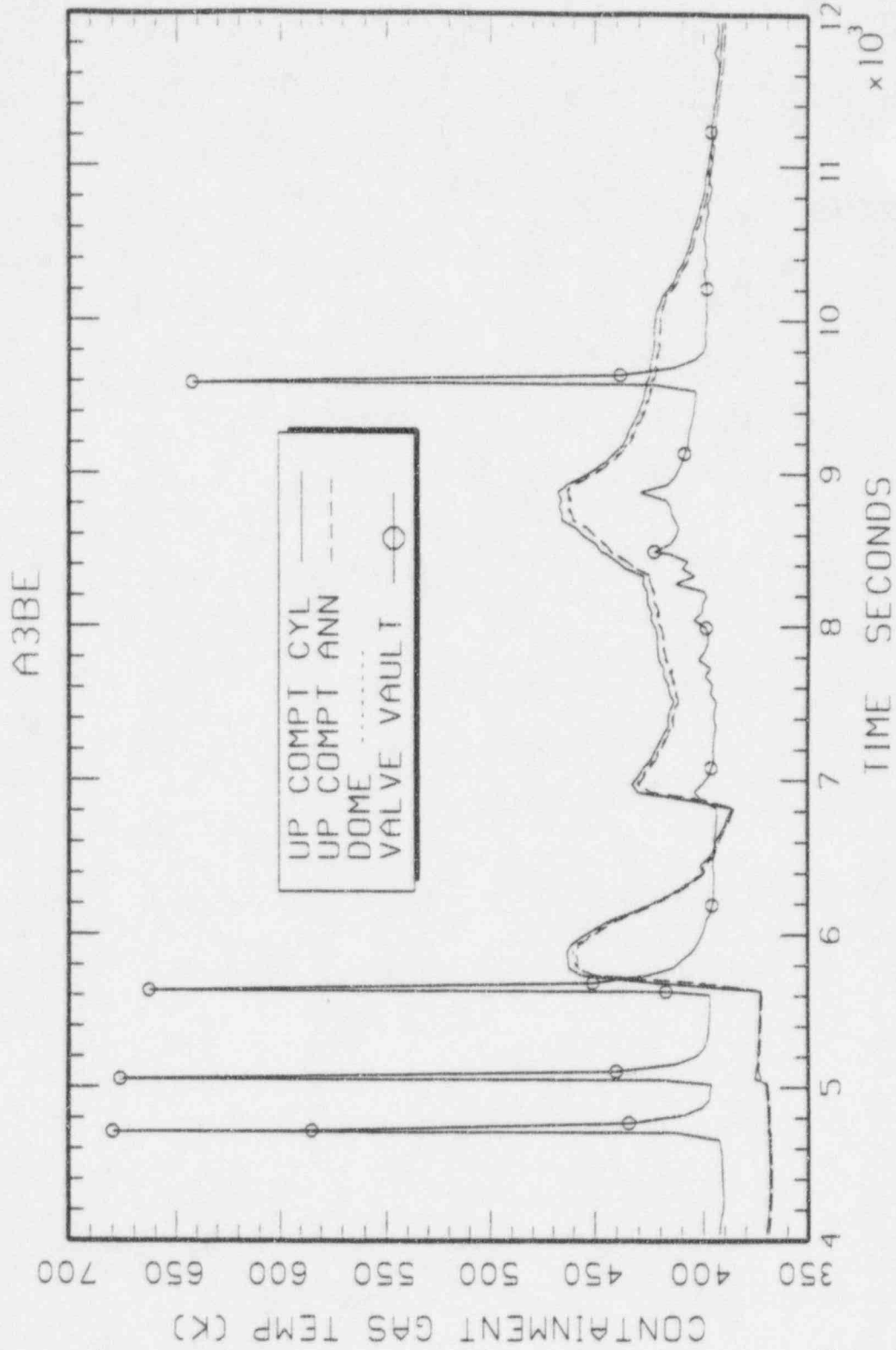

A3BE
UP COMPT CYL
UP COMPT ANN
DOME
VALVE VAULT
CONTAINMENT GAS TEMP (K)
350
400
450
500
550
600
650
700
4
5
6
7
8
9
10
11
12
$\times 10^3$
TIME SECONDS

Figure D.7.1-4

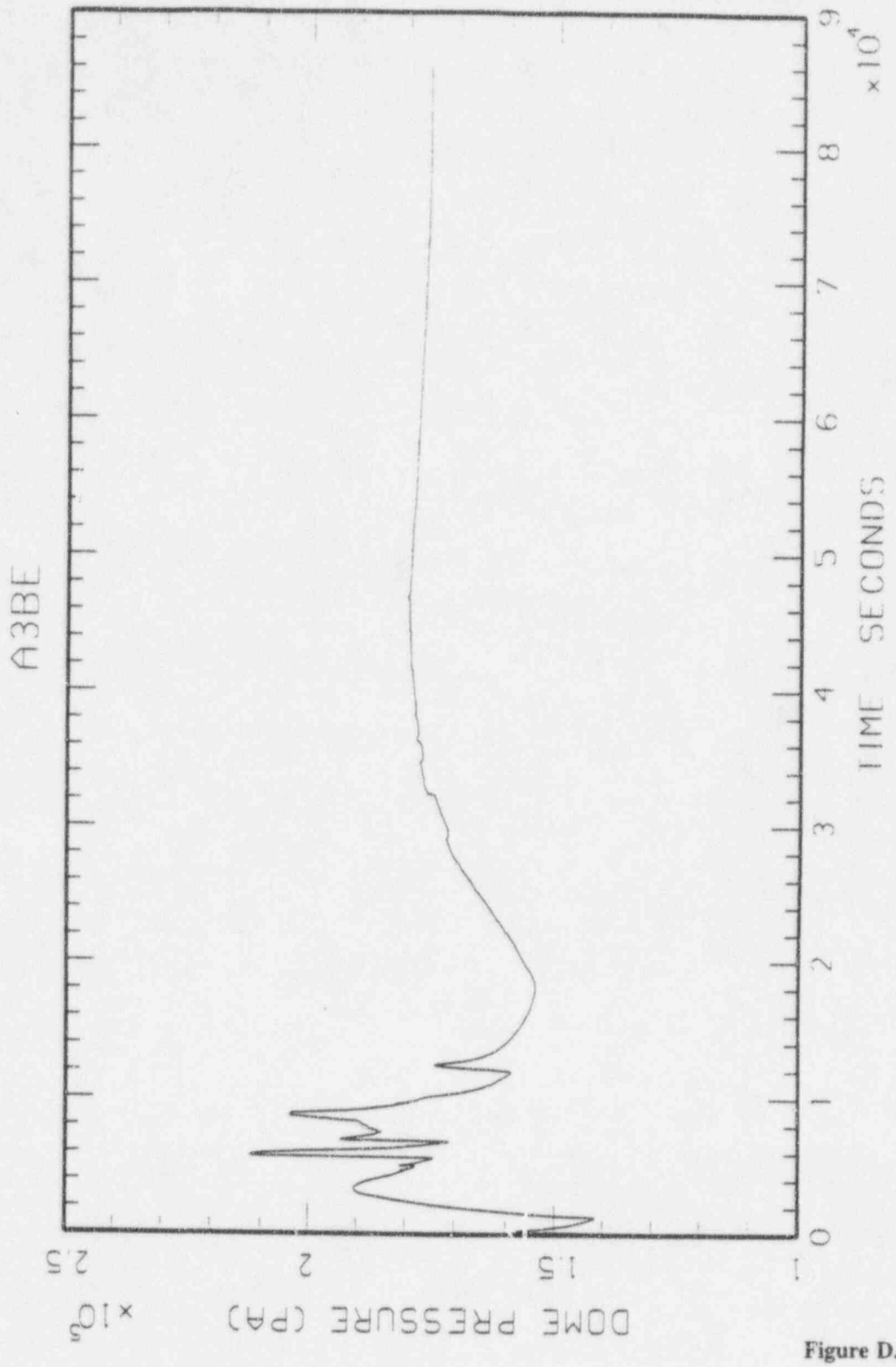

A3BE
DOME PRESSURE (PA)
×10^5
TIME SECONDS
×10^4
0
1
2
3
4
5
6
7
8
9
1
1.5
2
2.5

Figure D.7.1-5

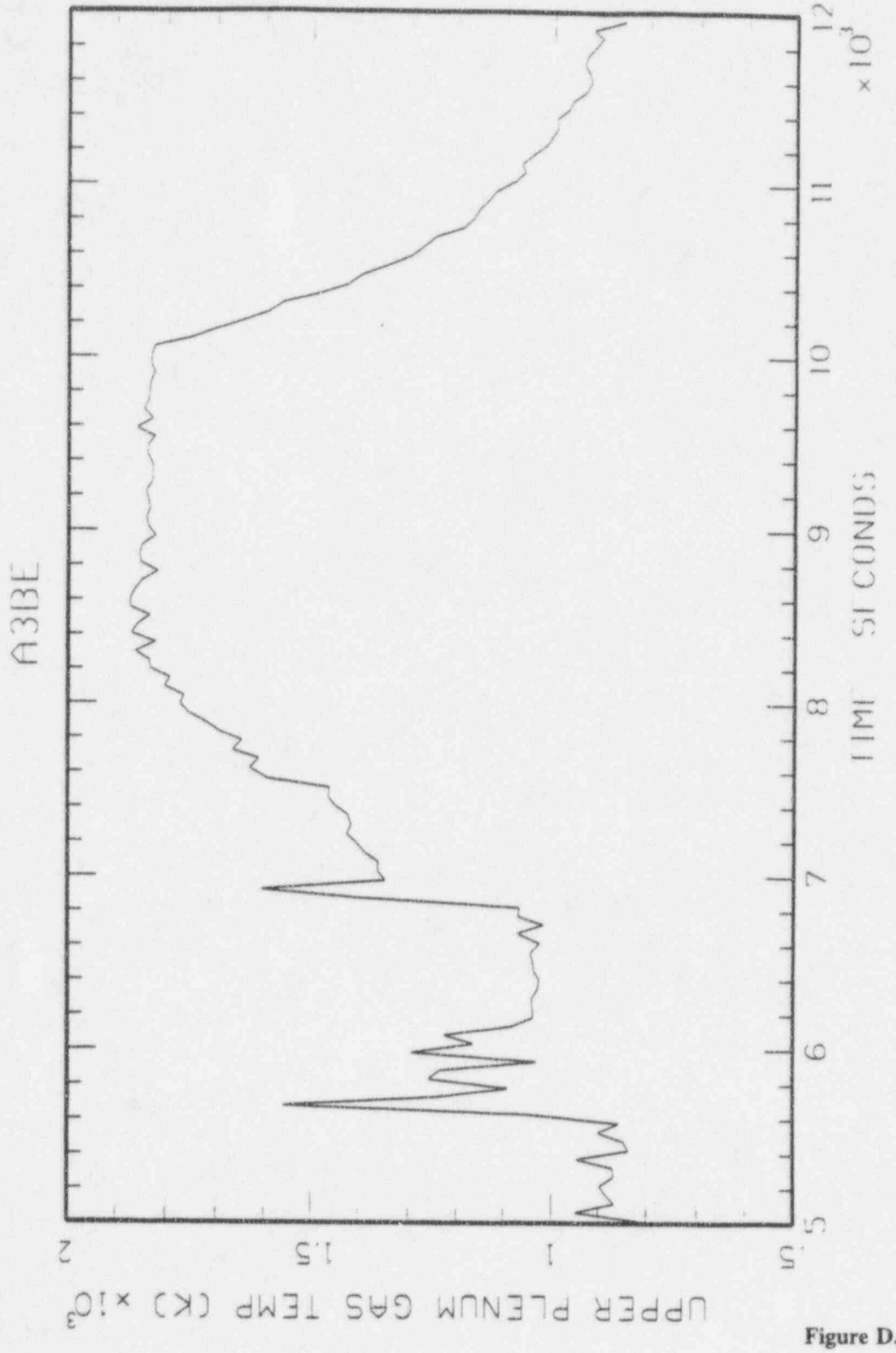

UPPER PLENUM GAS TEMP (K) x10³
2
1.5
1
.5
5
6
7
8
9
10
11
12
x10³
TIME SI CONDS
A3BE

Figure D.7.1-6

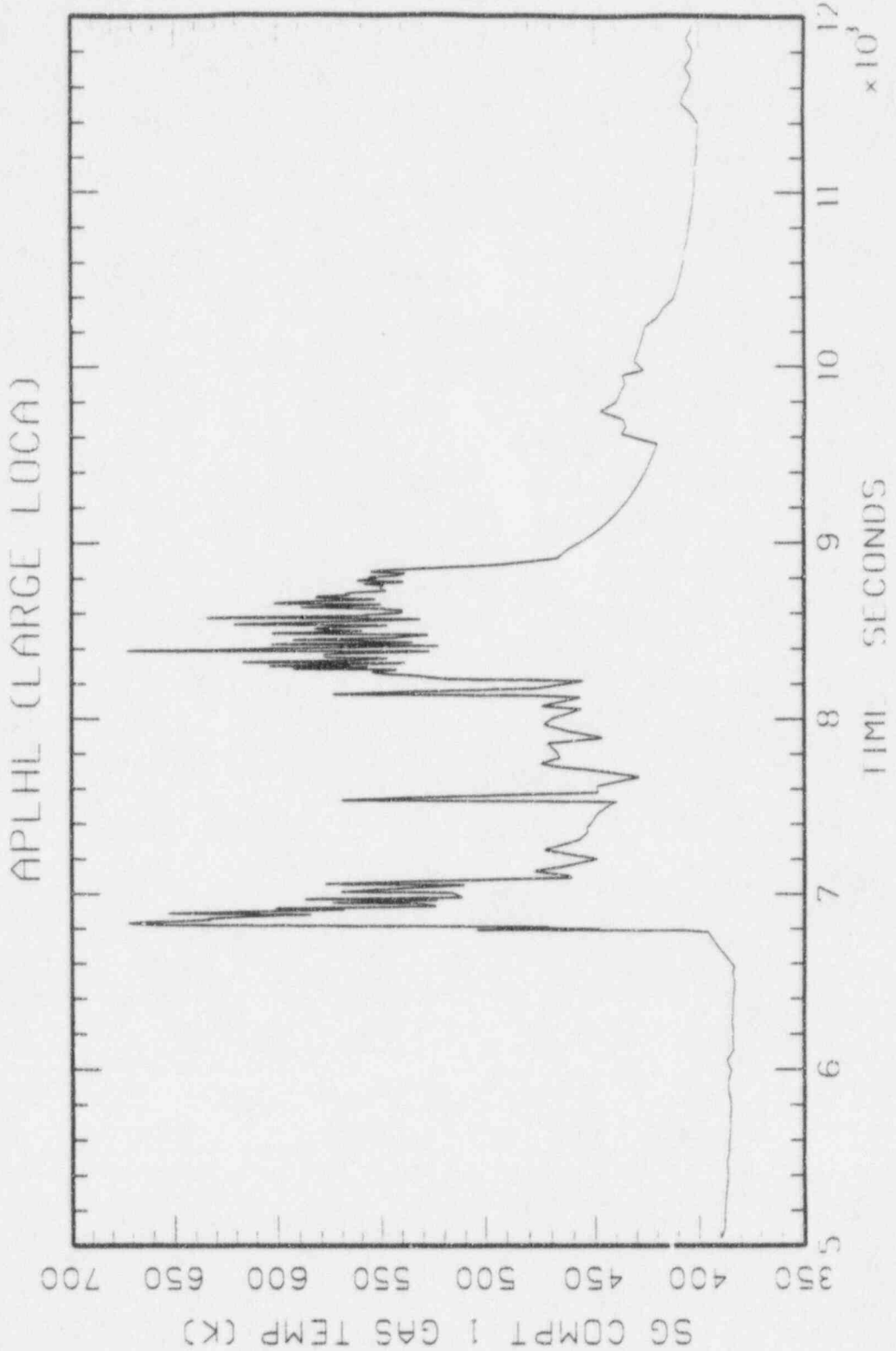

APLHL (LARGE LOCA)
SG COMPT 1 GAS TEMP (K)
350
400
450
500
550
600
650
700
5
6
7
8
9
10
11
12
TIME SECONDS
x10³

Figure D.7.1-7

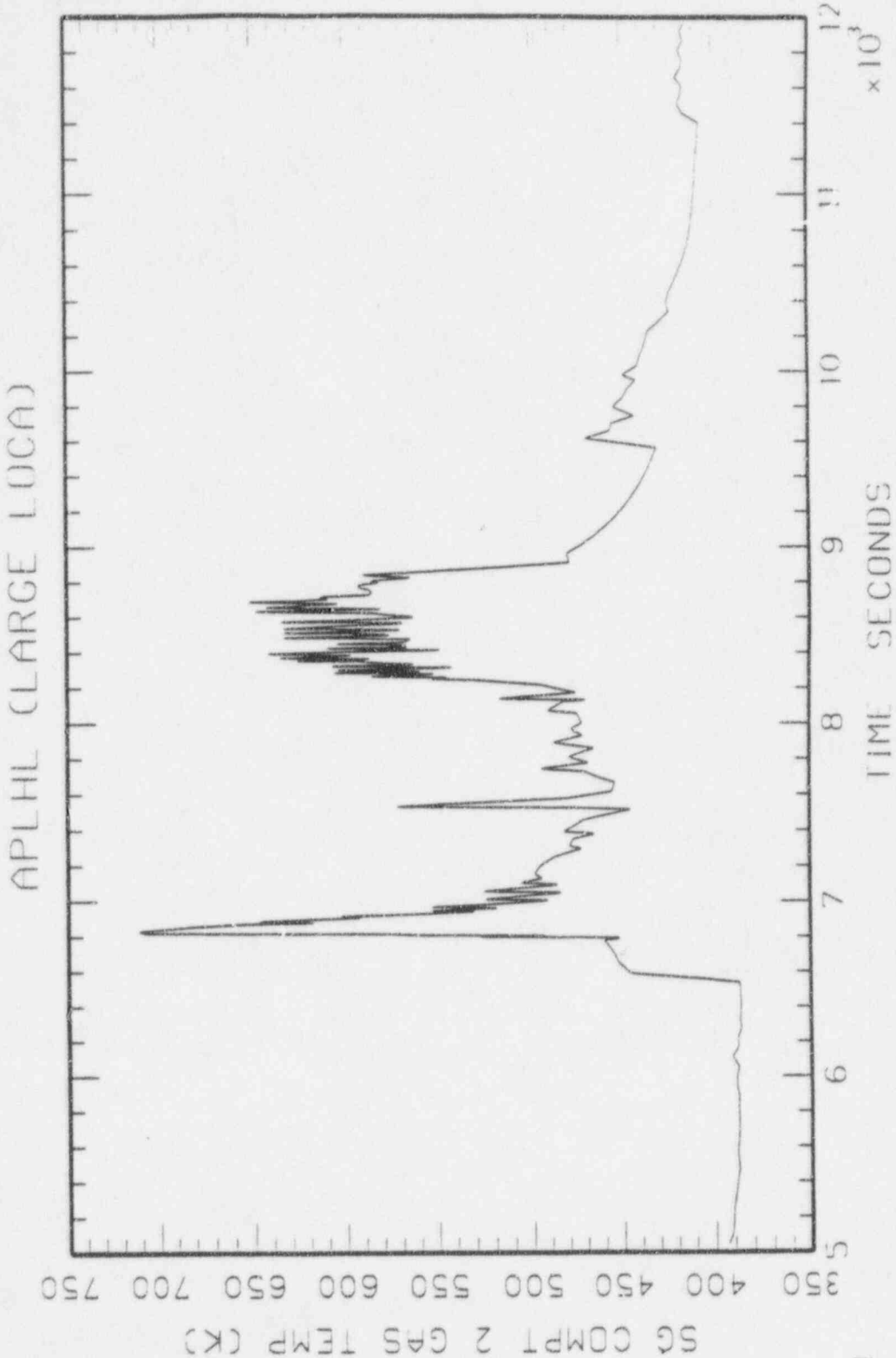

APLHL CLARGE LOCA)
SG COMPT 2 GAS TEMP (K)
350
400
450
500
550
600
650
700
750
5
6
7
8
9
10
11
12
x10³
TIME SECONDS

Figure D.7.1-8

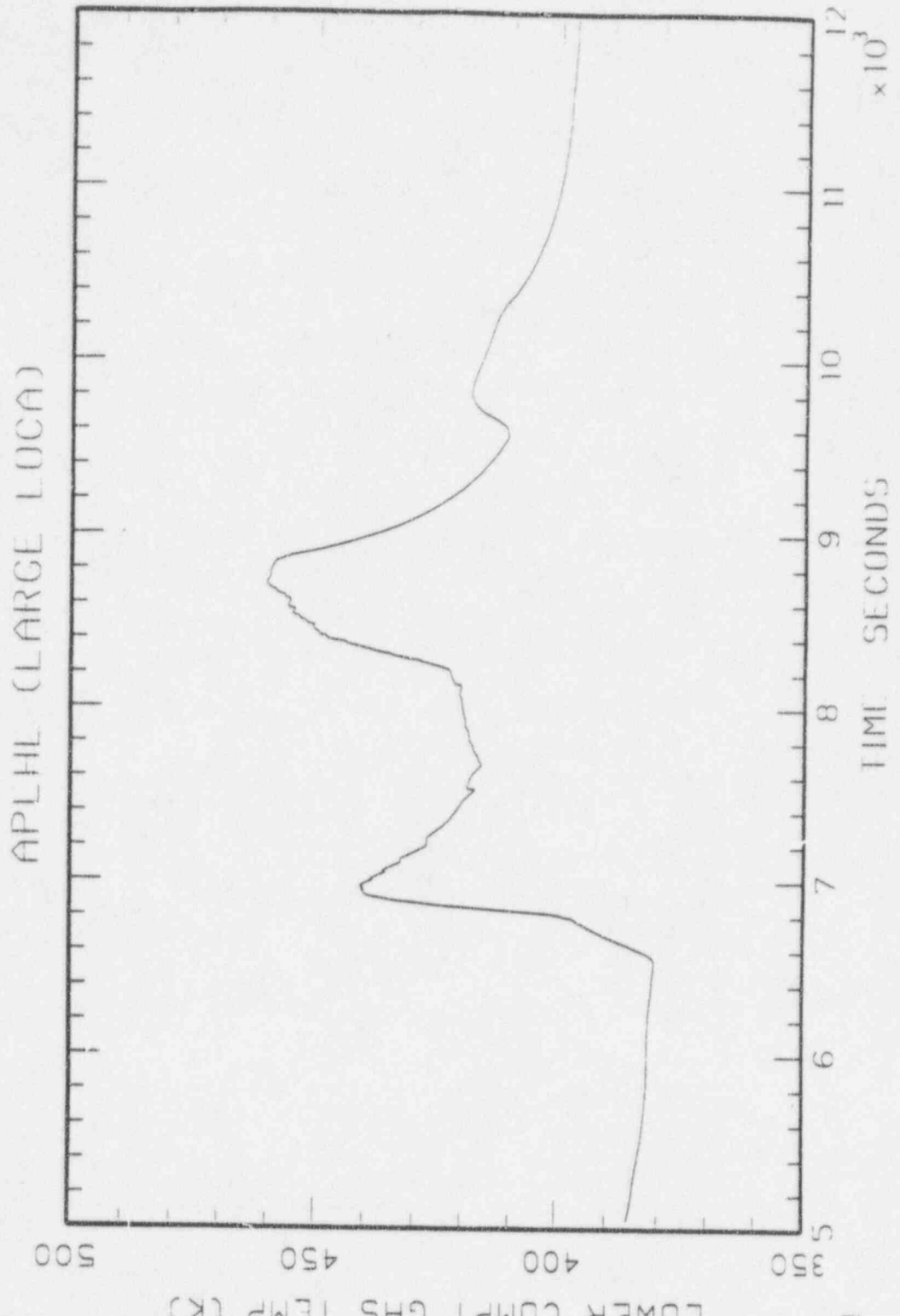

APLHL (LARGE LOCA)
LOWER COMPT GAS TEMP (K)
500
450
400
350
5
6
7
8
9
10
11
12
x10³
TIME SECONDS

Figure D.7.1-9

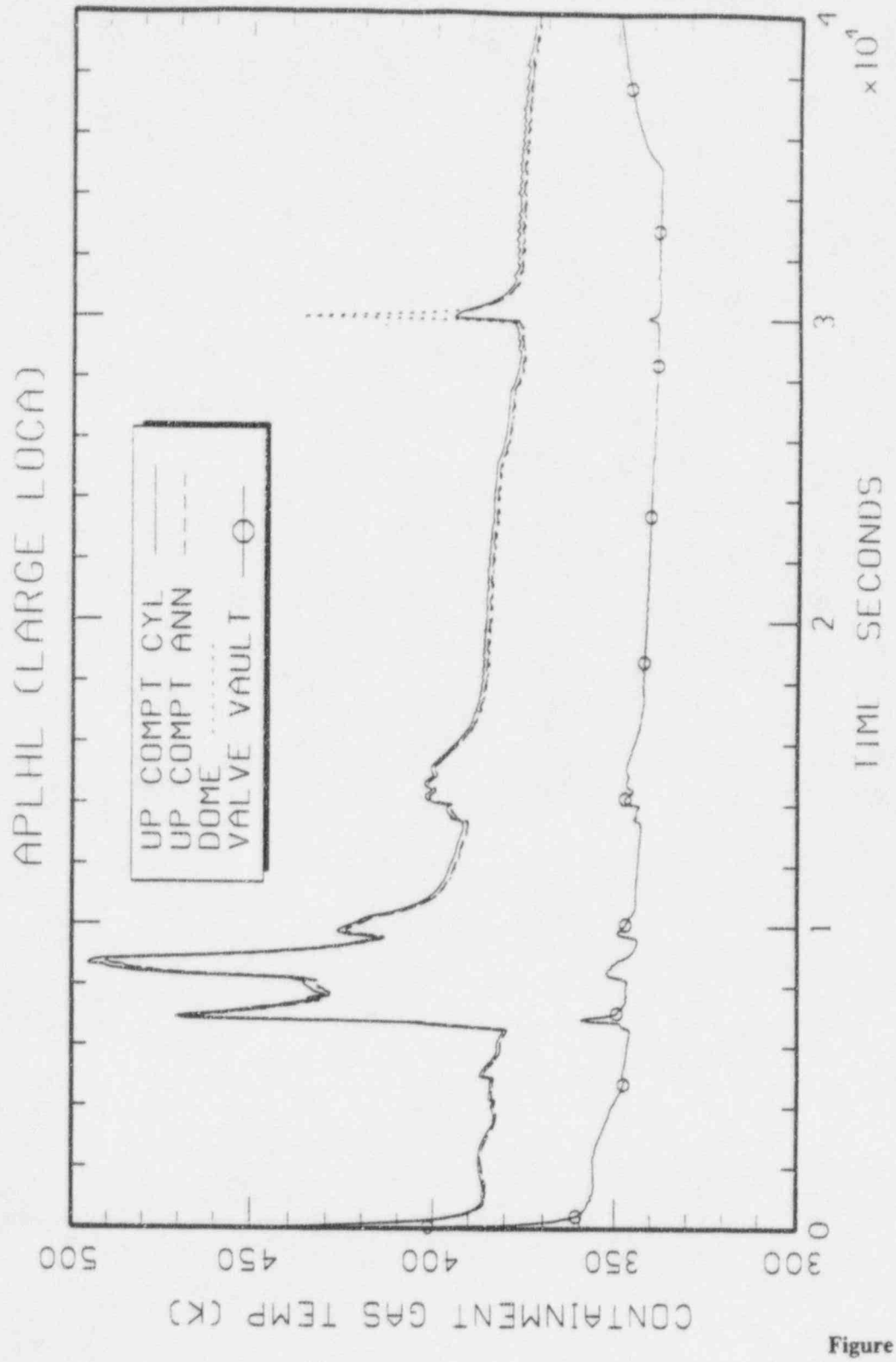



Figure D.7.1-10

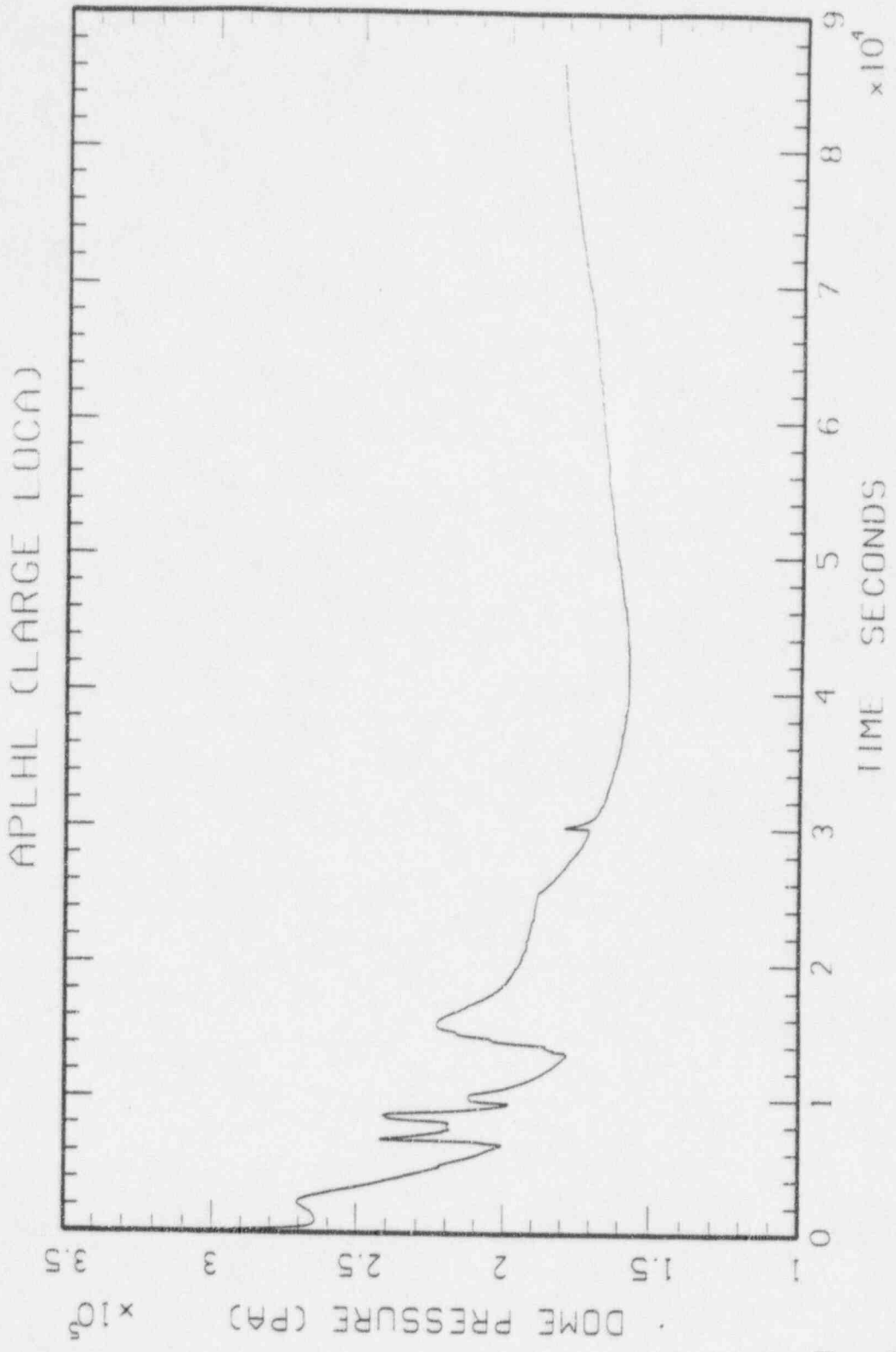



Figure D.7.1-11

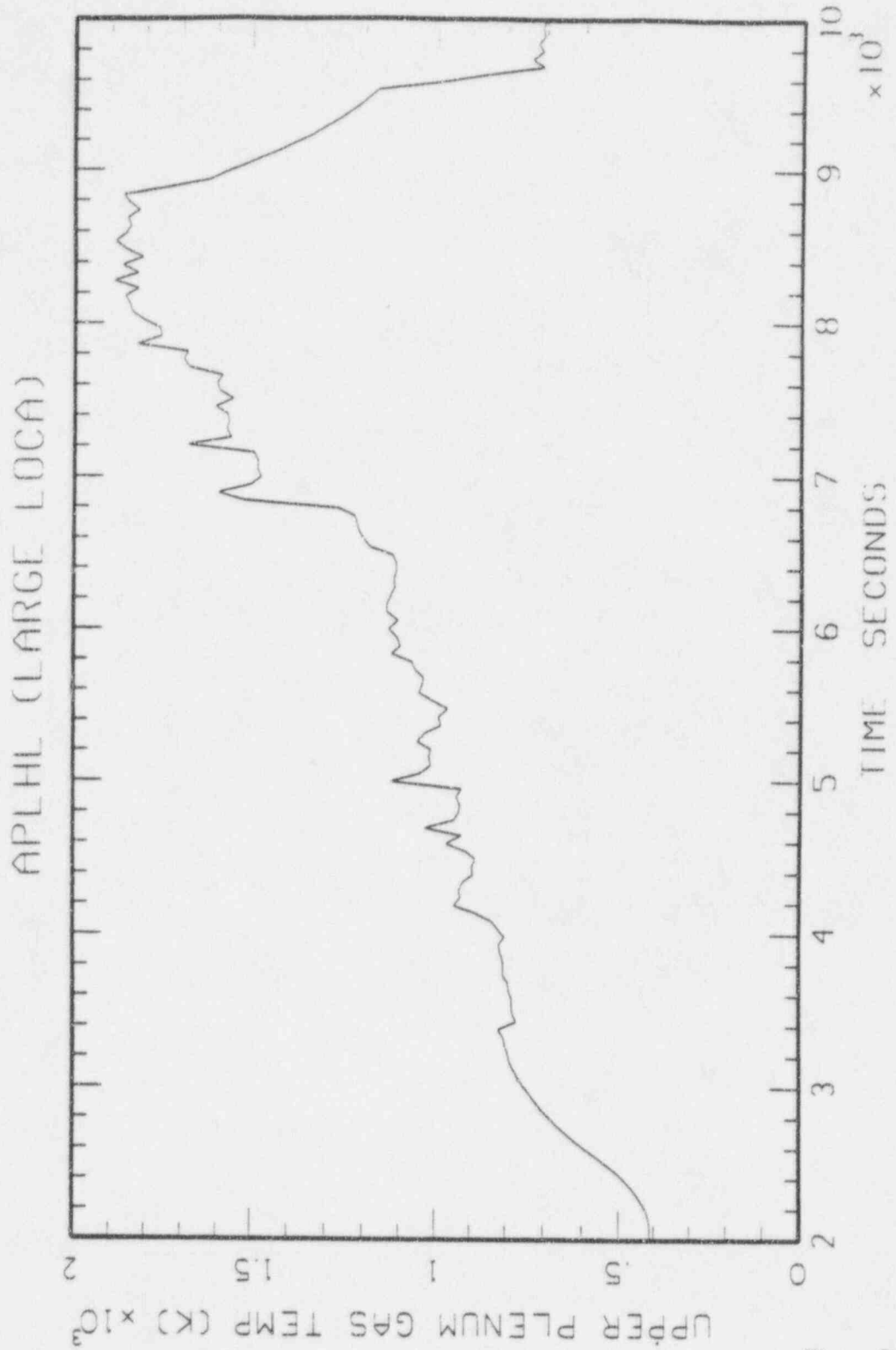



Figure D.7.1-12

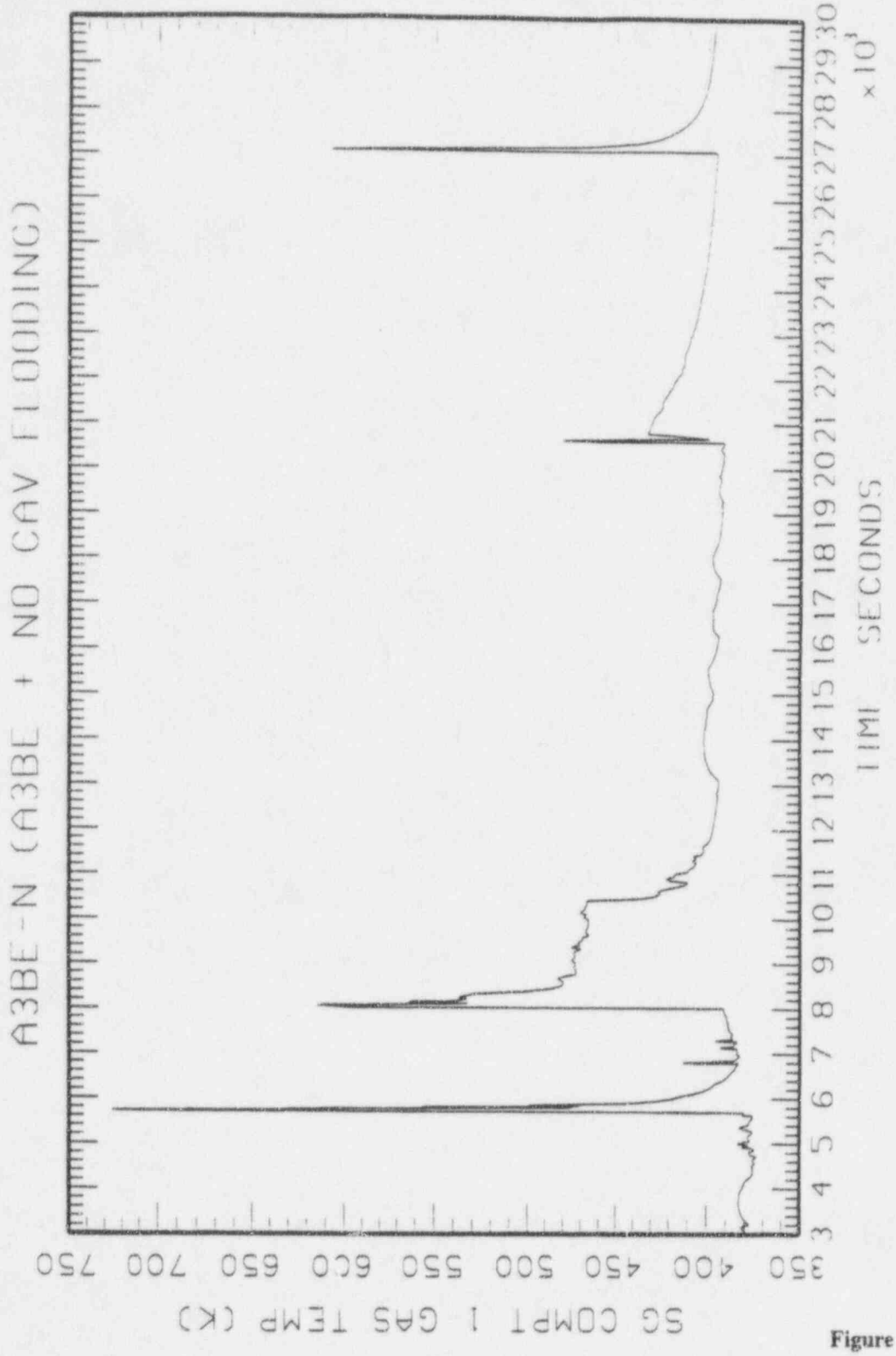



Figure D.7.1-13

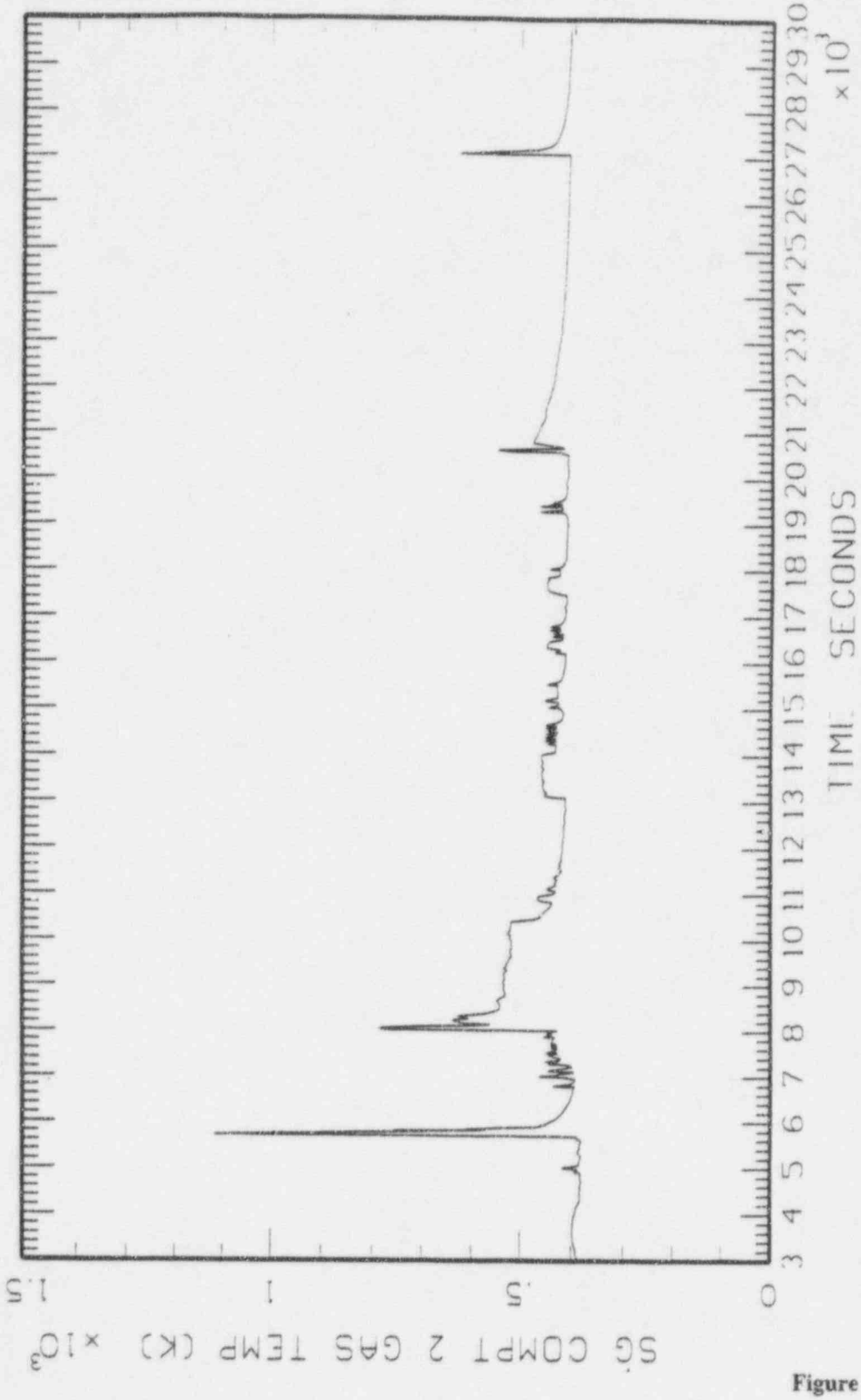



Figure D.7.1-14

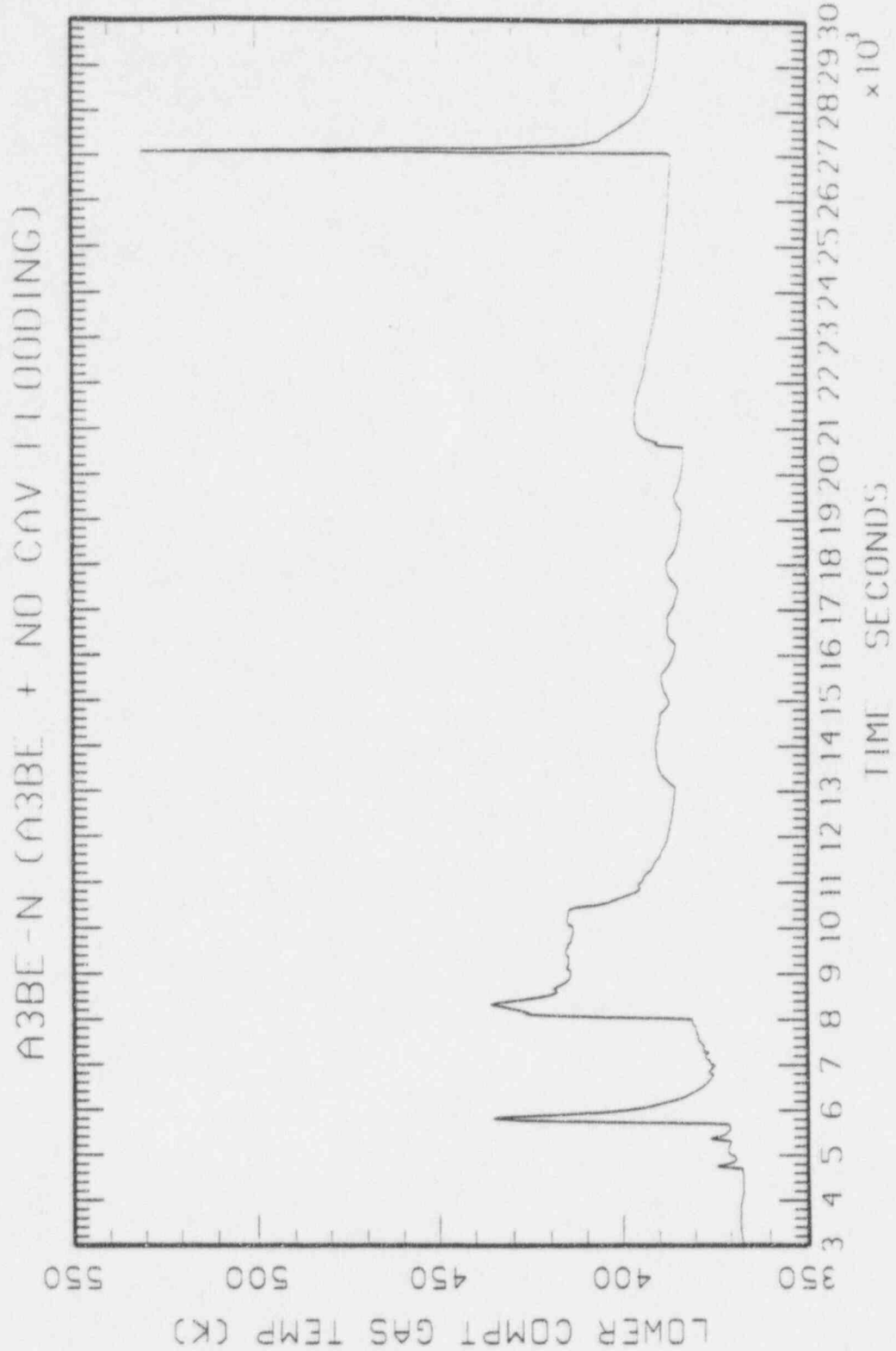



Figure D.7.1-15

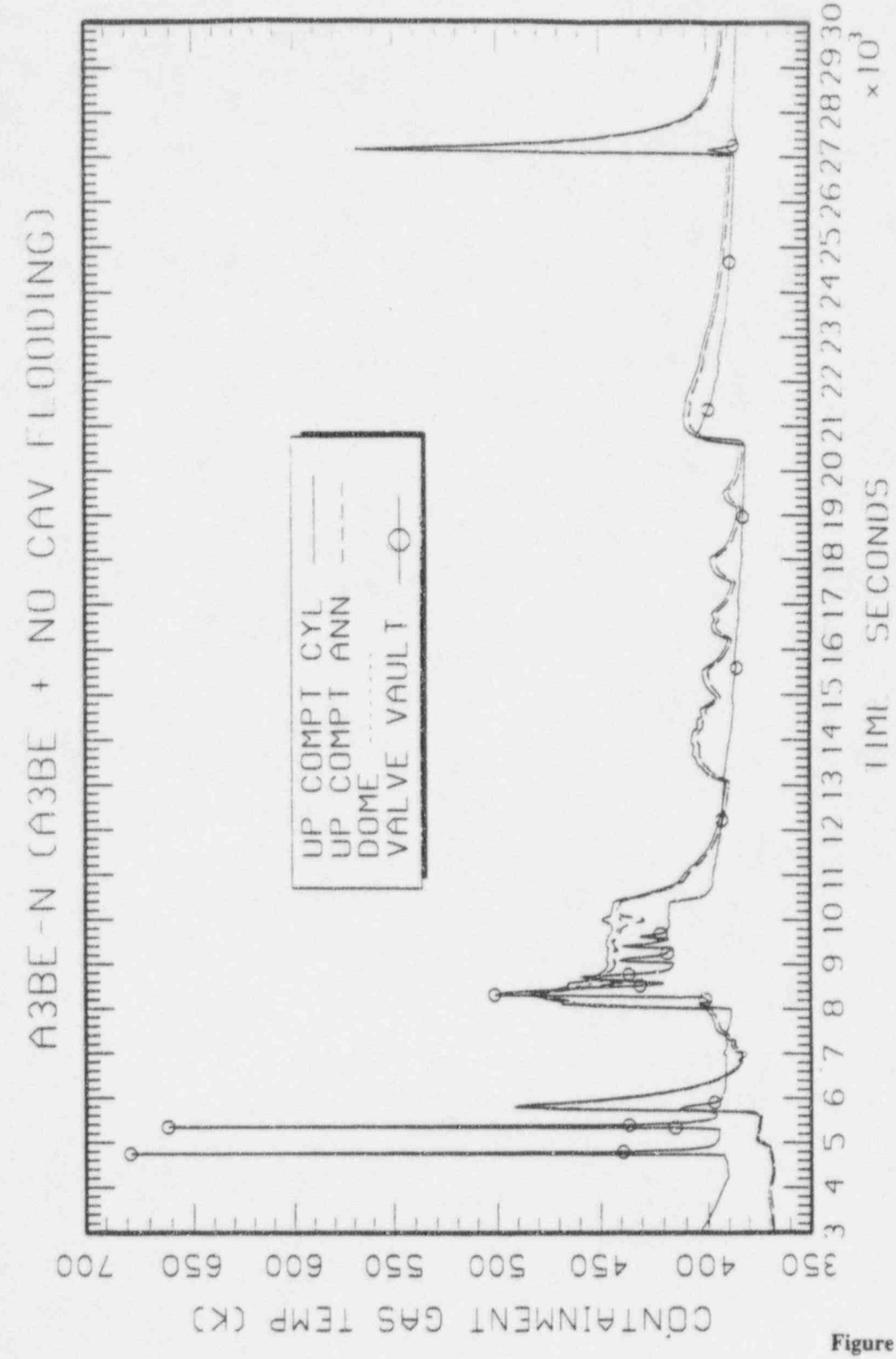



Figure D.7.1-16

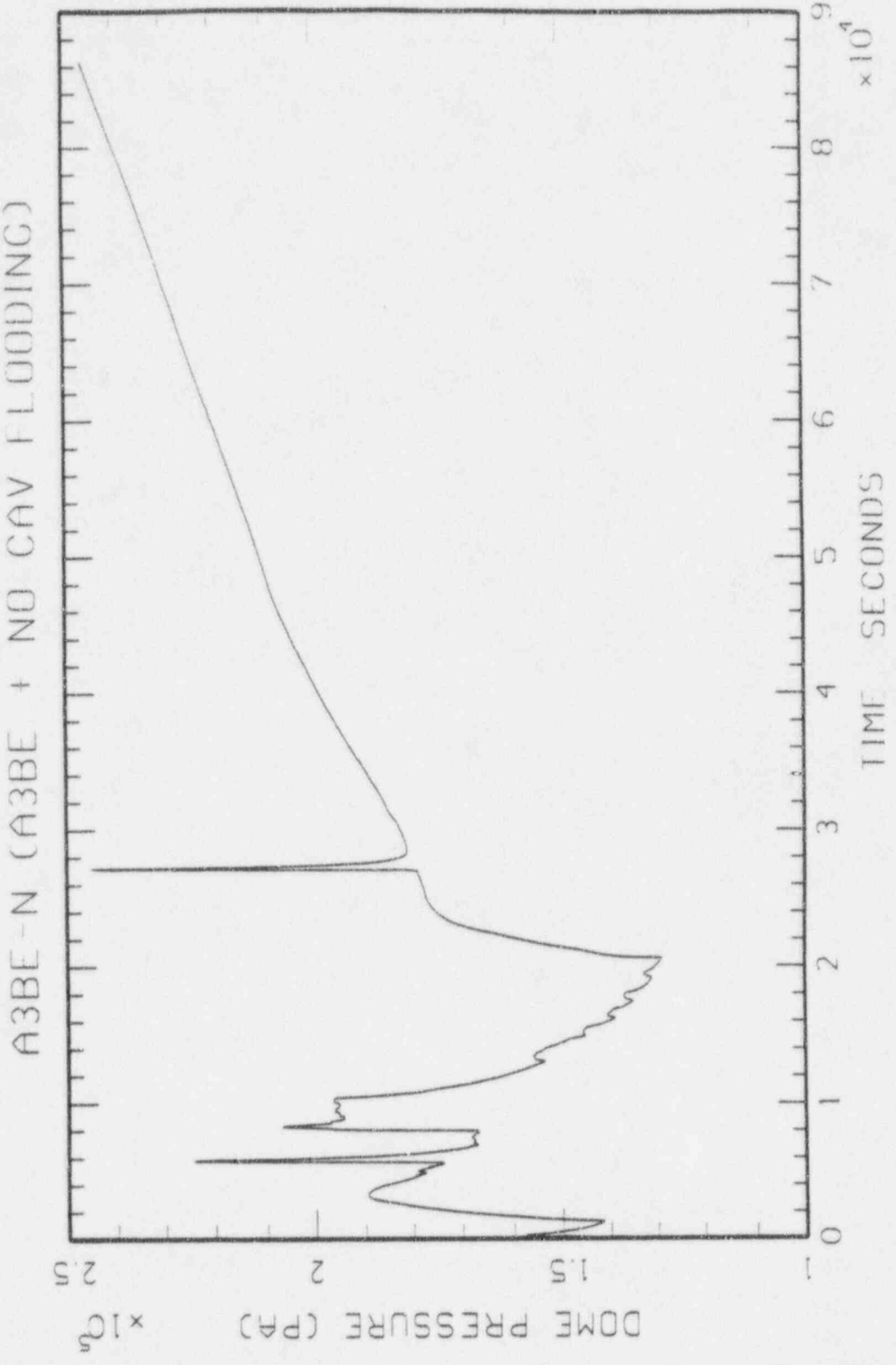



Figure D.7.1-17

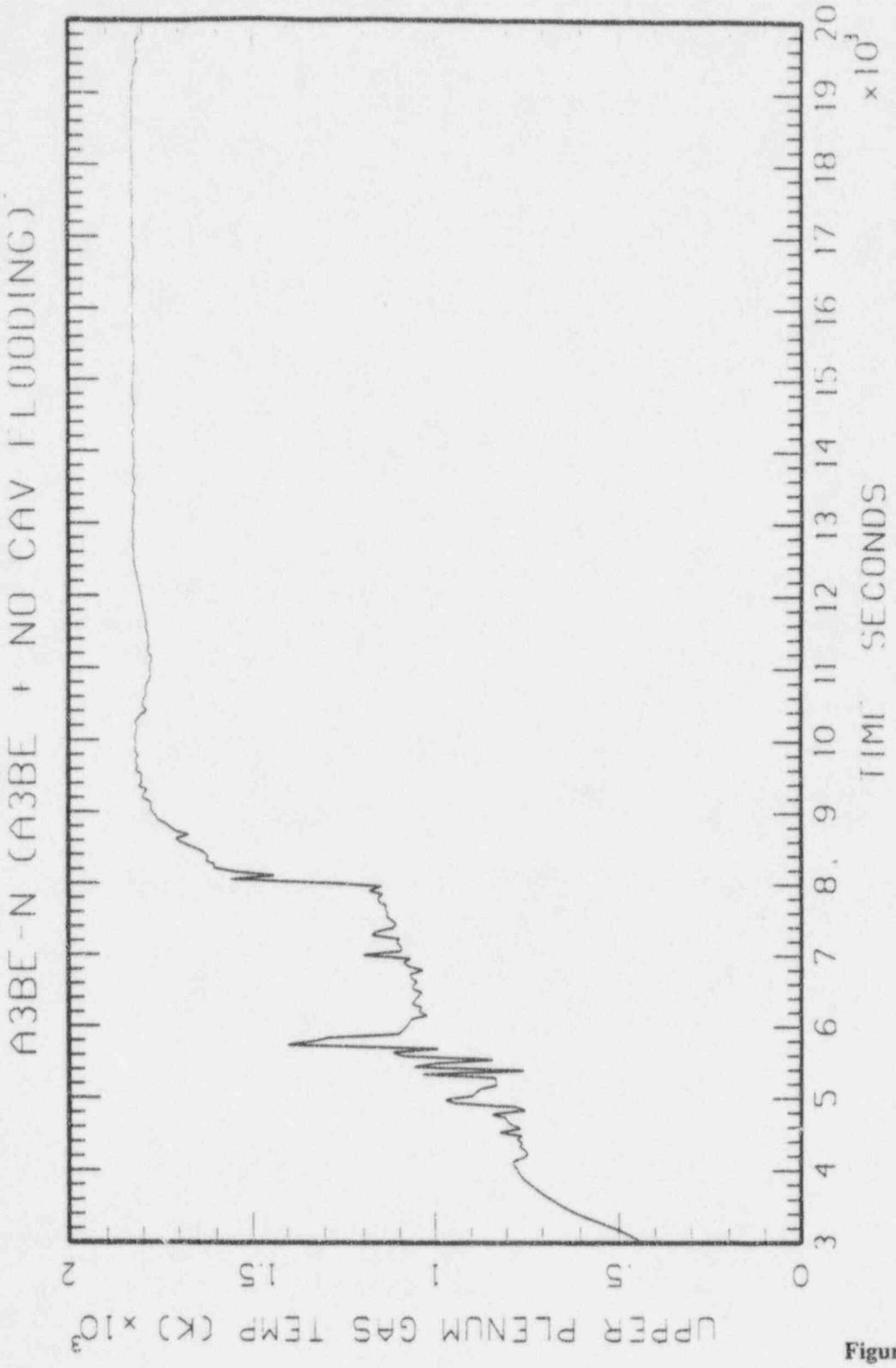



Figure D.7.1-18

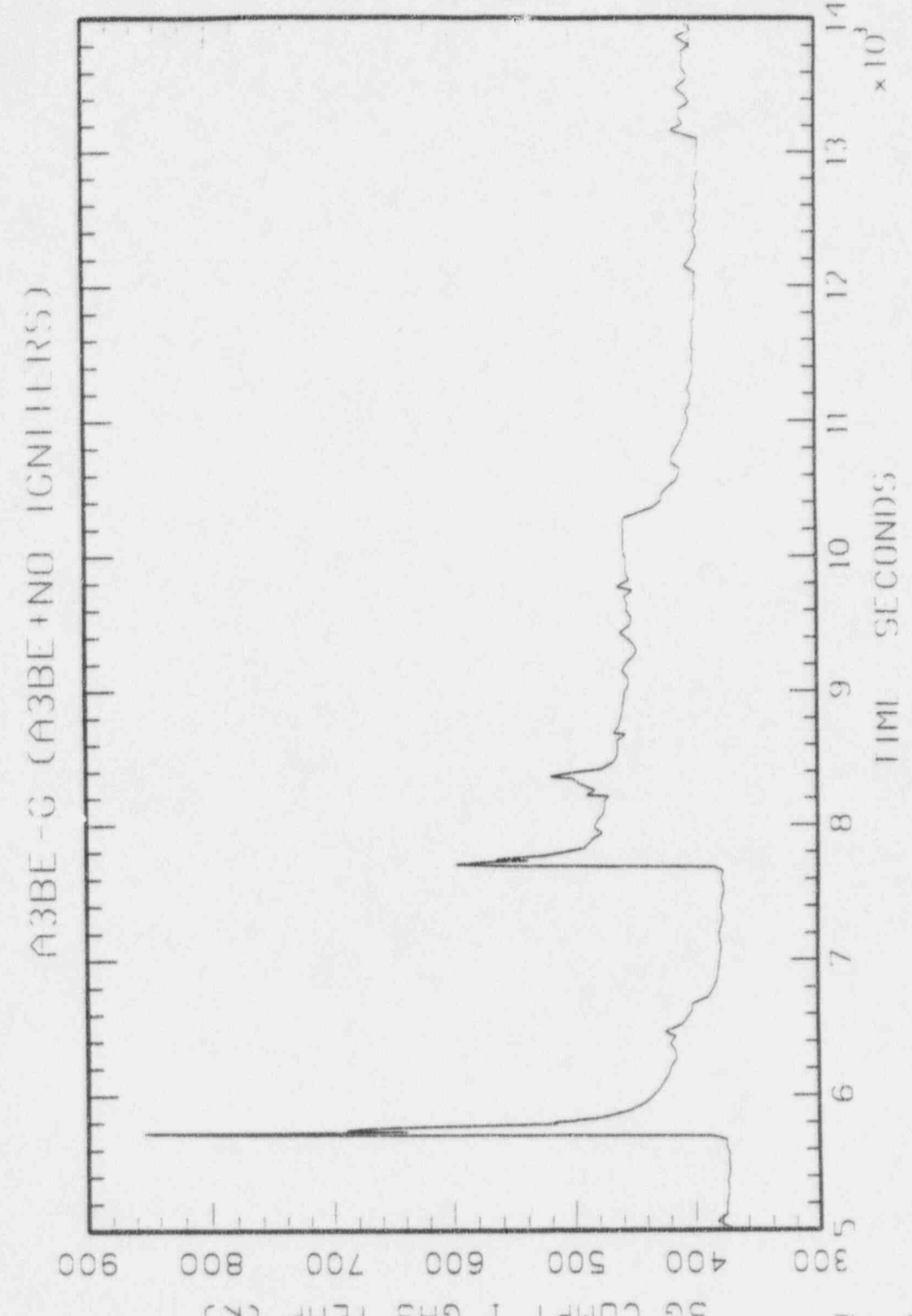



Figure D.7.1-19

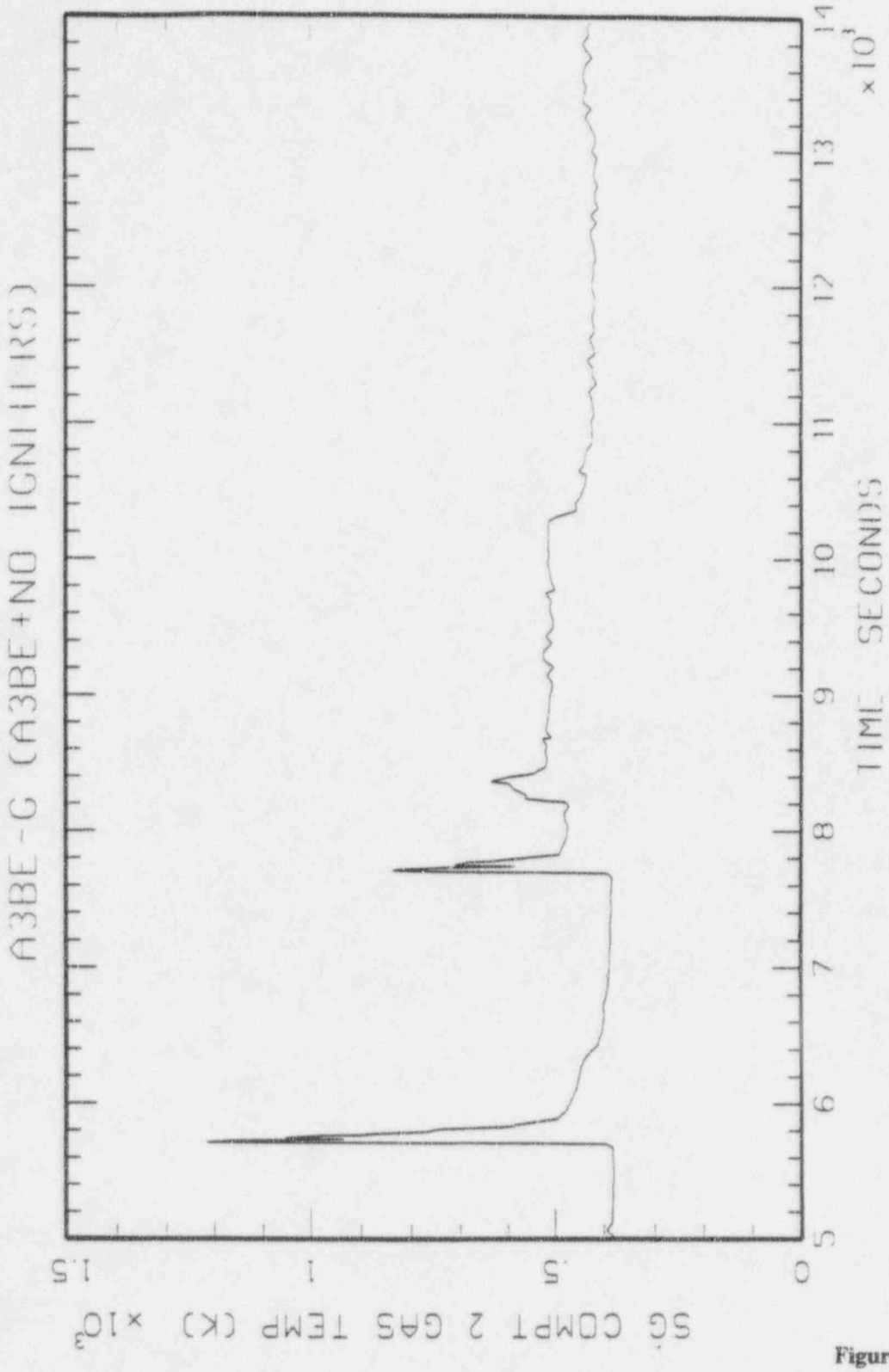



Figure D.7.1-20

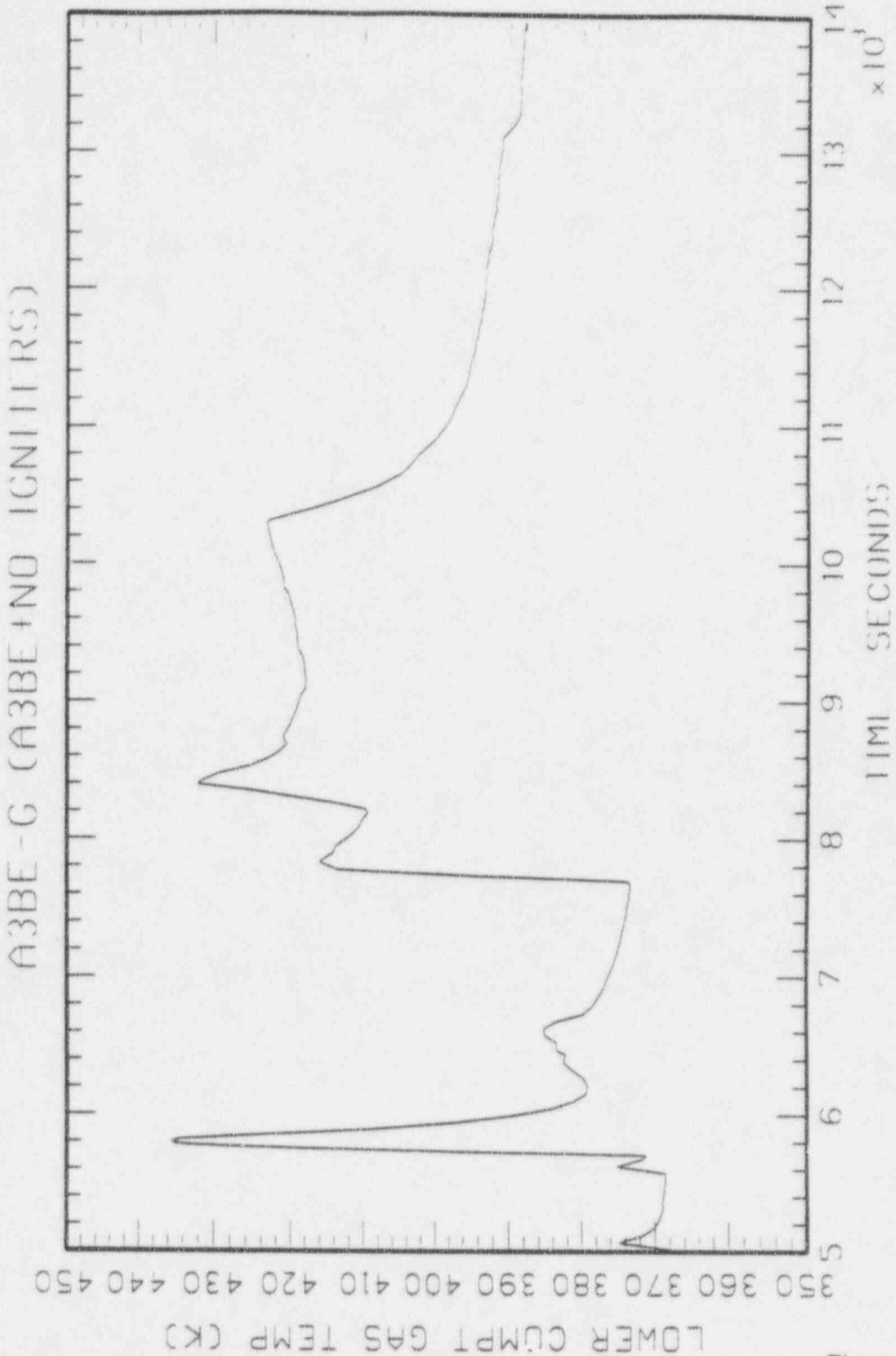



Figure D.7.1-21

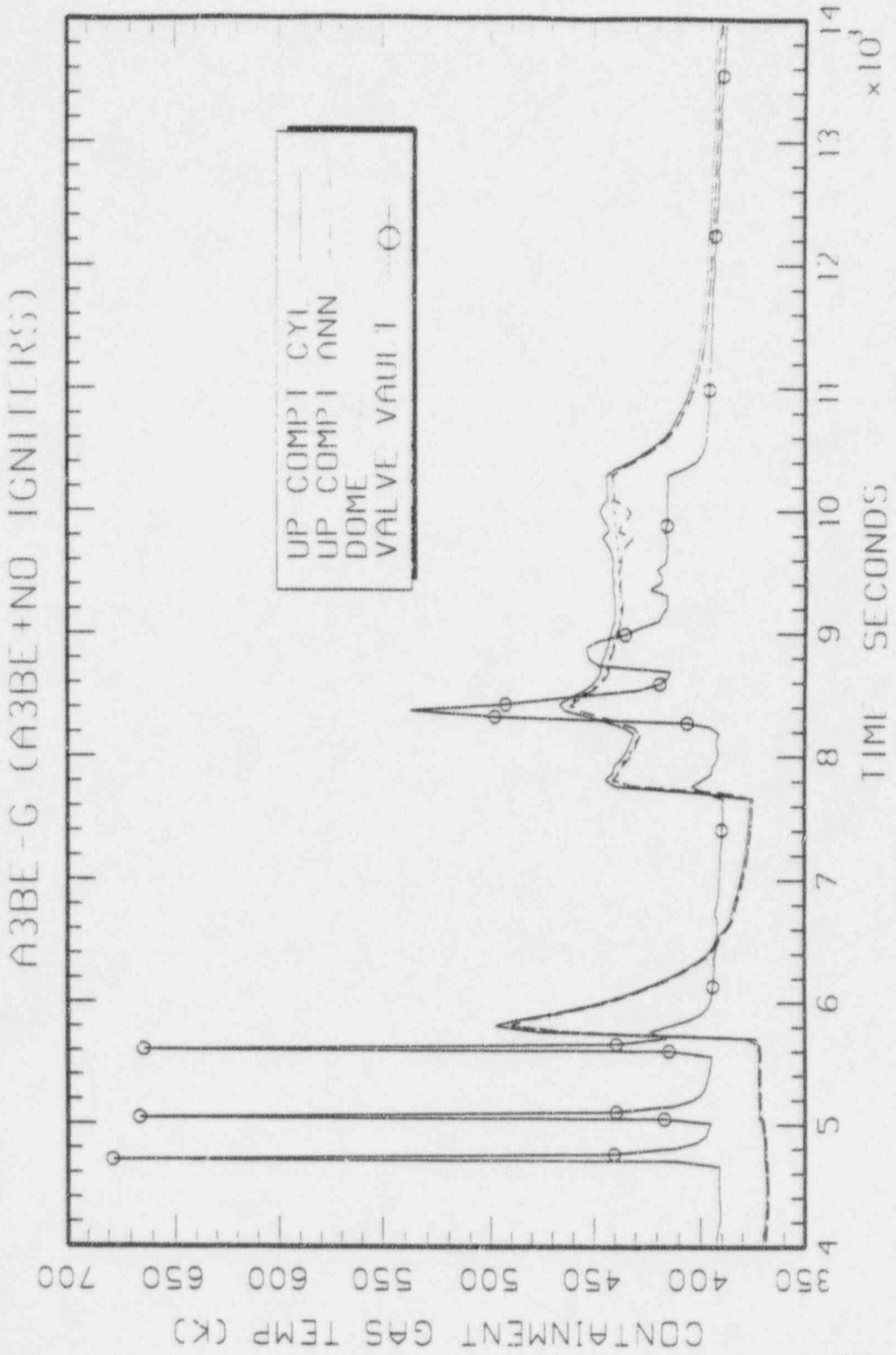



Figure D.7.1-22

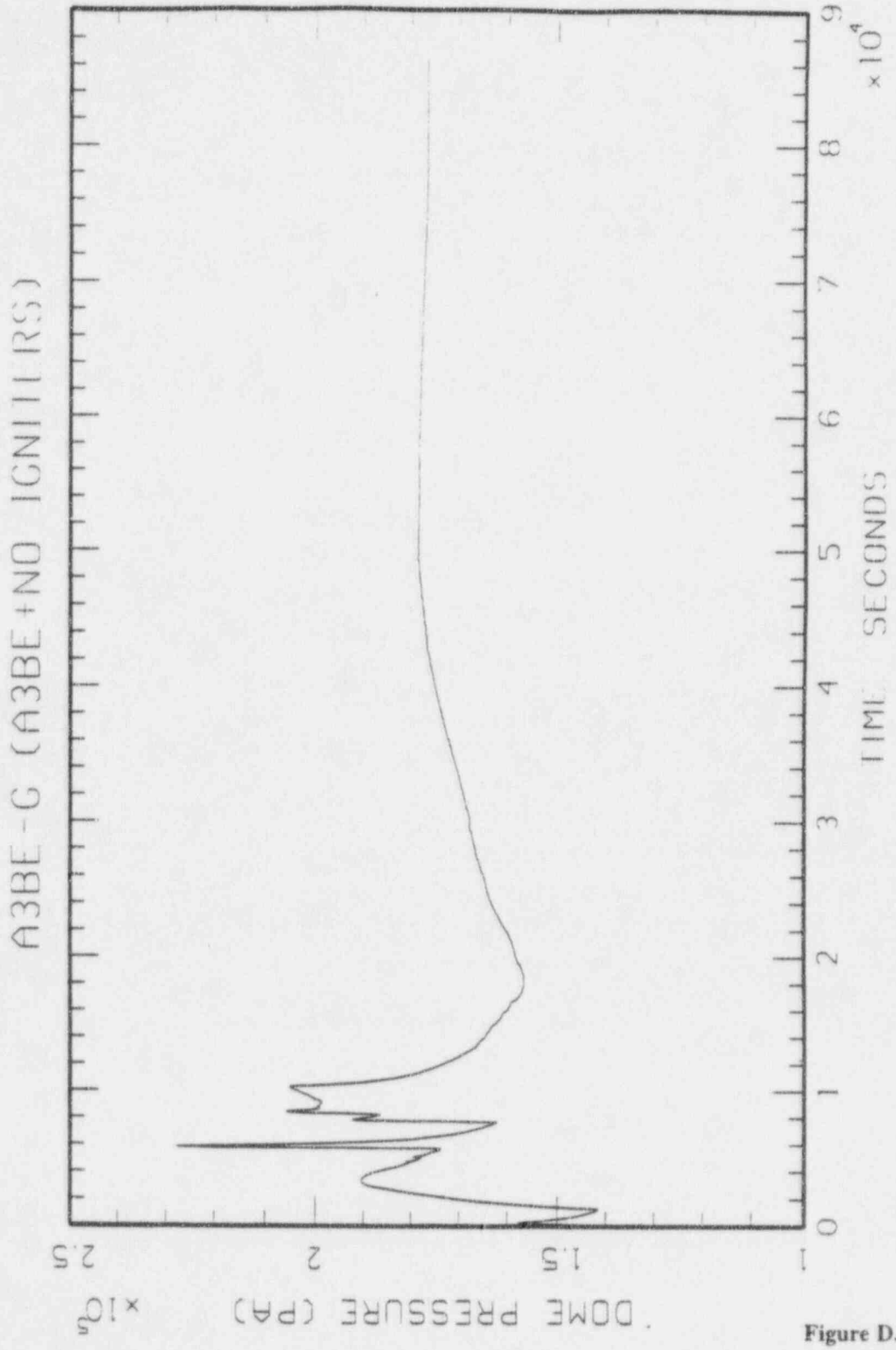



Figure D.7.1-23

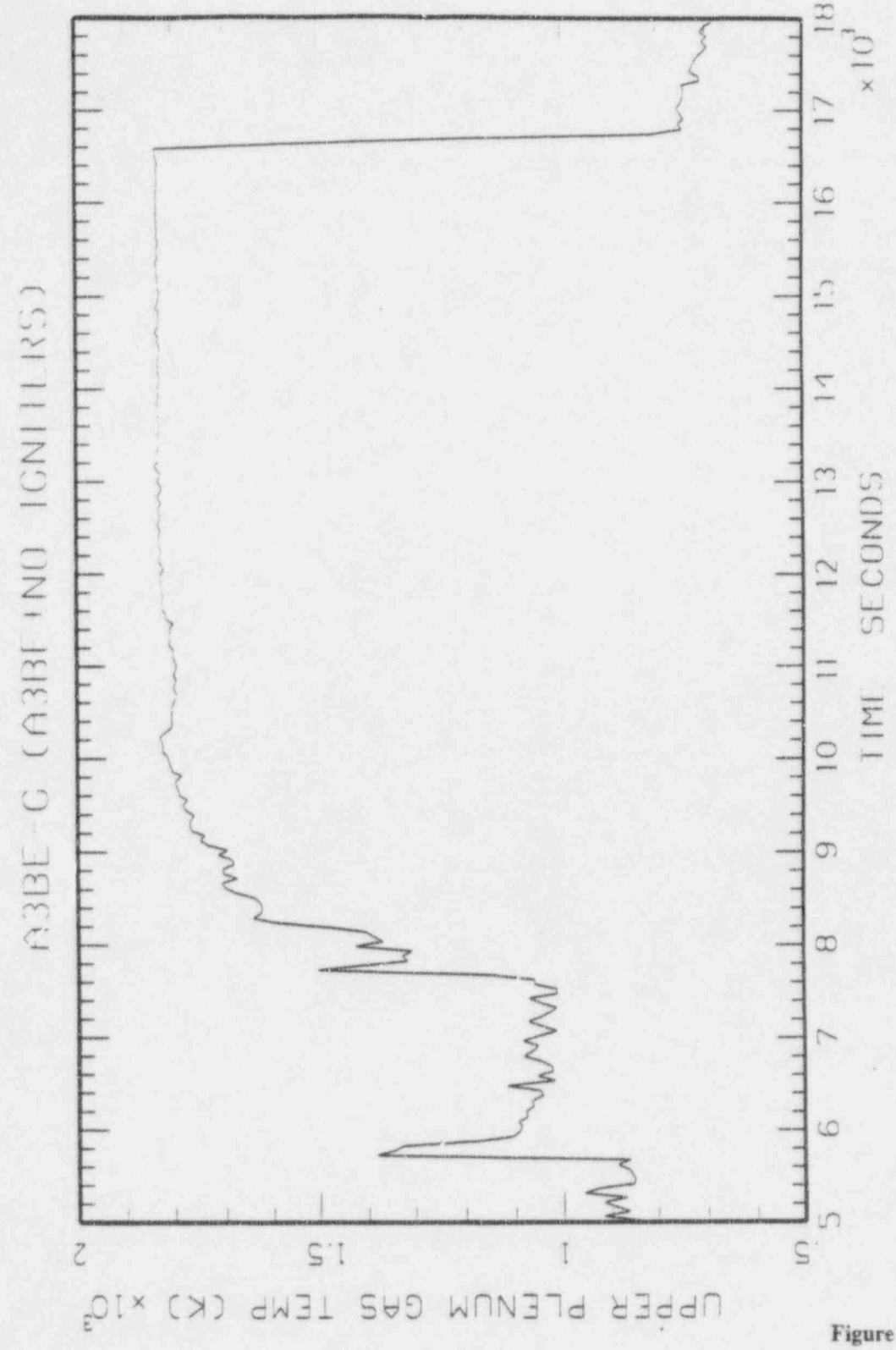



Figure D.7.1-24

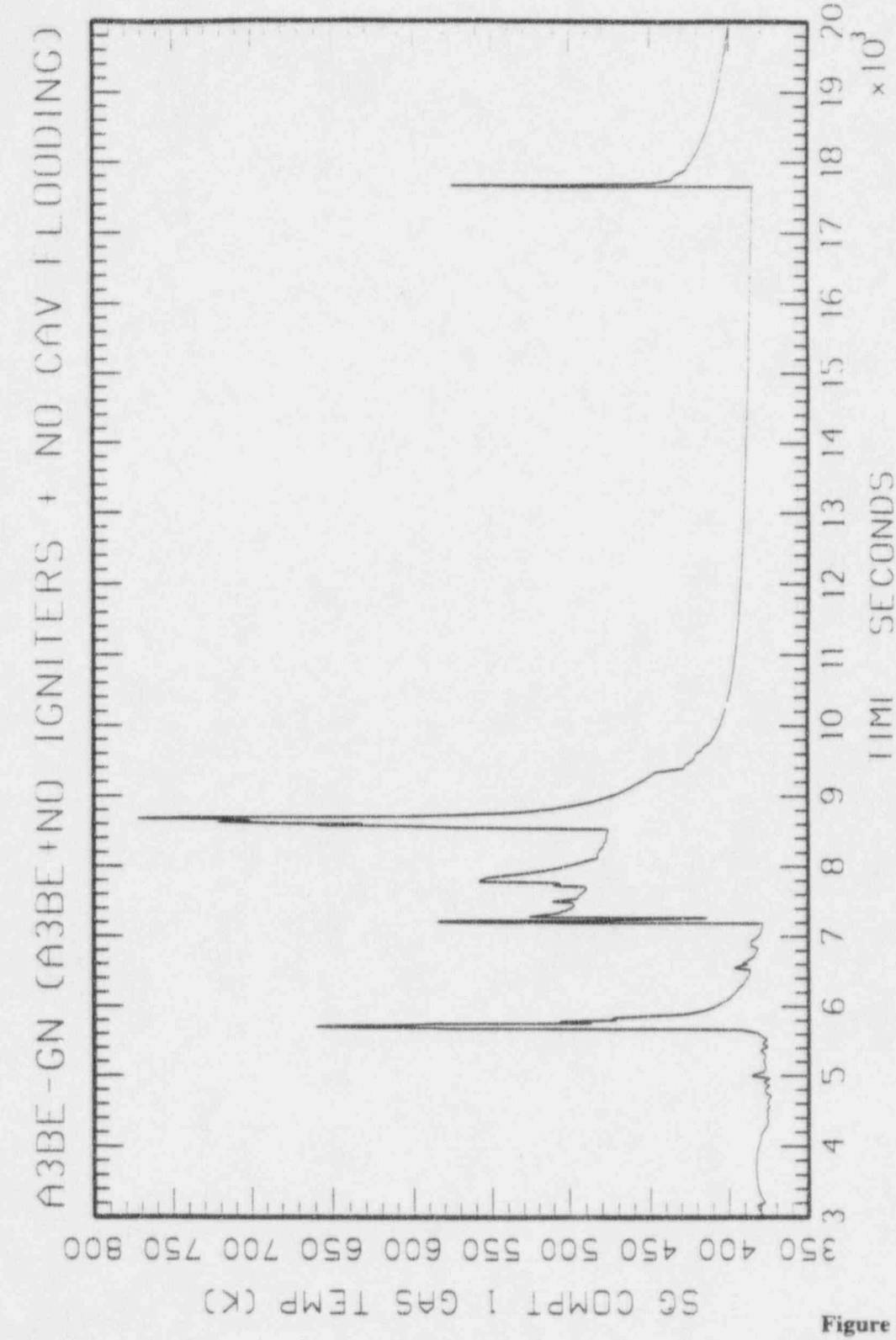



Figure D.7.1-25

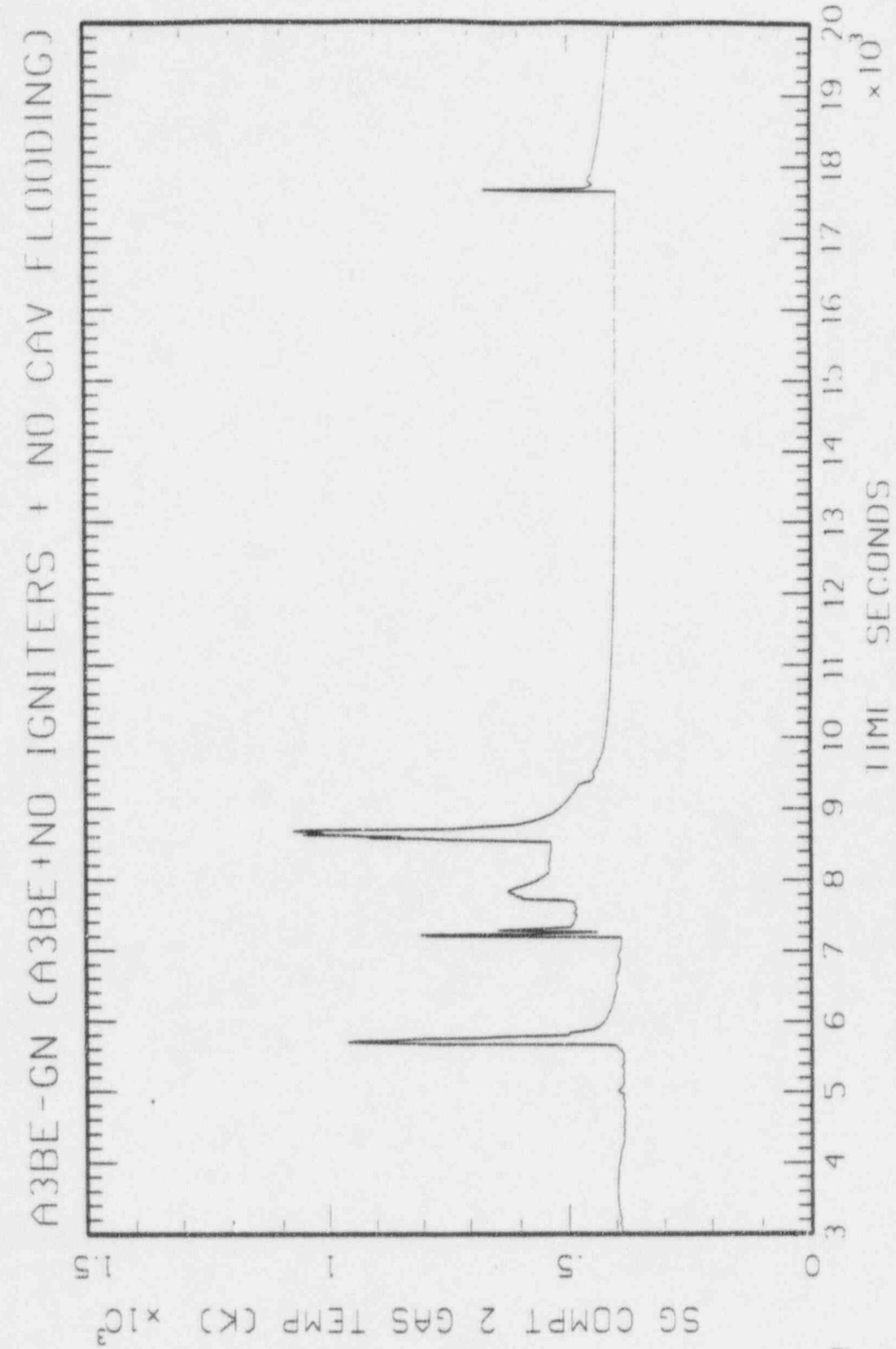



Figure D.7.1-26

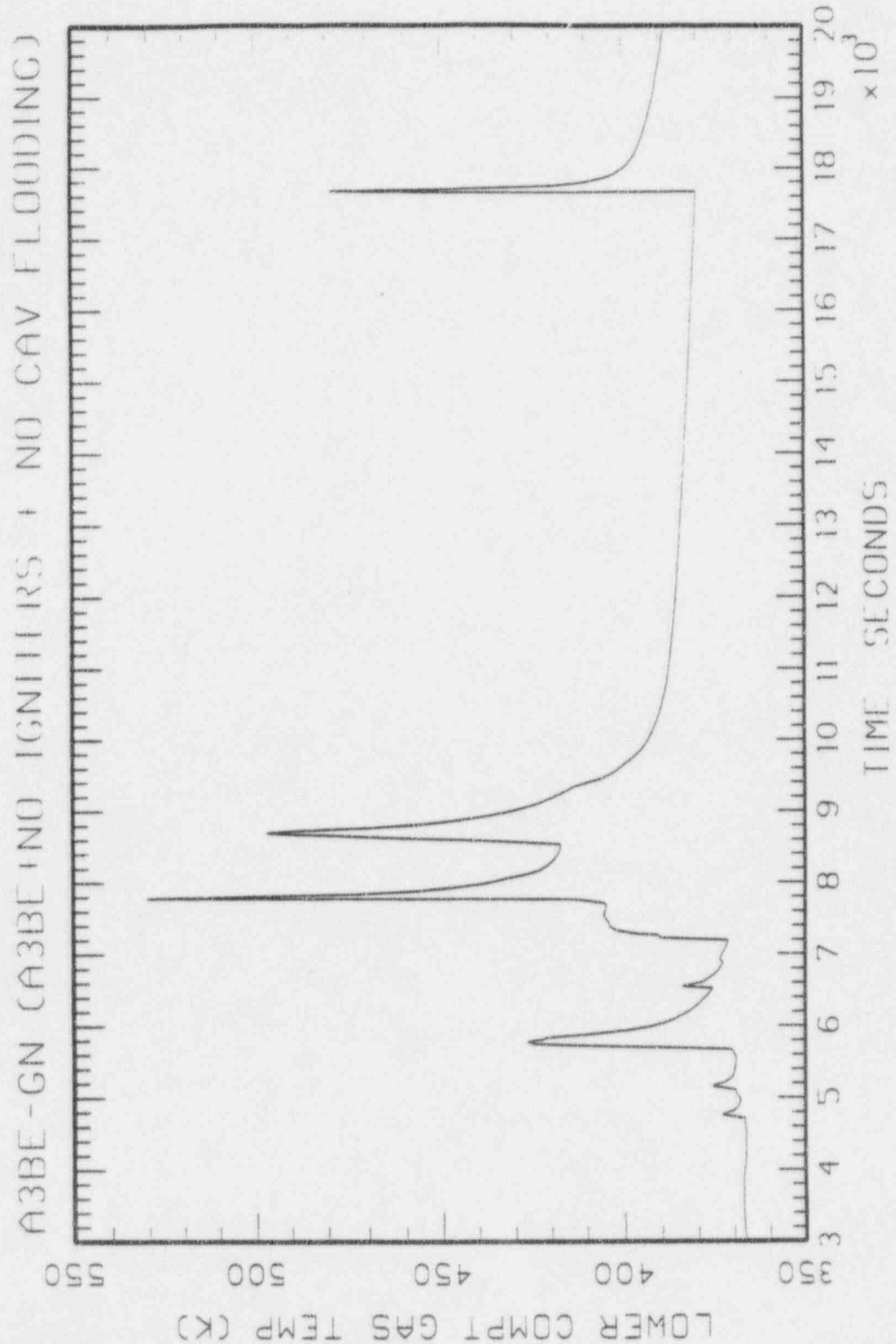



Figure D.7.1-27

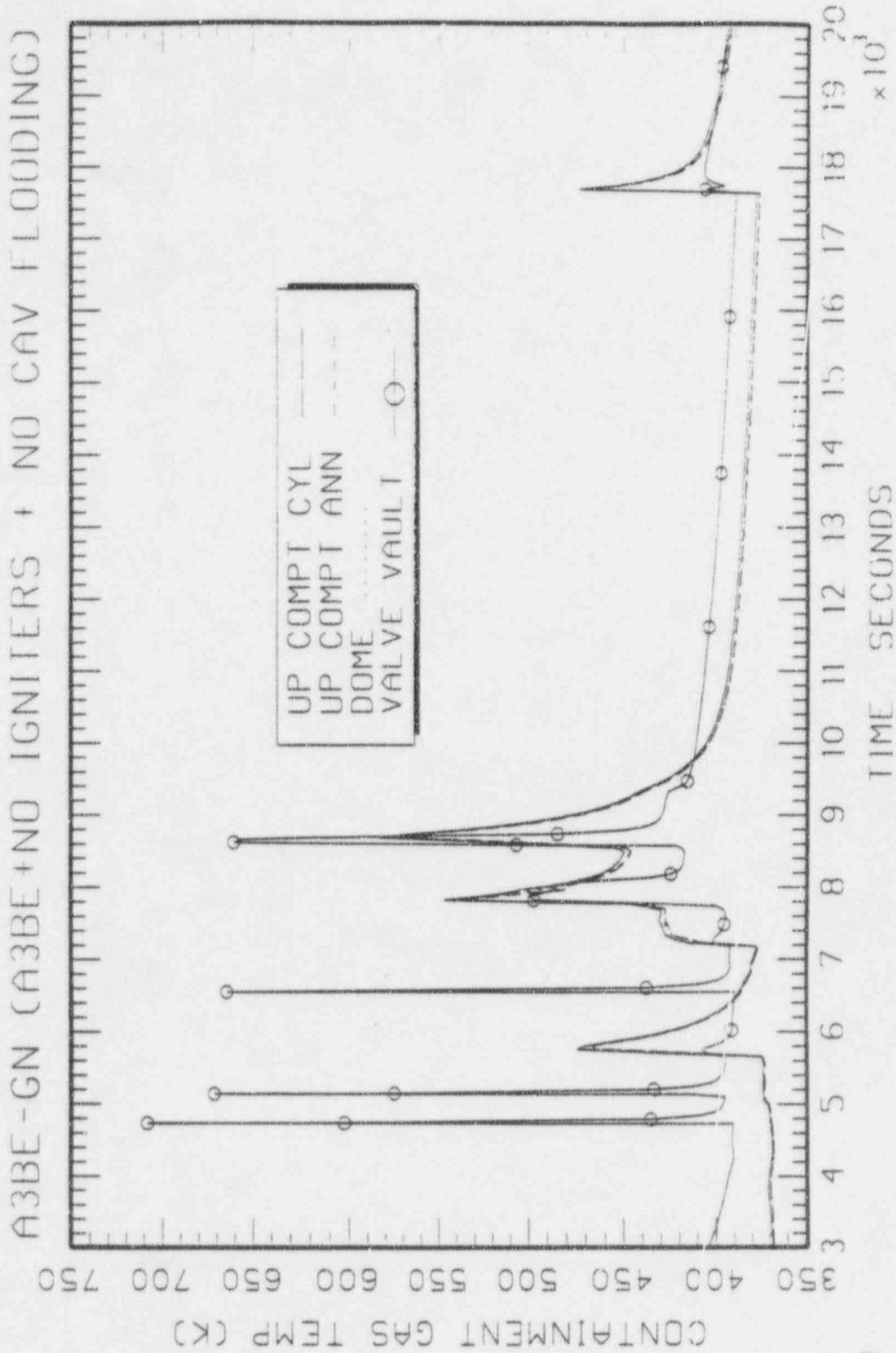



Figure D.7.1-28

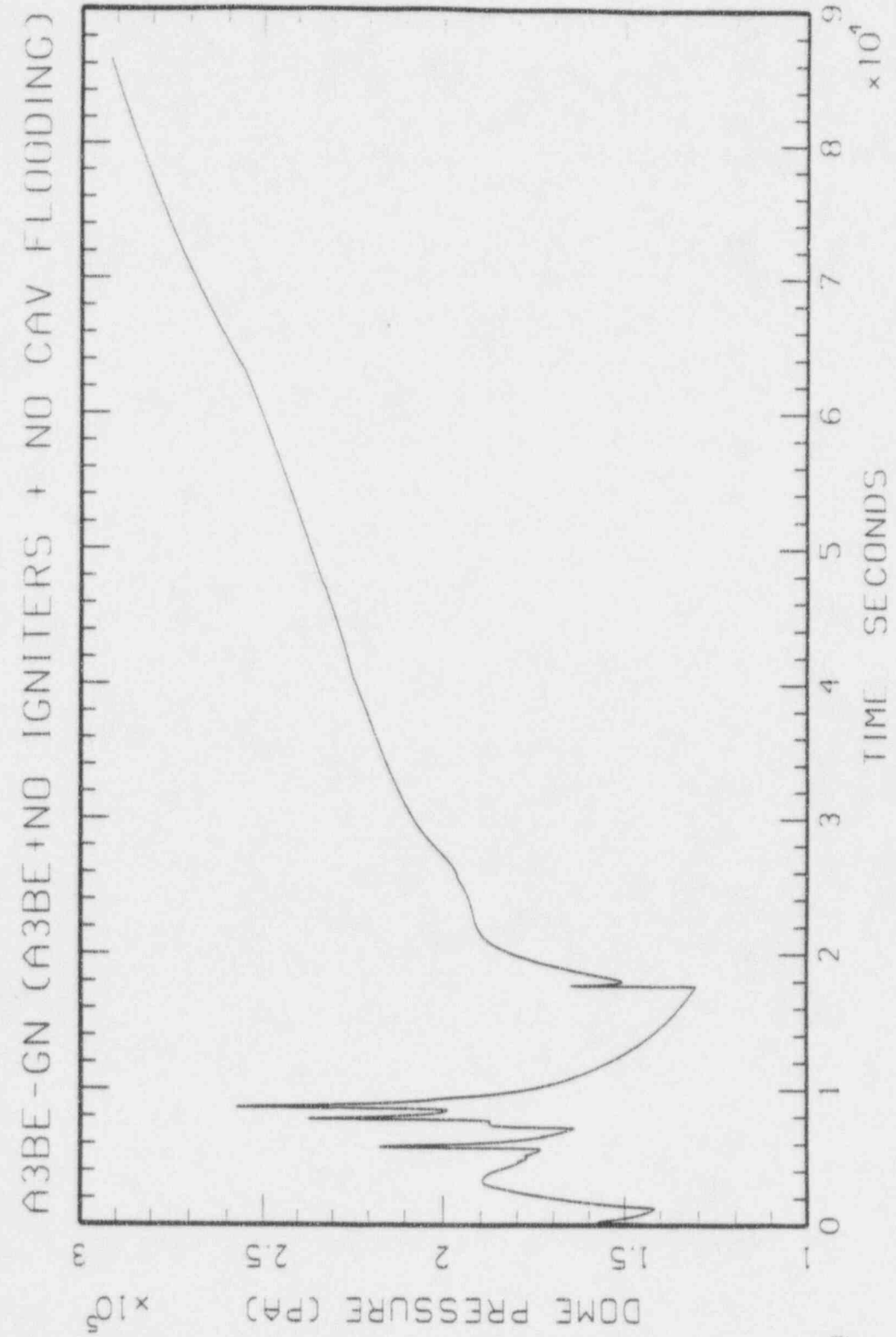



Figure D.7.1-29

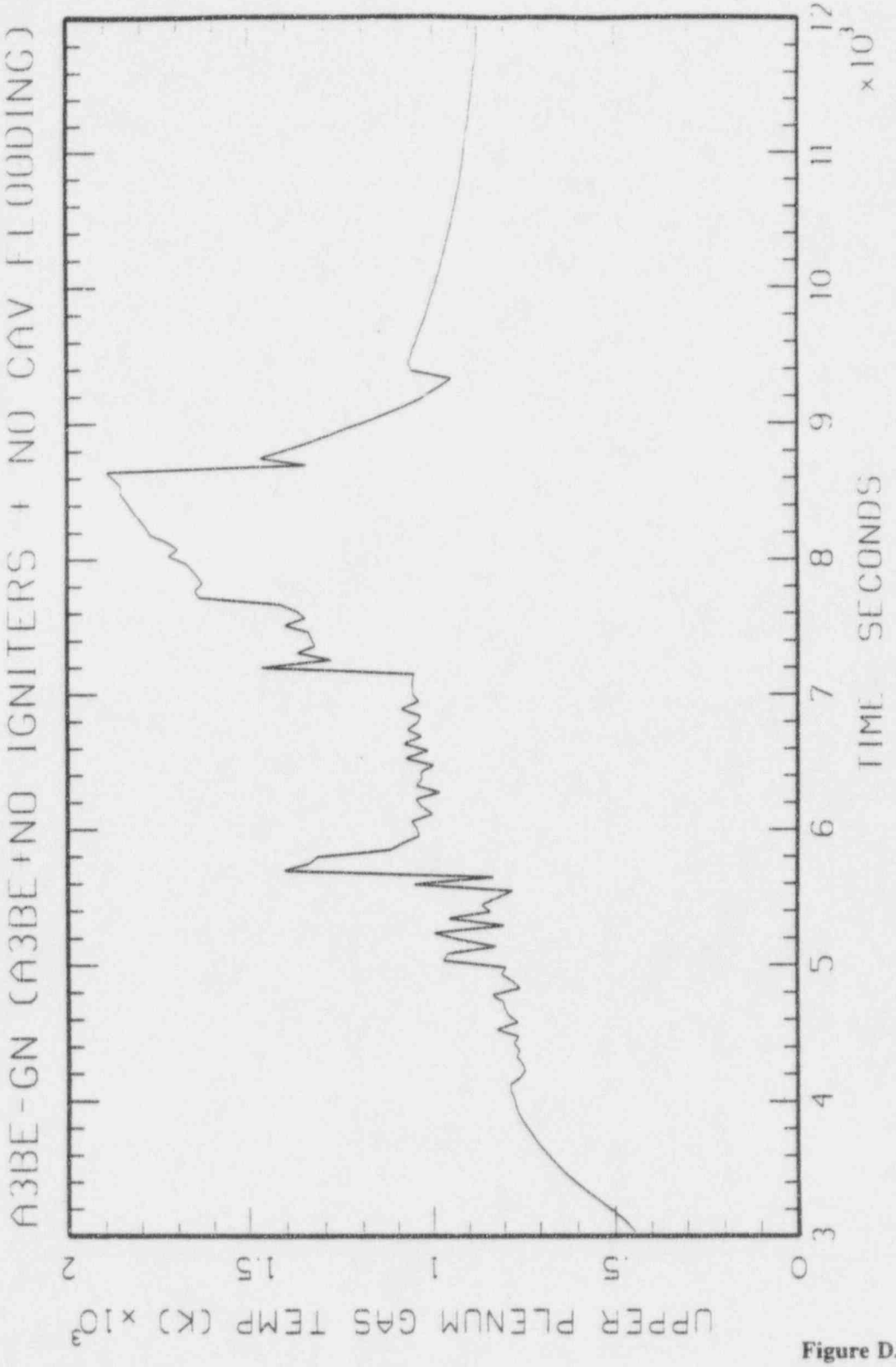



Figure D.7.1-30

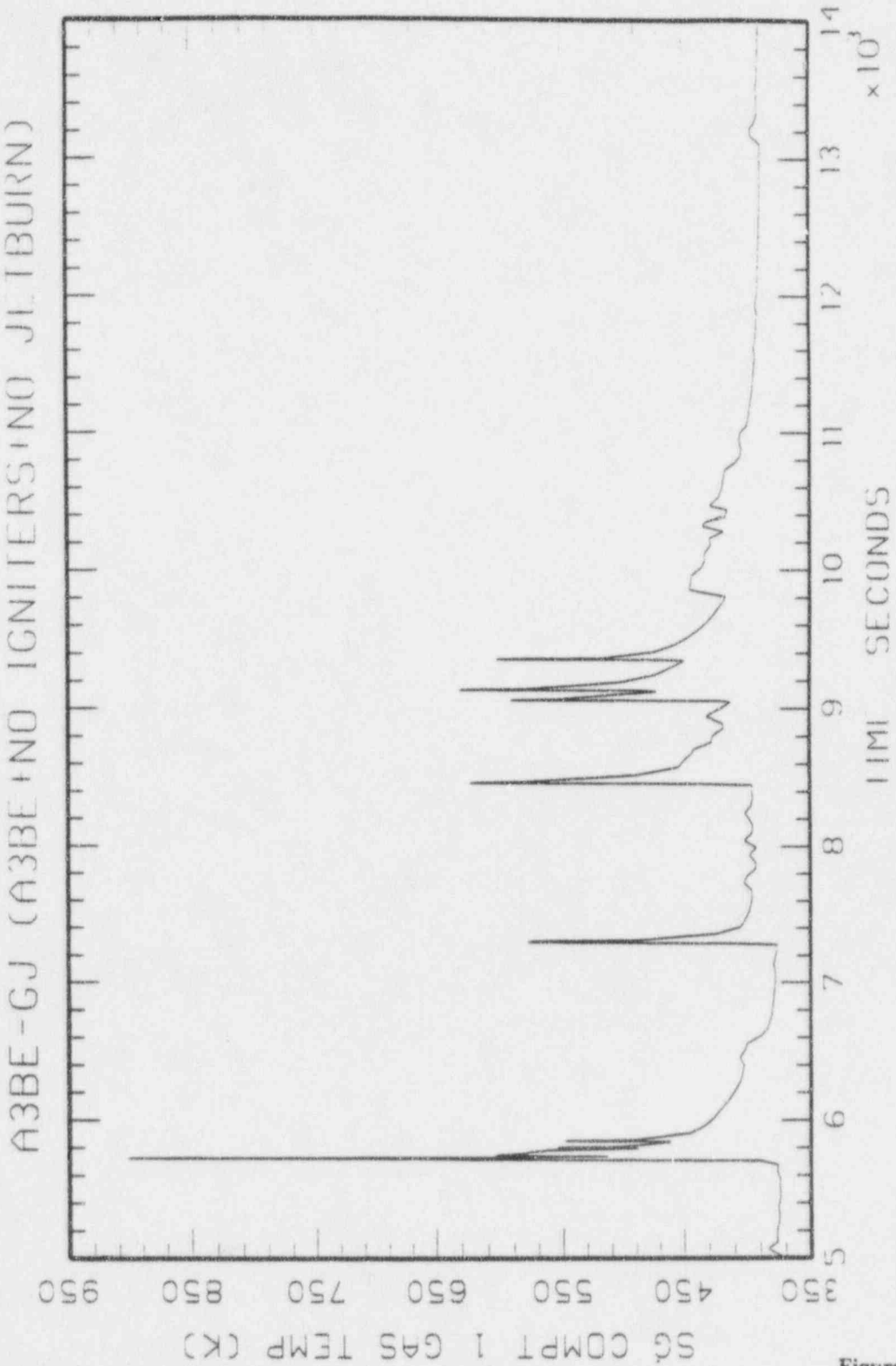



Figure D.7.1-31

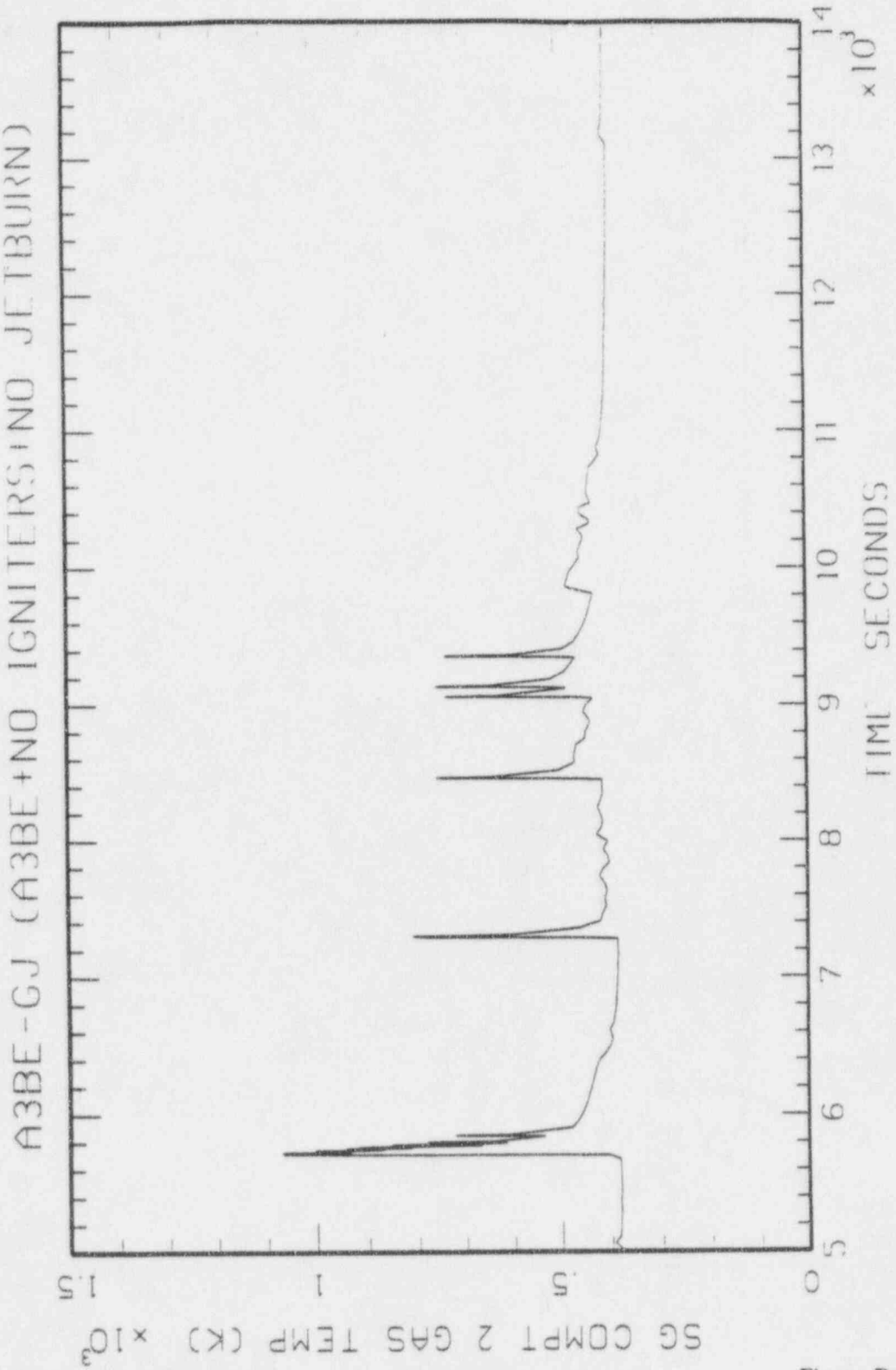



Figure D.7.1-32

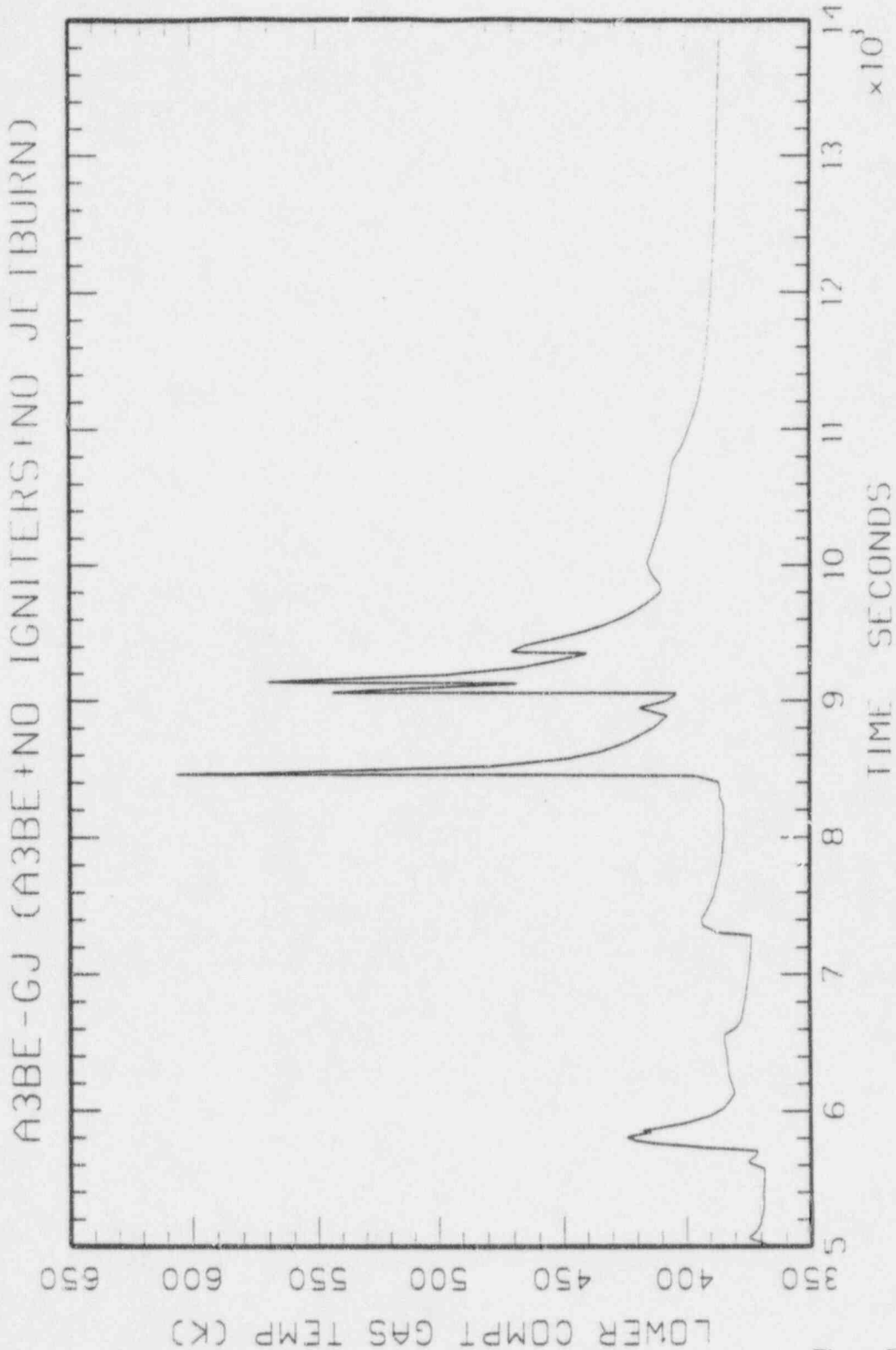



Figure D.7.1-33

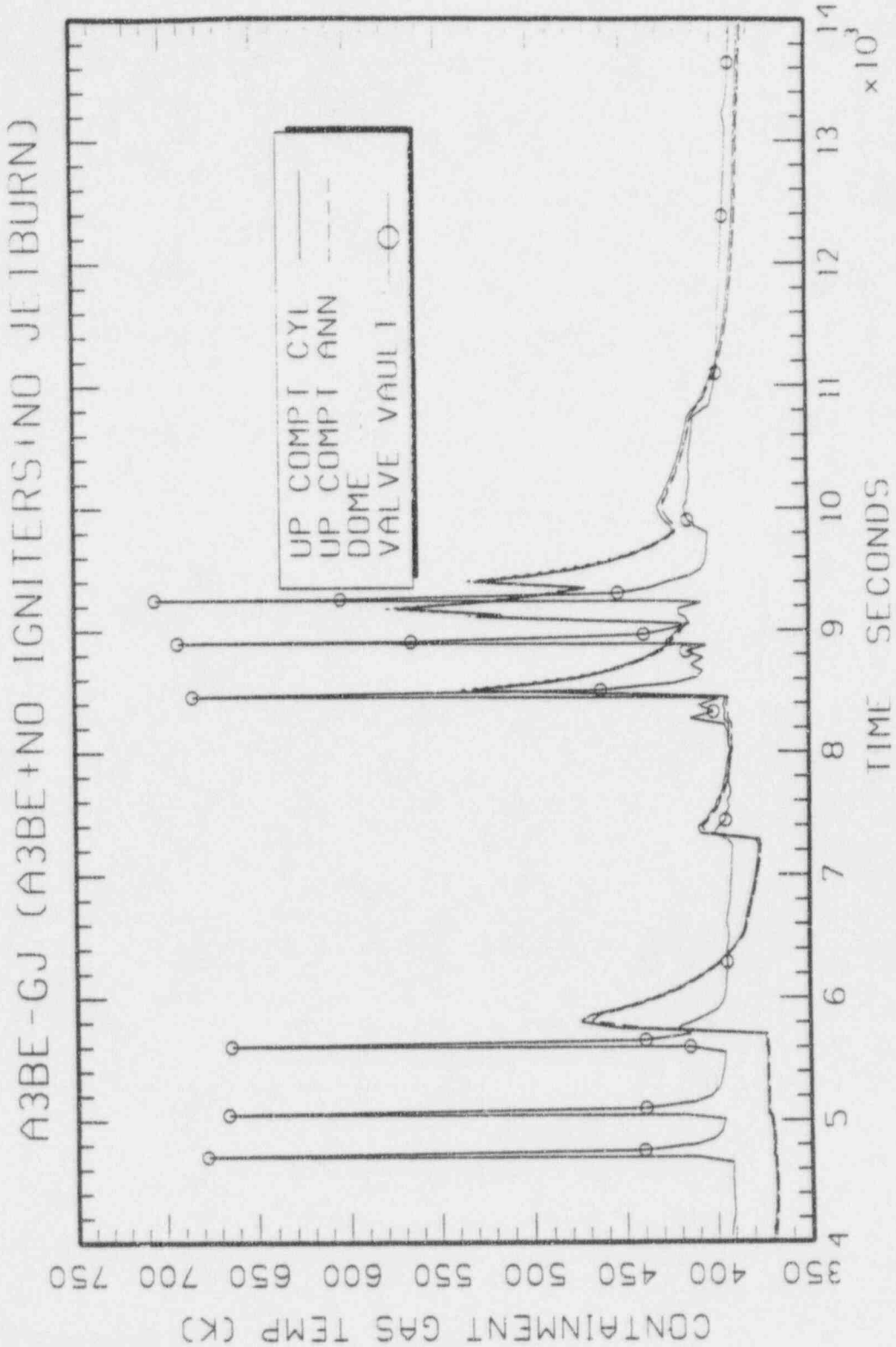



Figure D.7.1-34

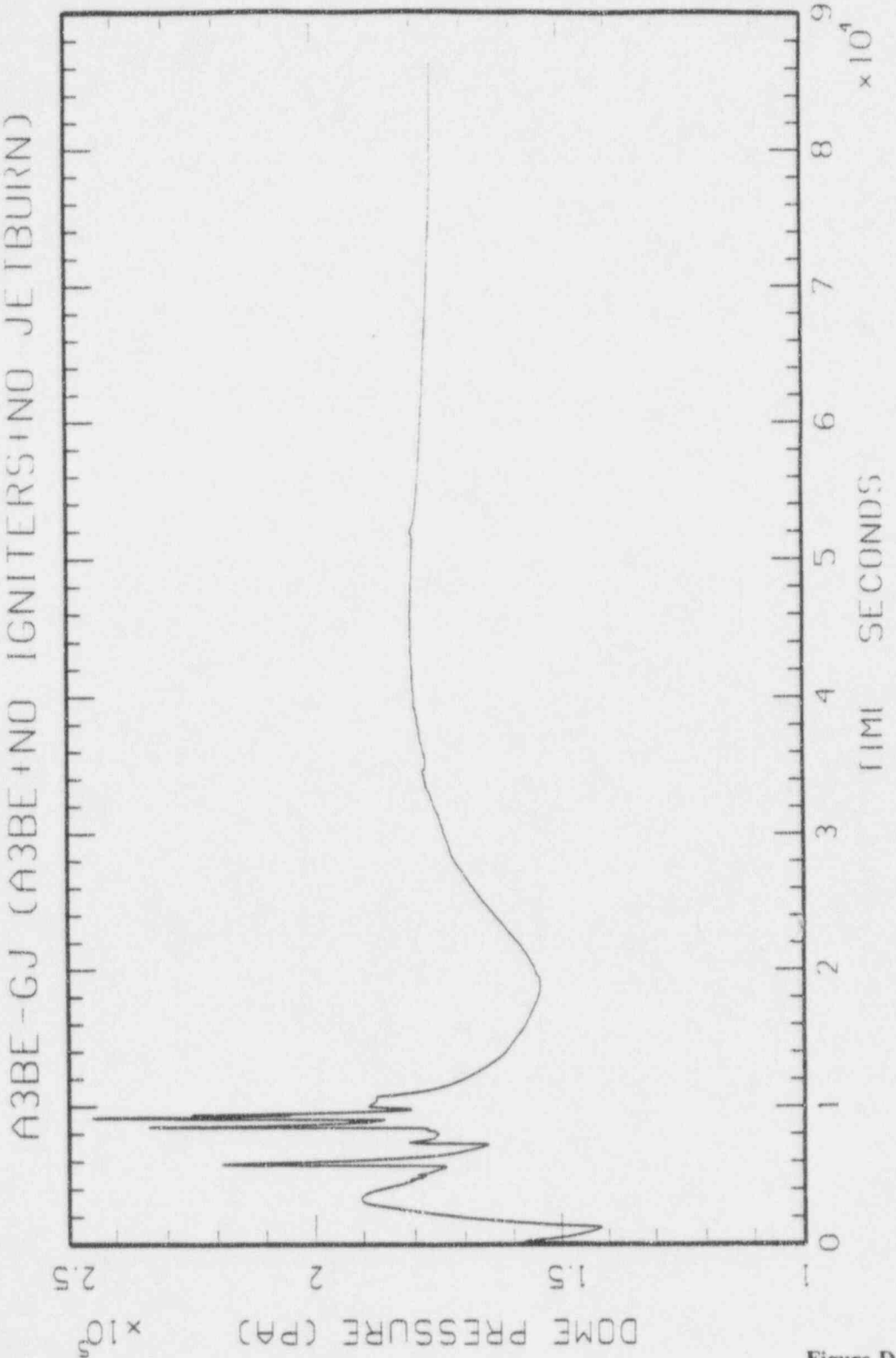



Figure D.7.1-35

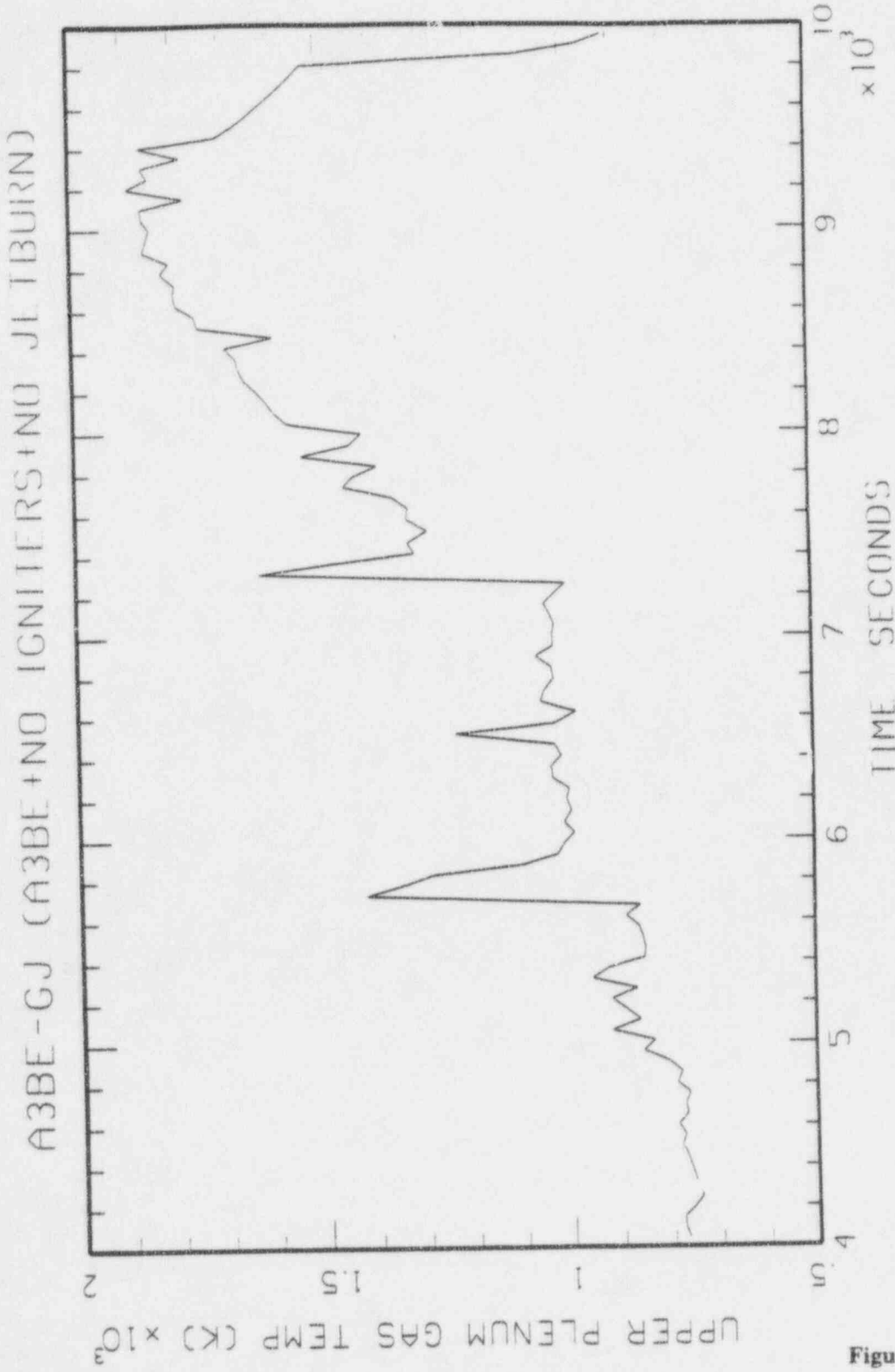



**Figure D.7.1-36**

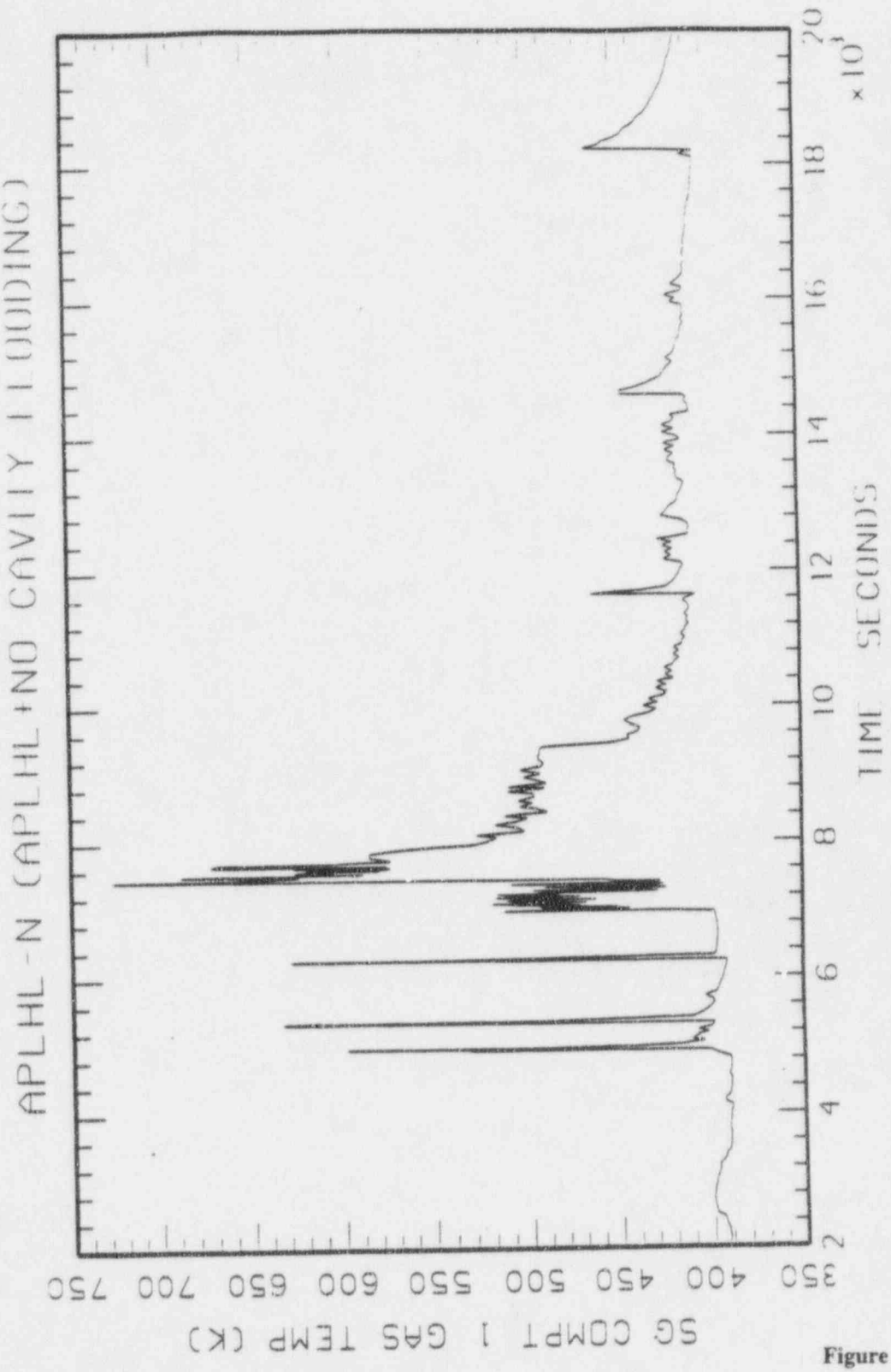



Figure D.7.1-37

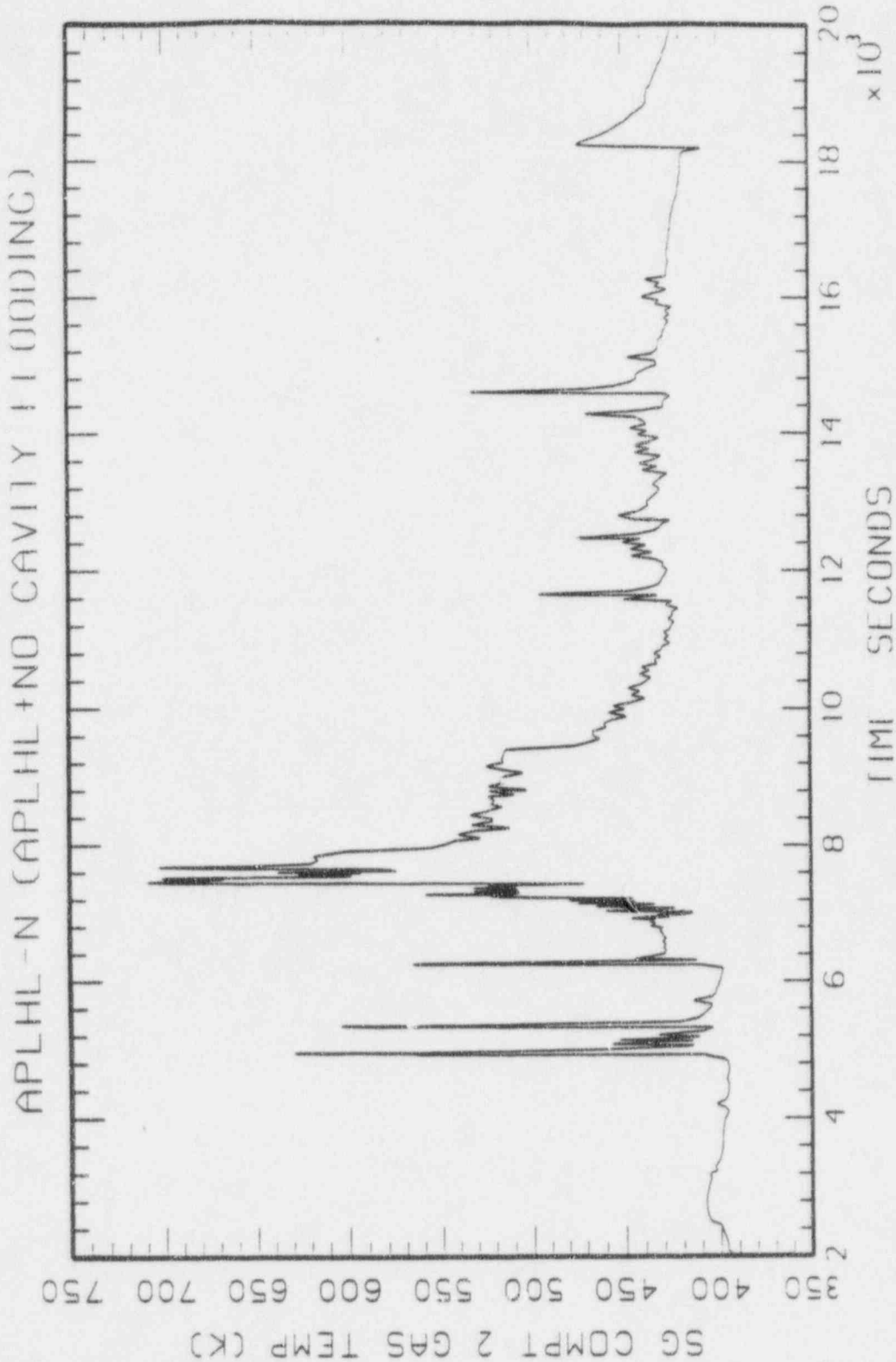



**Figure D.7.1-38**

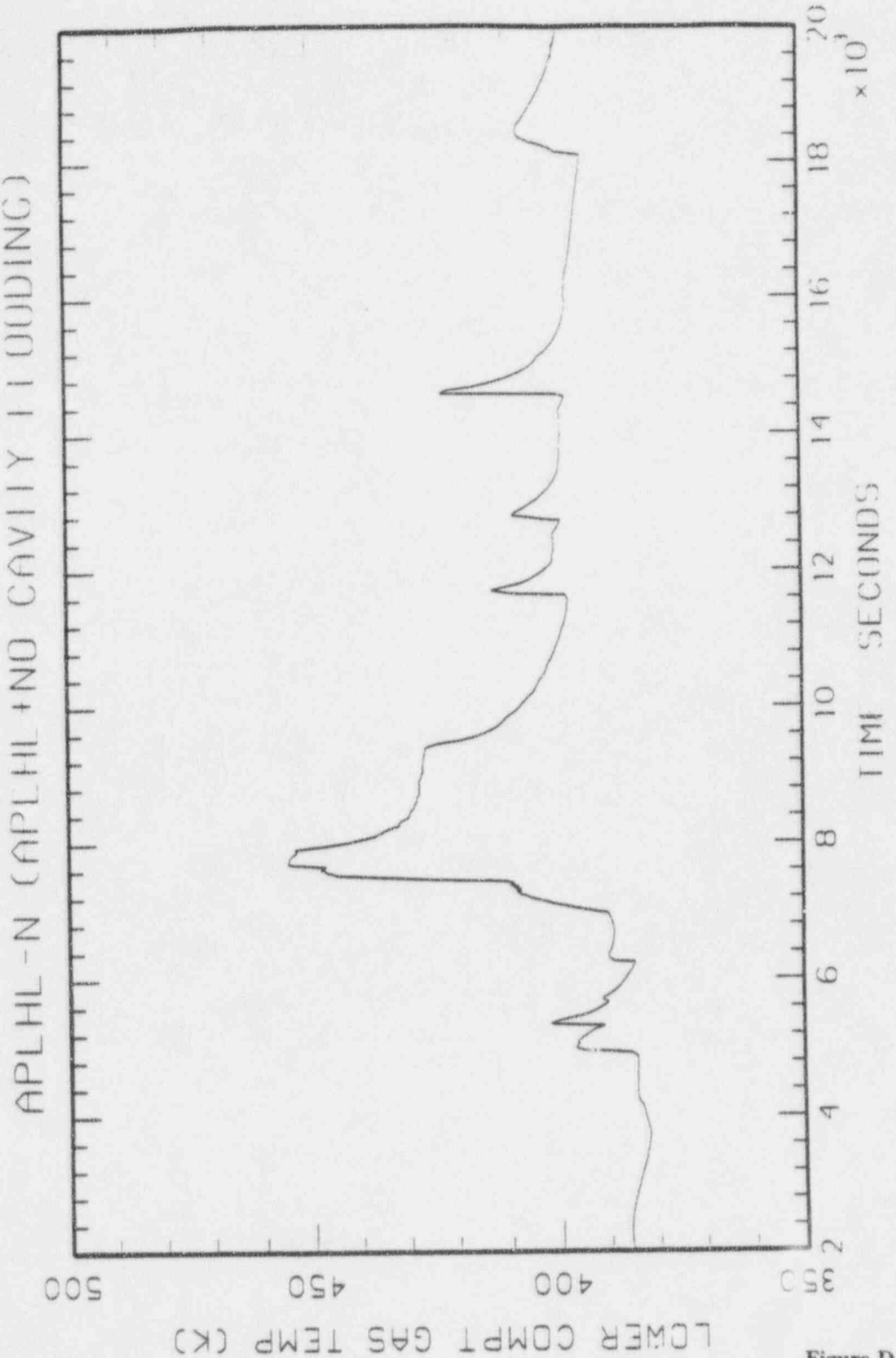



Figure D.7.1-39

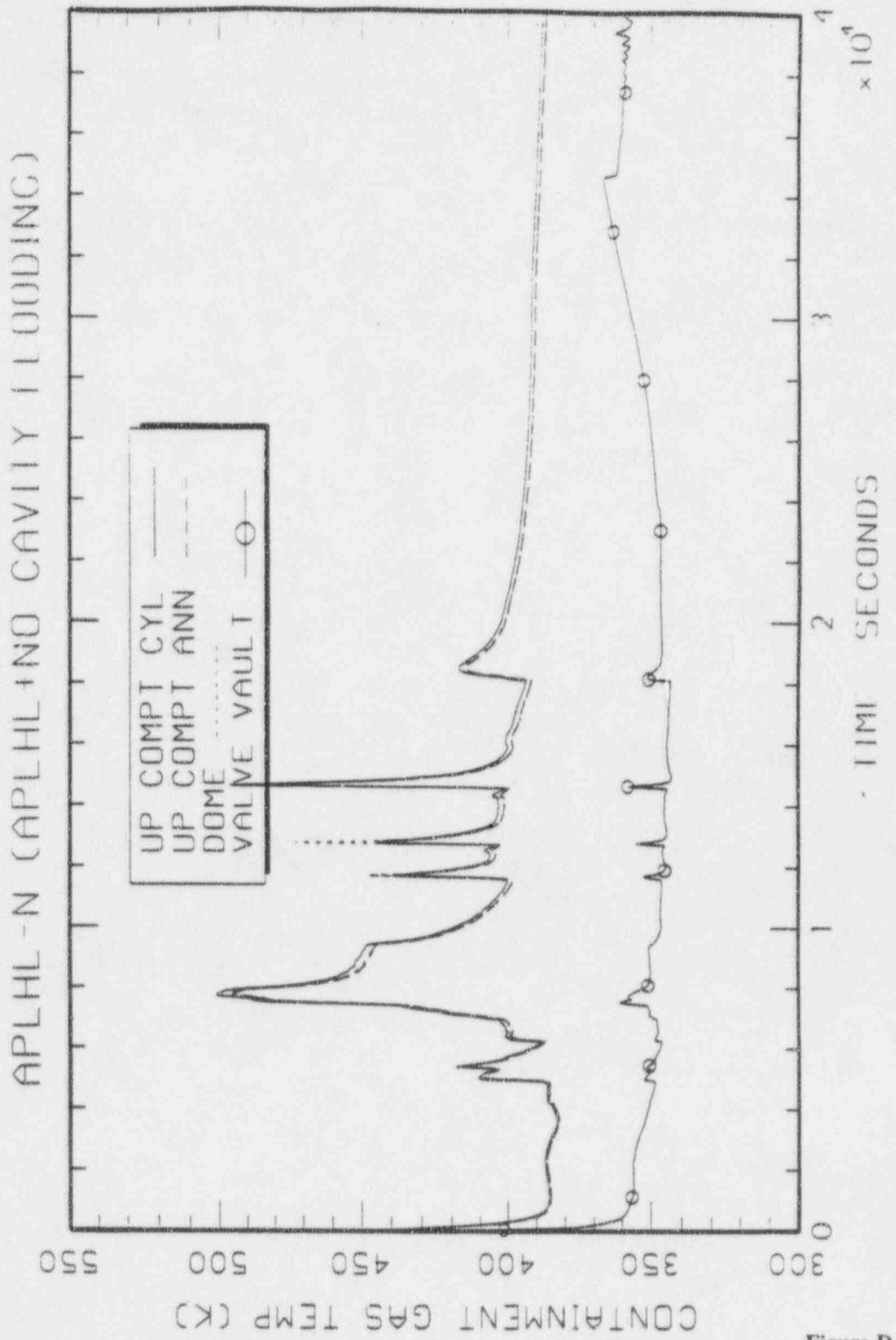



Figure D.7.1-40

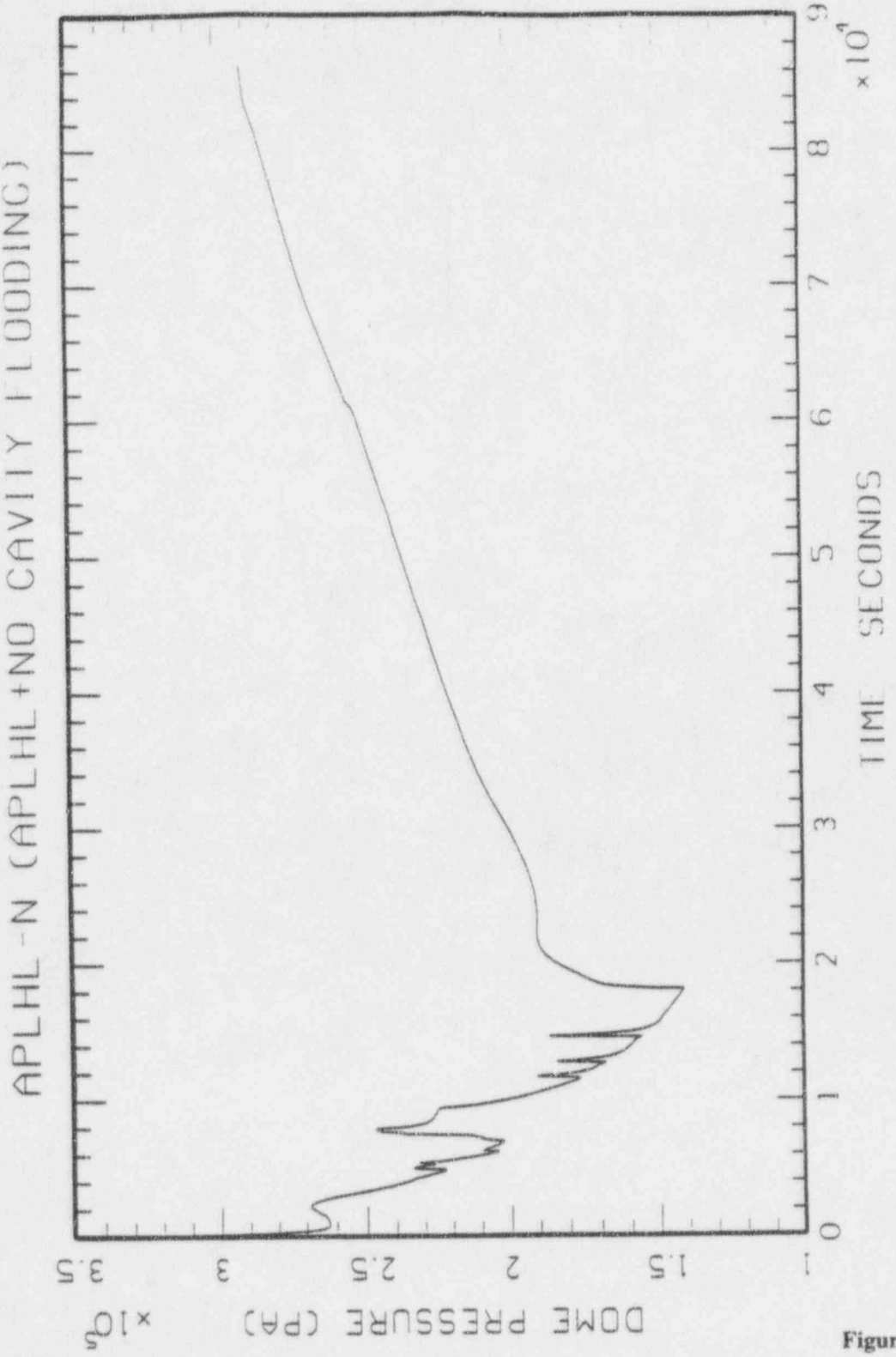



Figure D.7.1-41

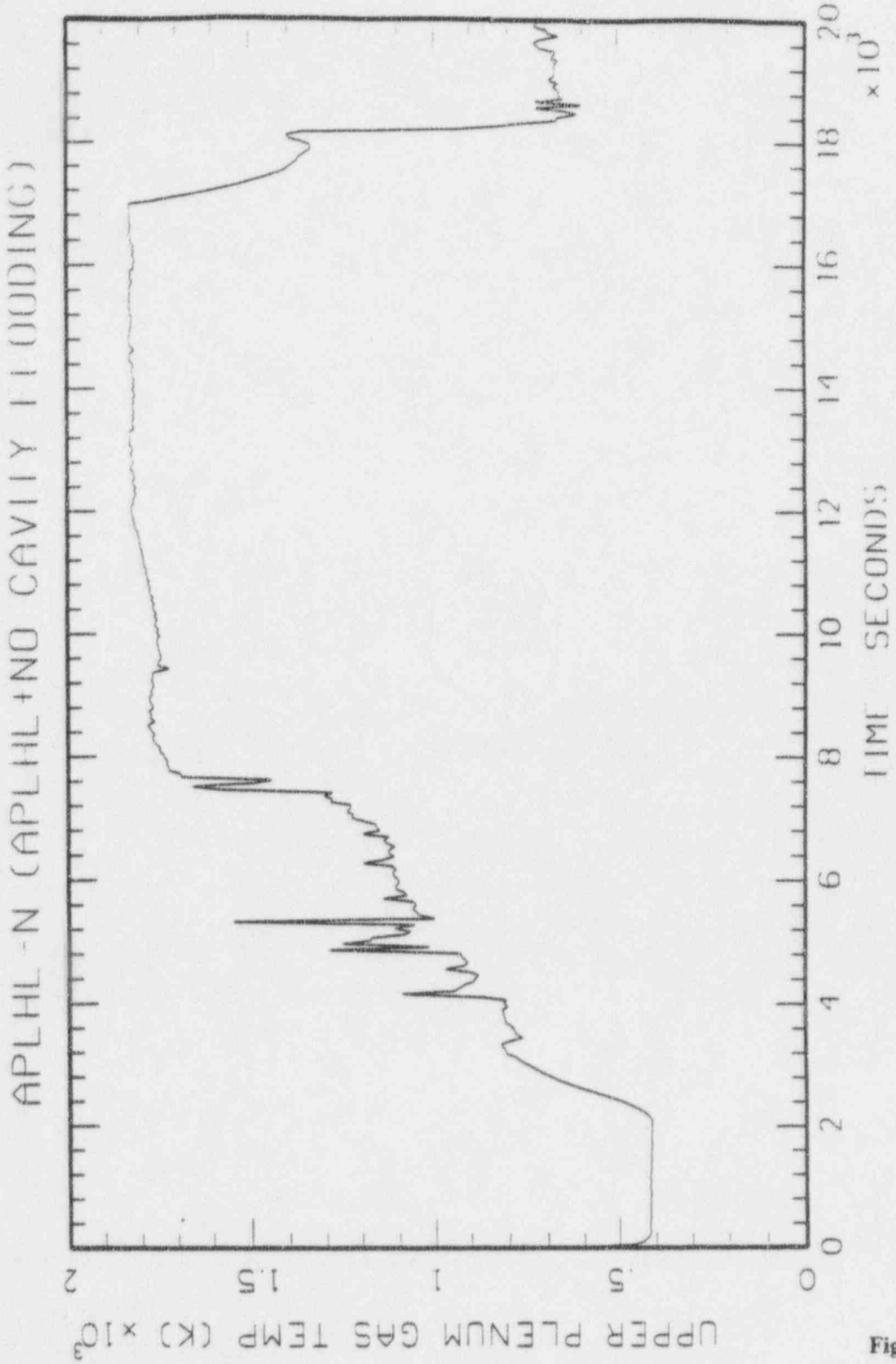



Figure D.7.1-42

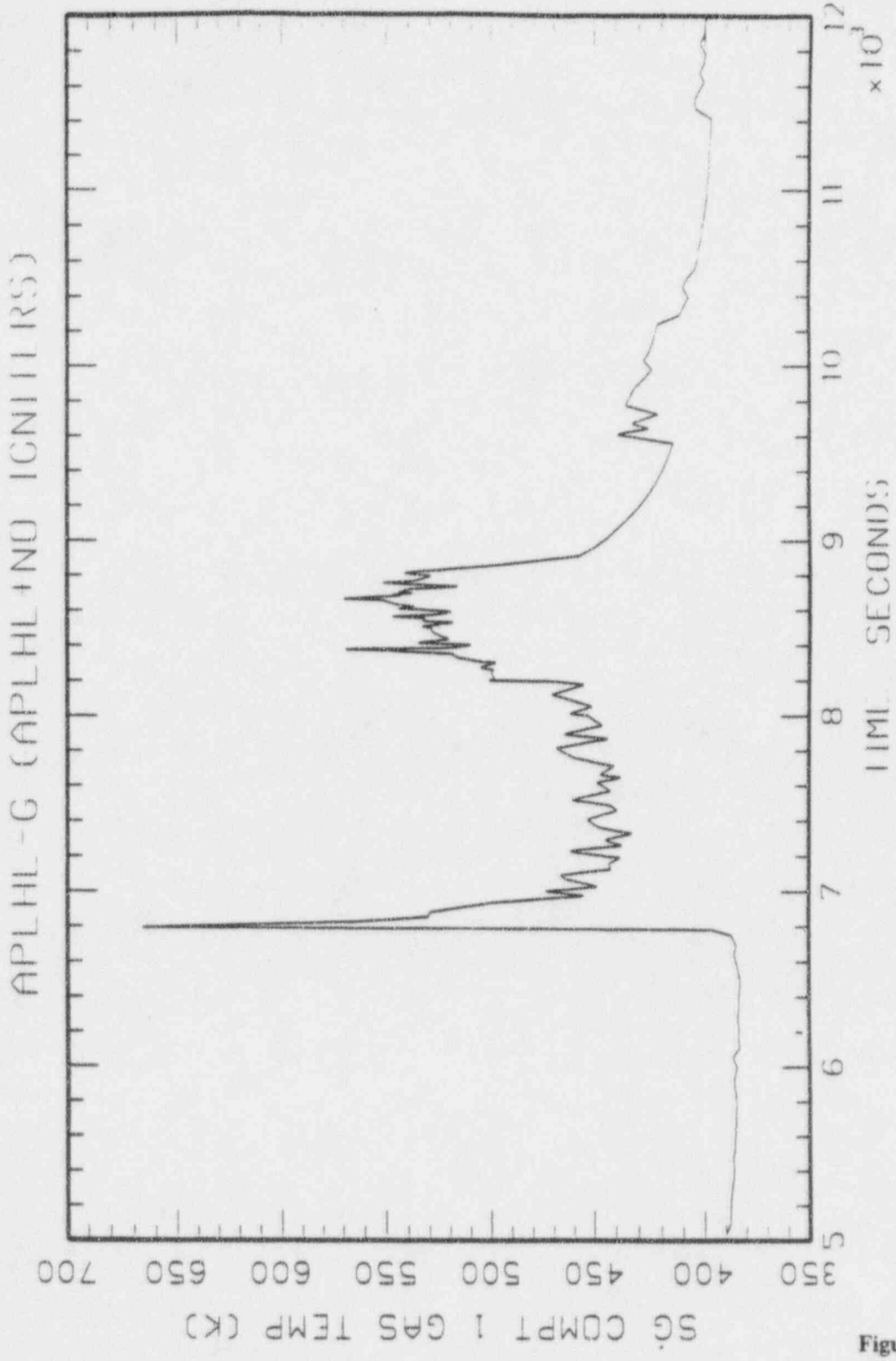



Figure D.7.1-43

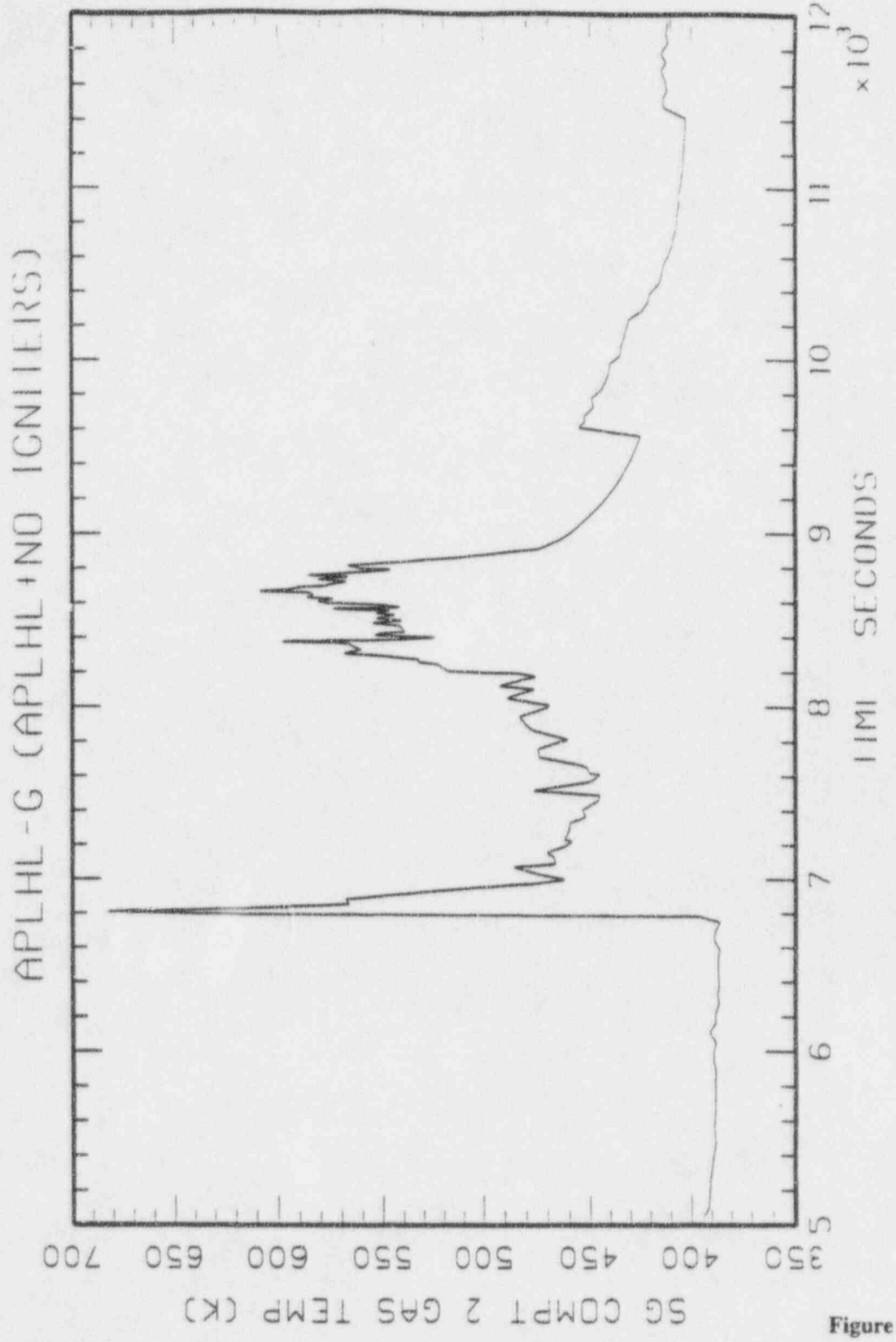



Figure D.7.1-44

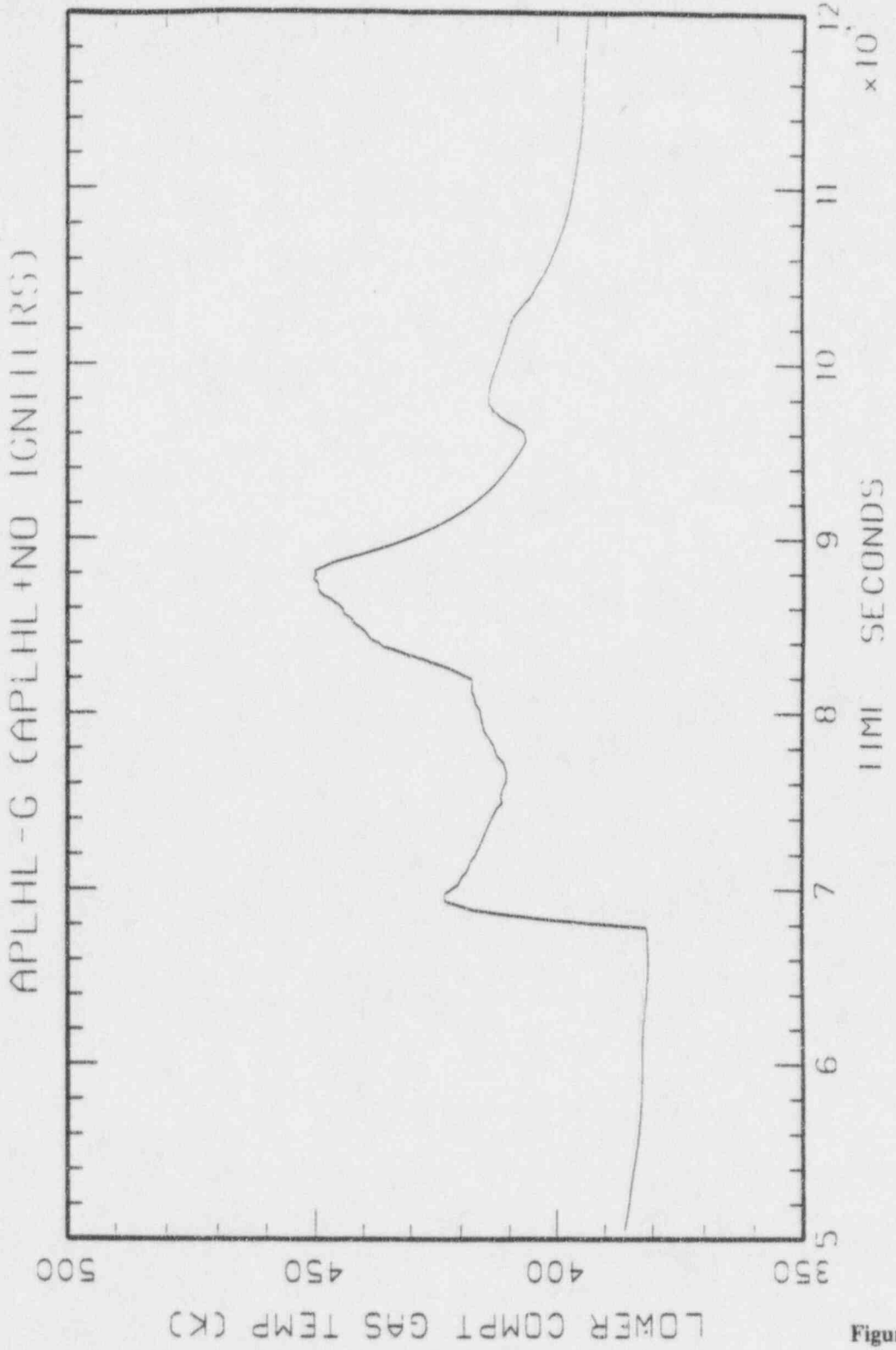



Figure D.7.1-45

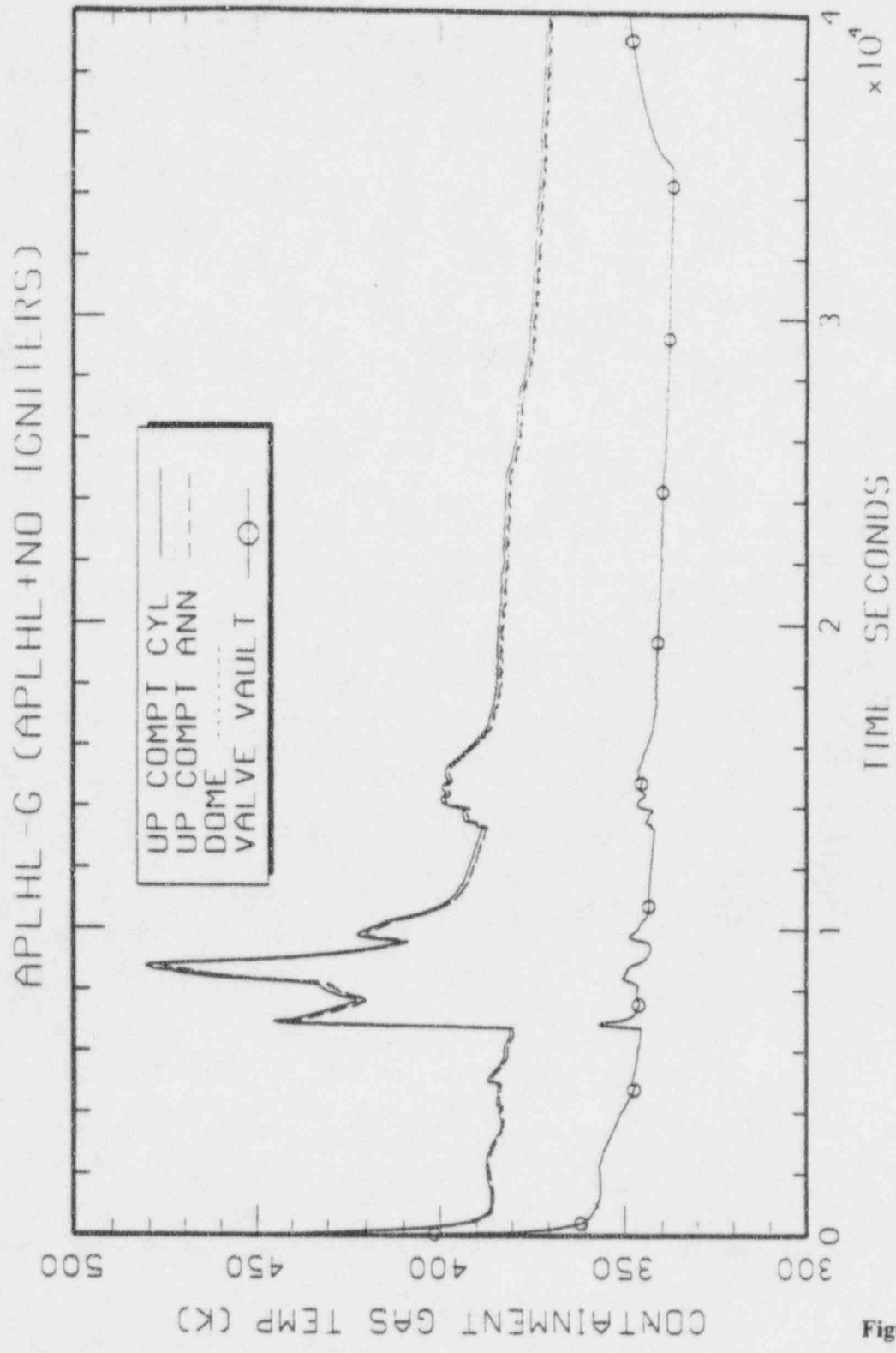



Figure D.7.1-46

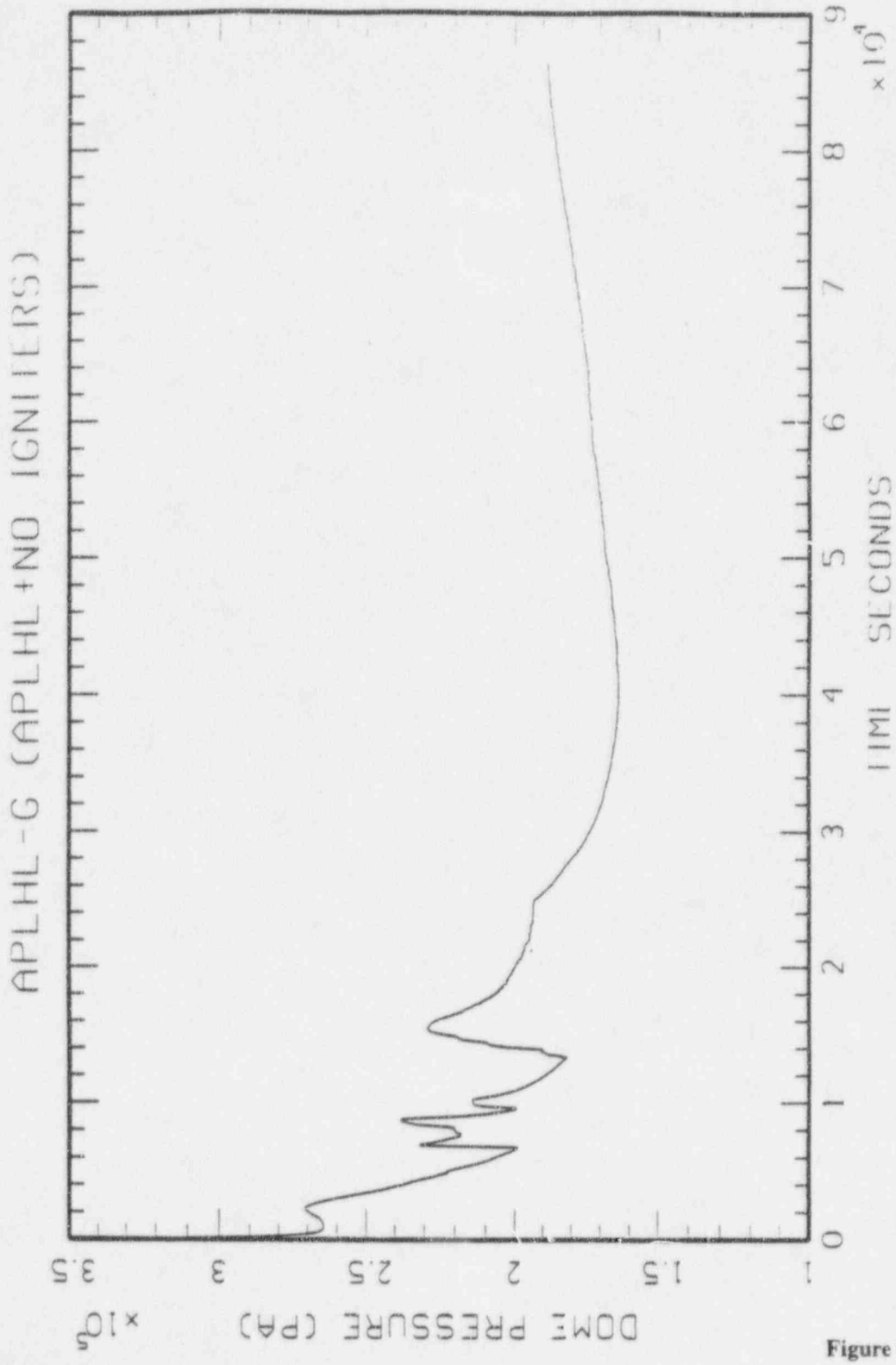



Figure D.7.1-47

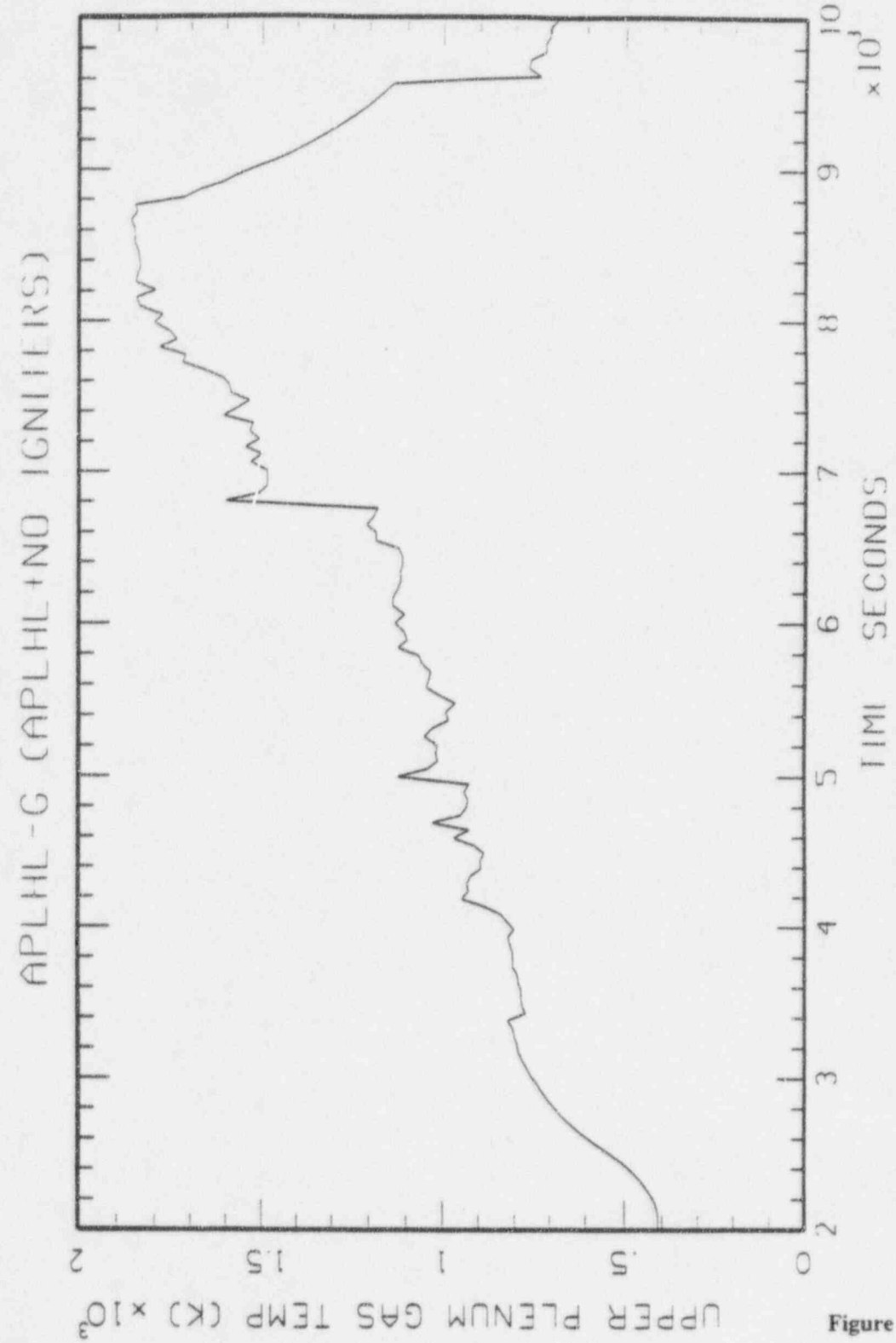



Figure D.7.1-48

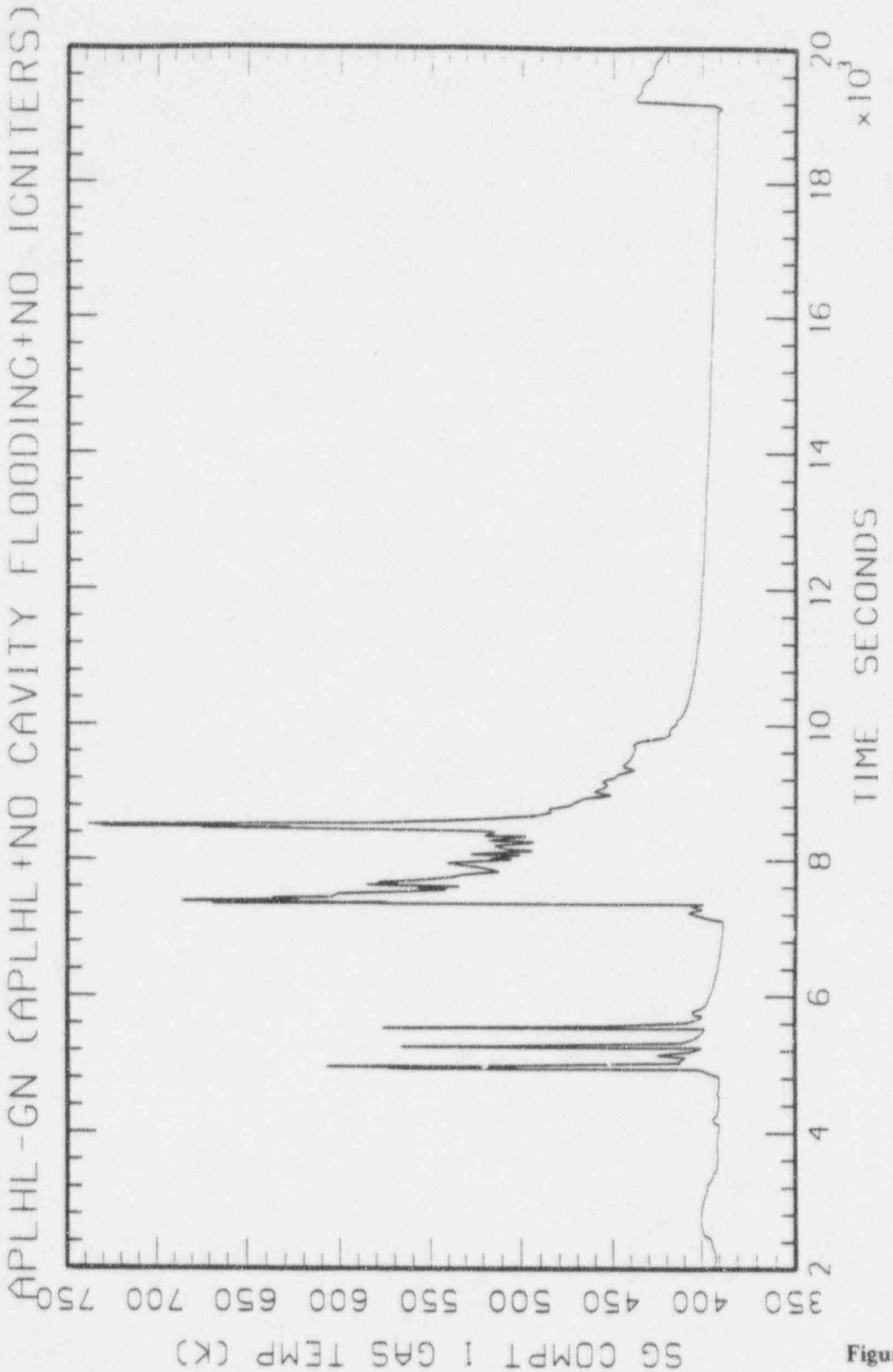



Figure D.7.1-49

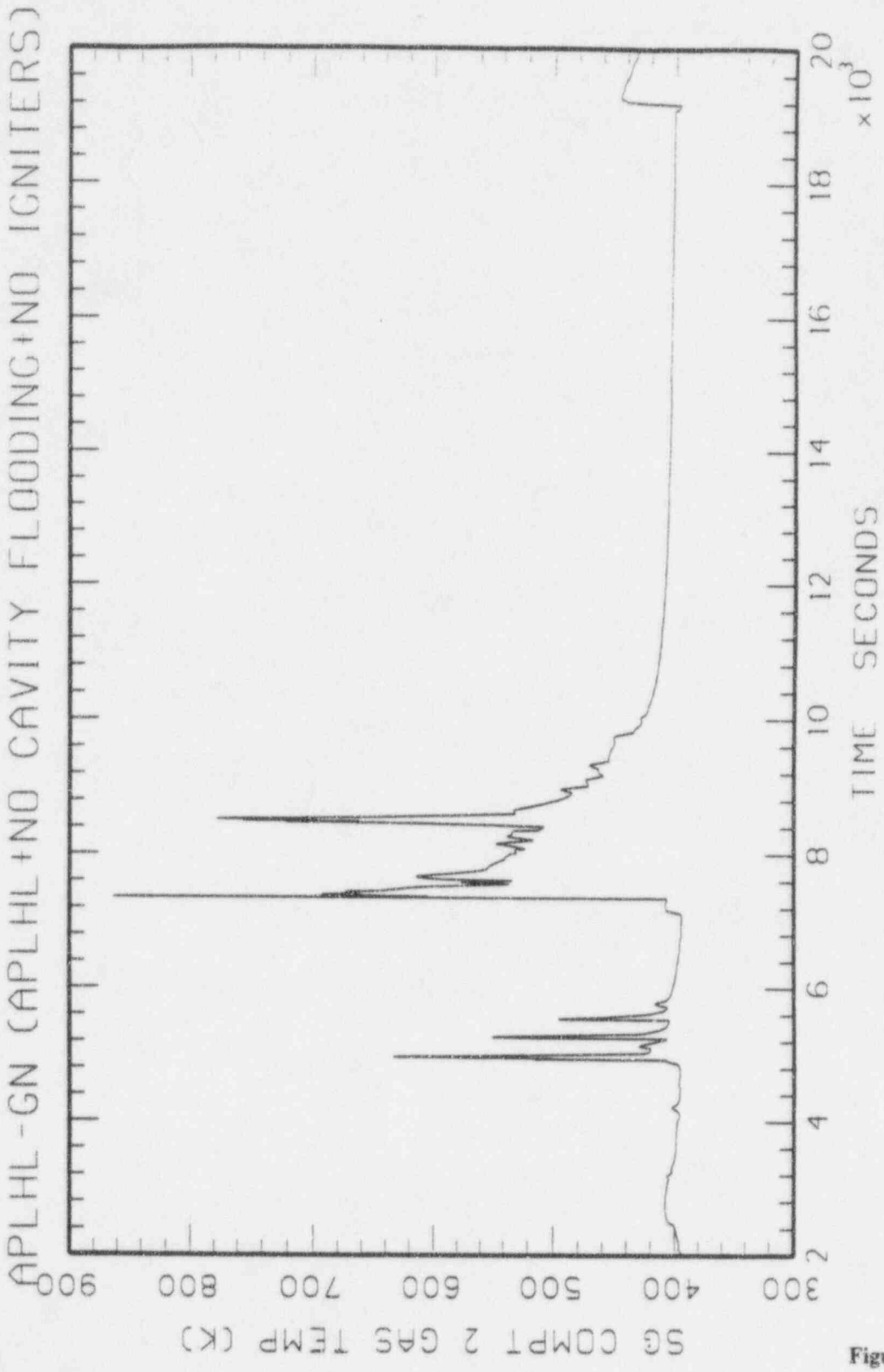



Figure D.7.1-50

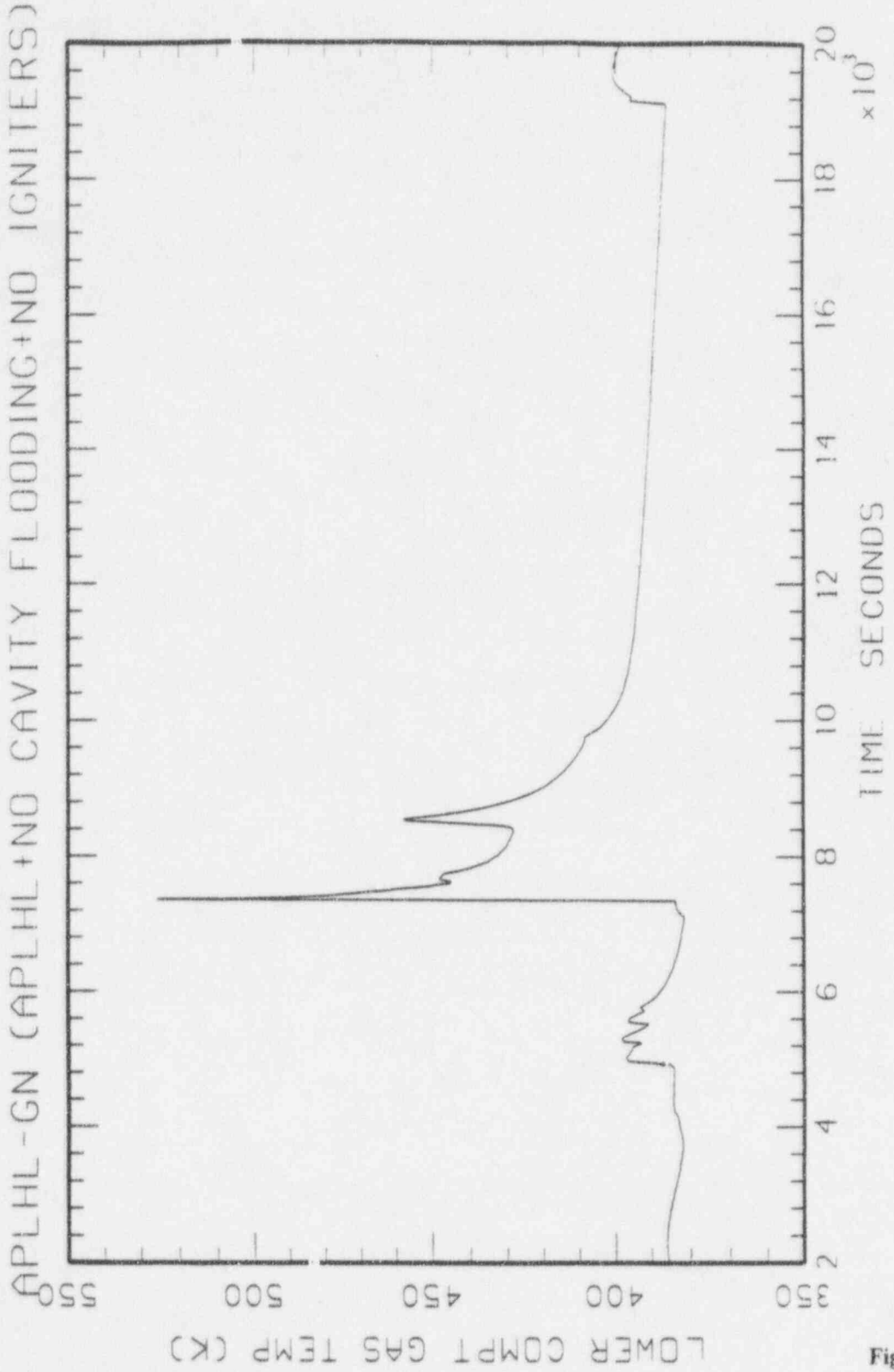



Figure D.7.1-51

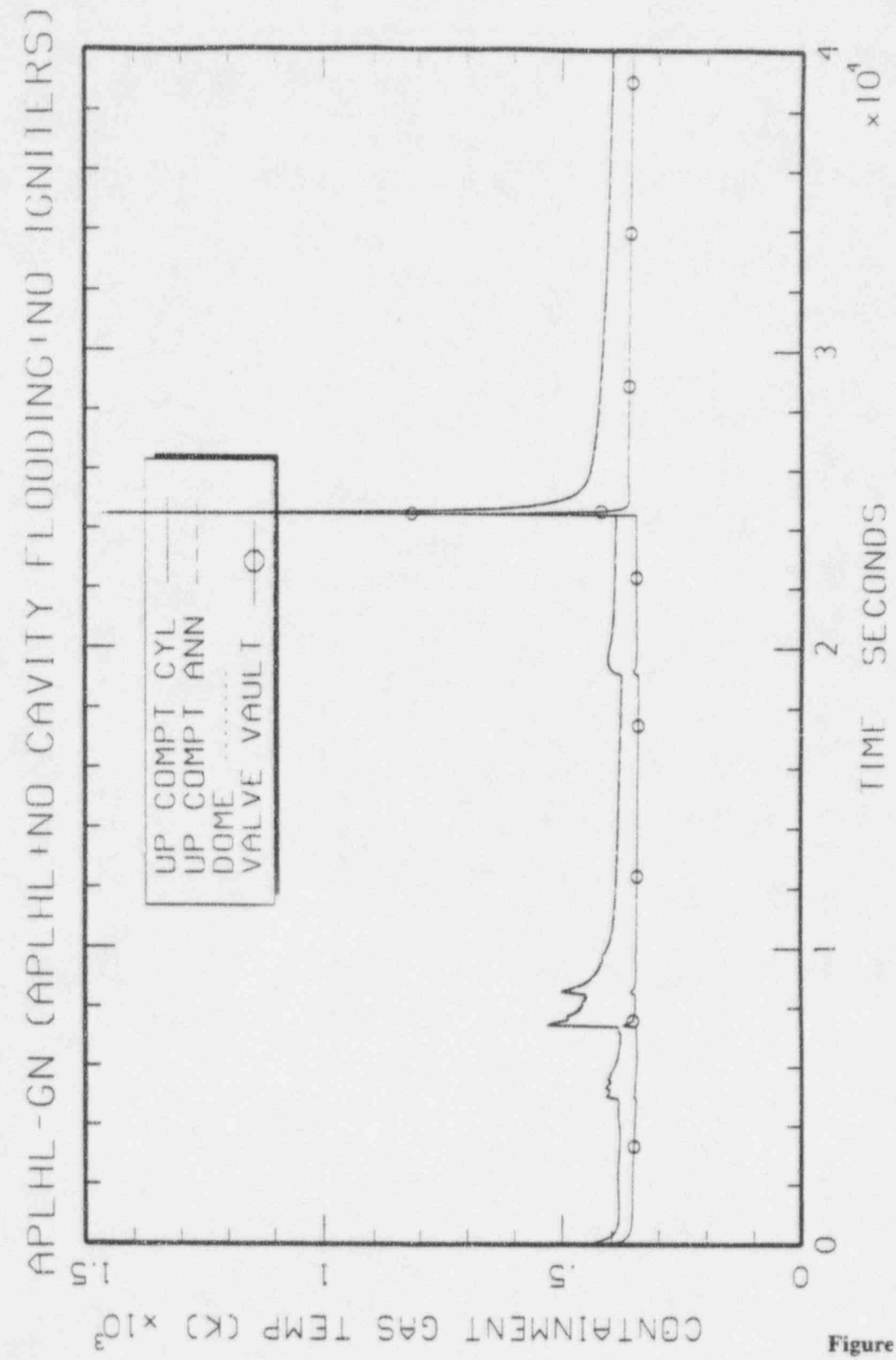



Figure D.7.1-52

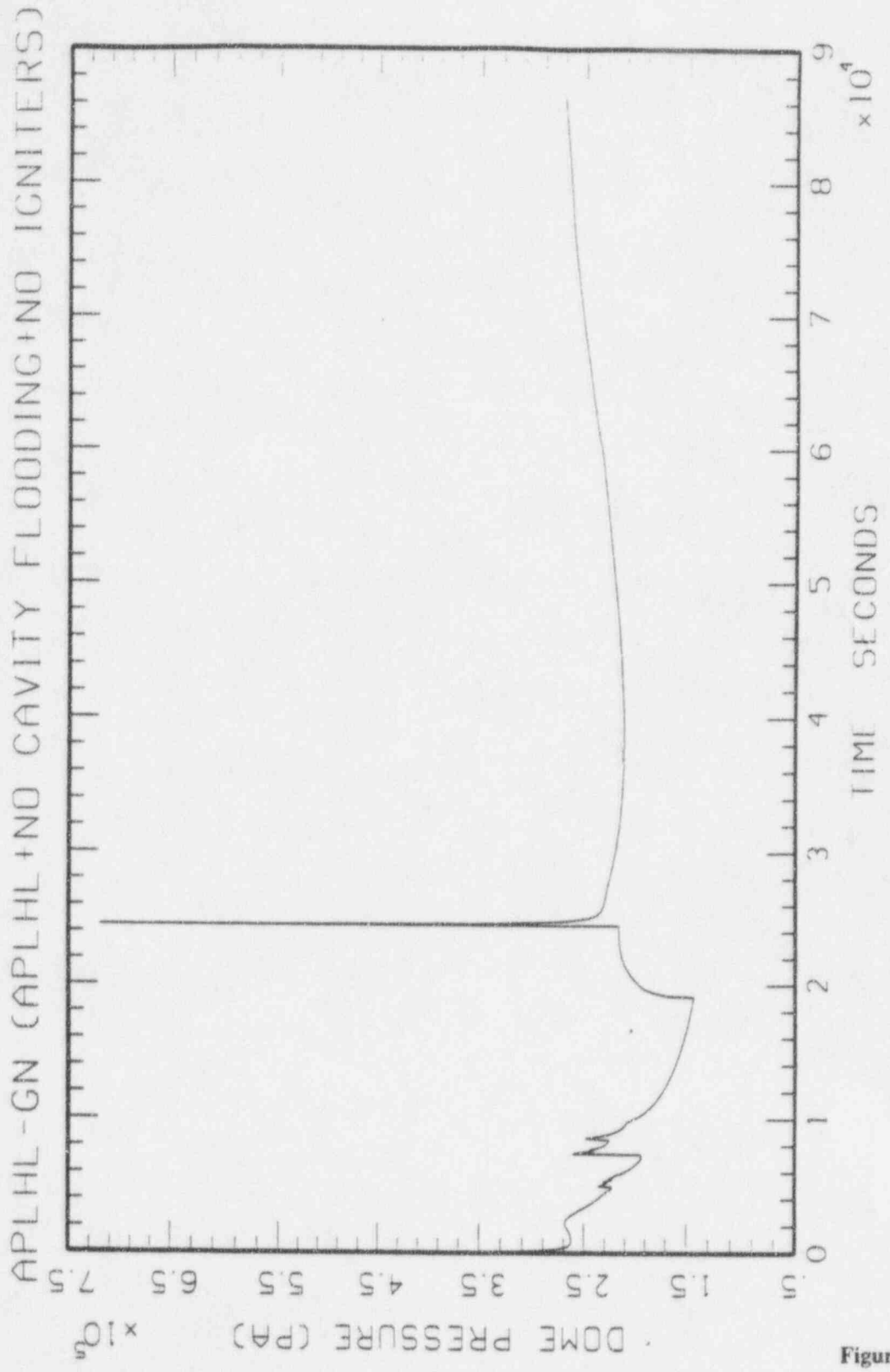



Figure D.7.1-53

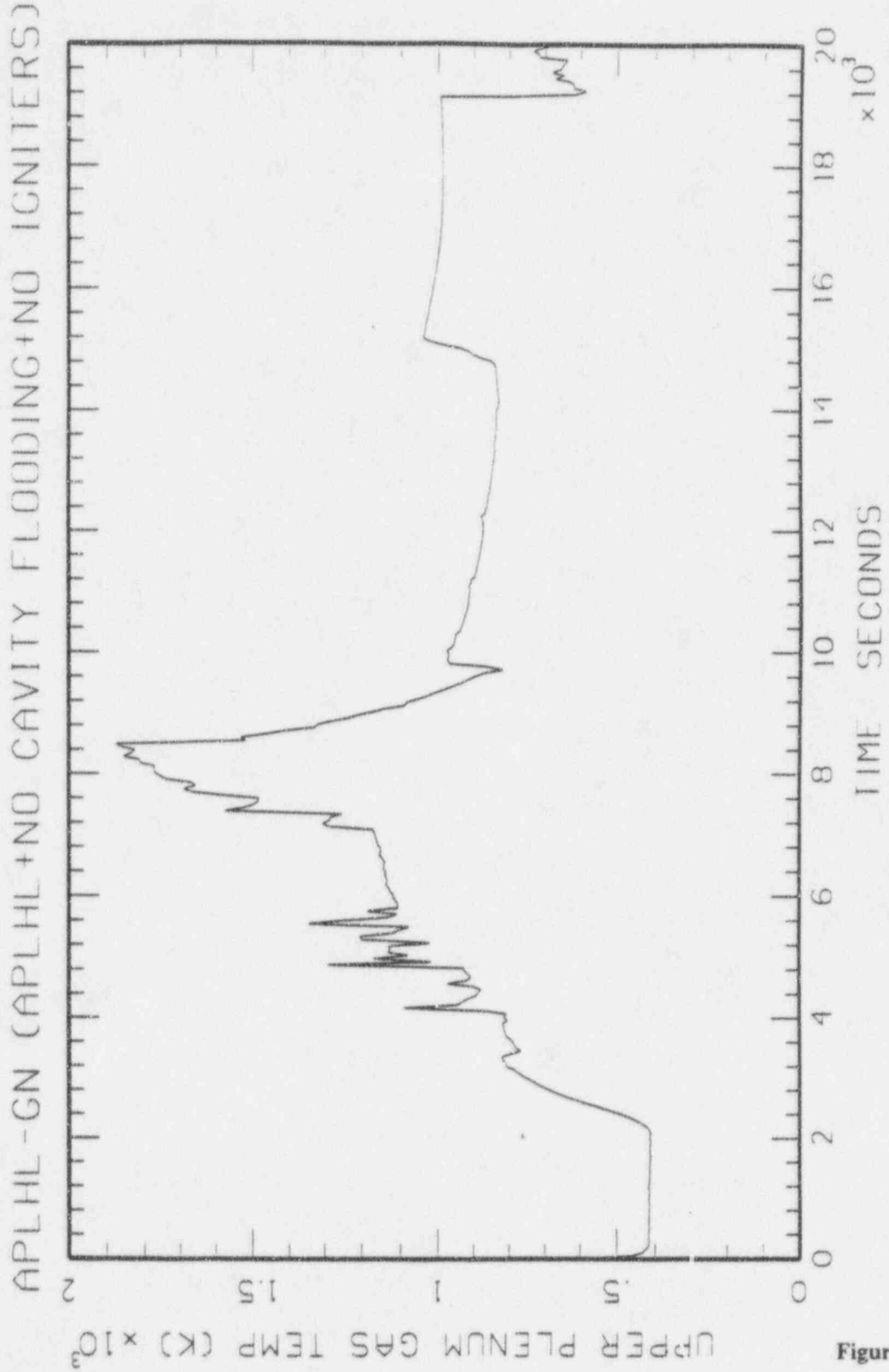



Figure D.7.1-54

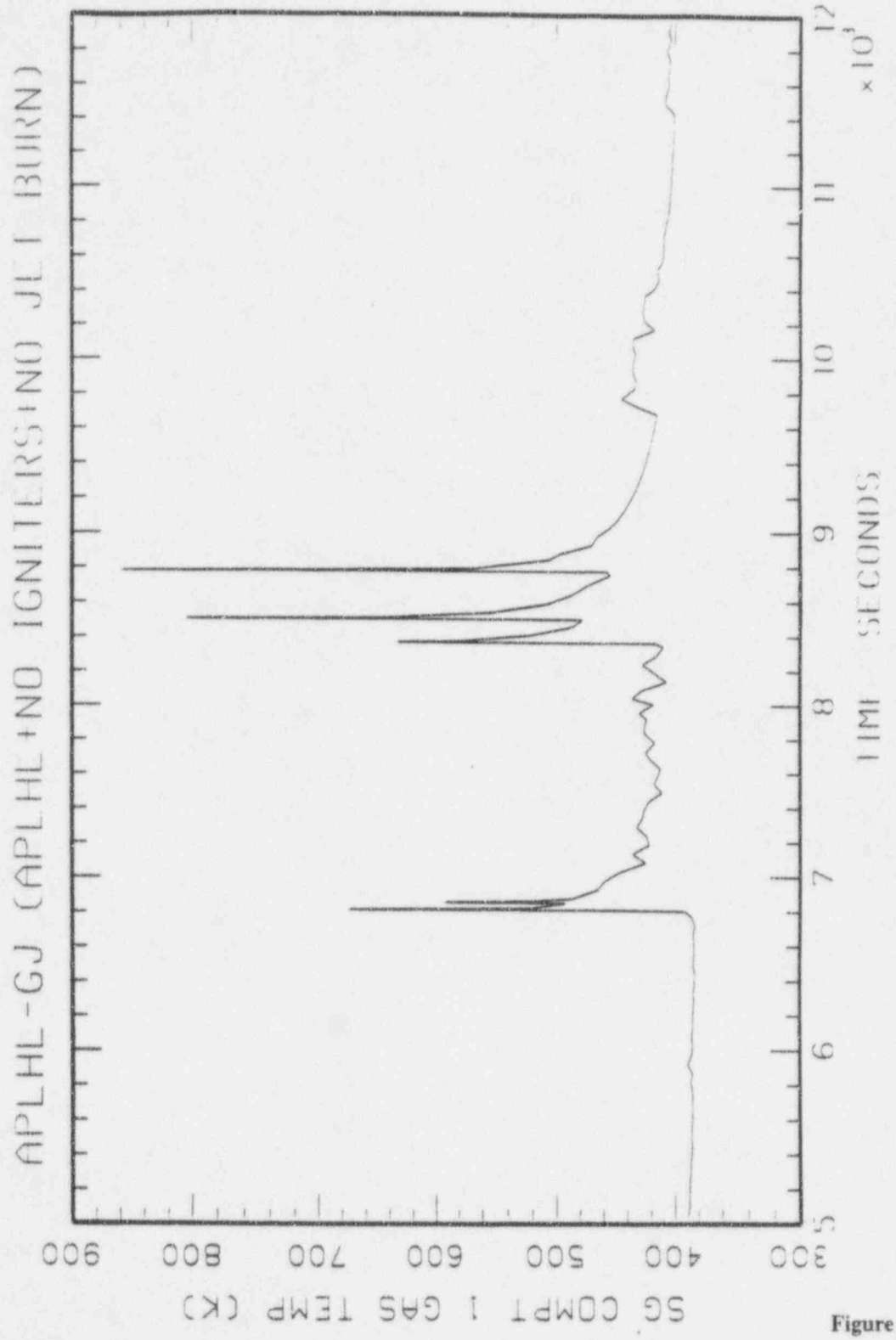



Figure D.7.1-55

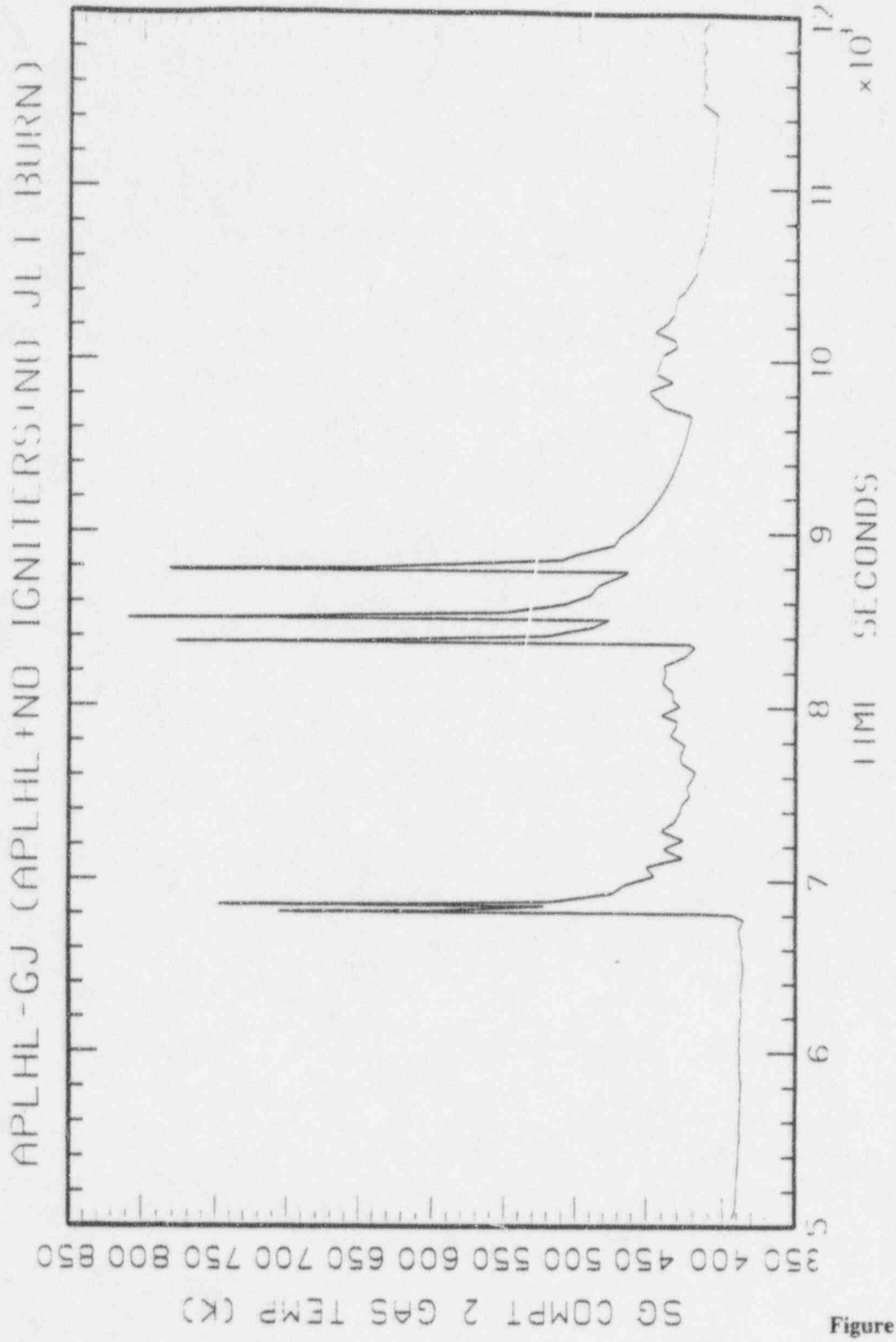



Figure D.7.1-56

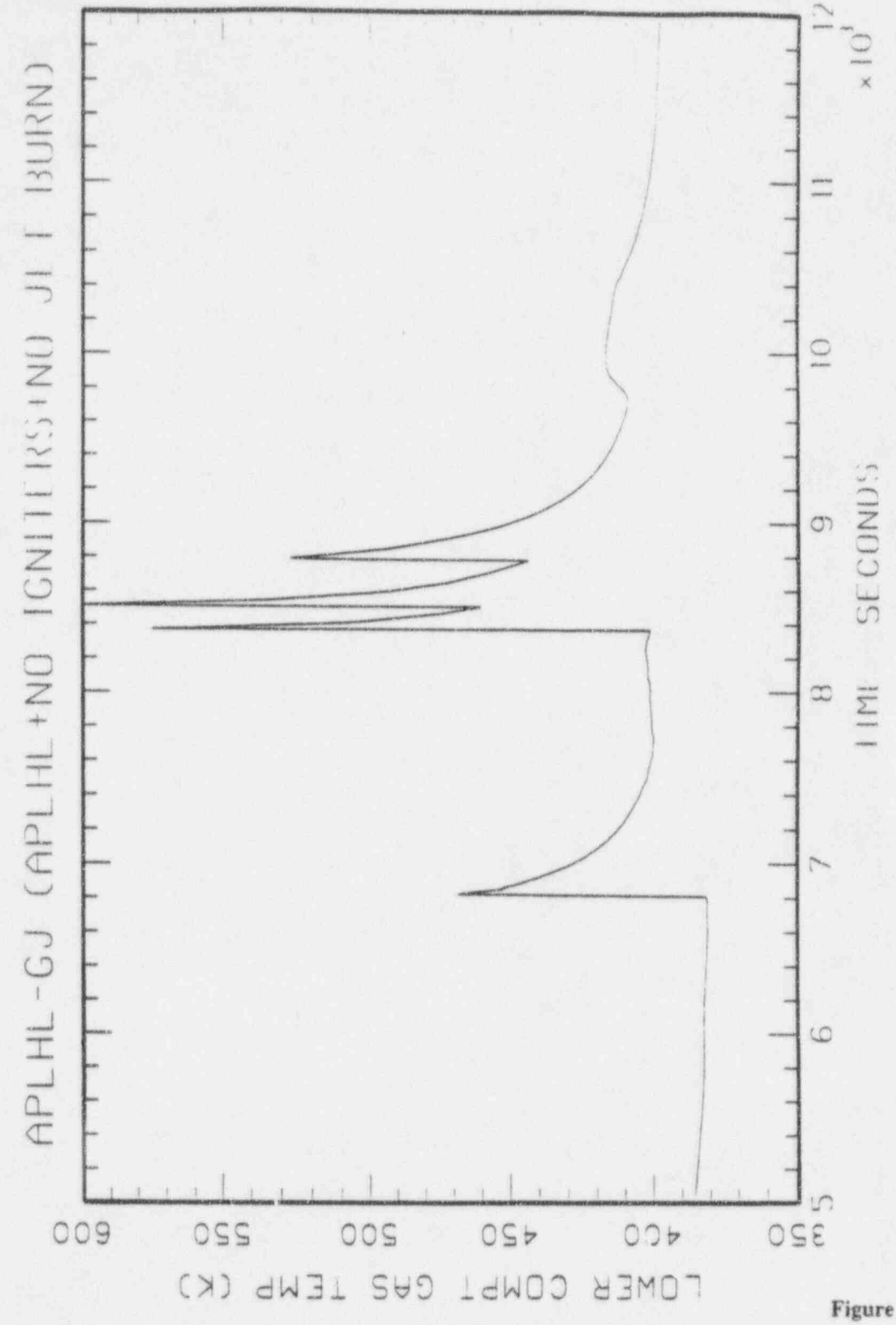



Figure D.7.1-57

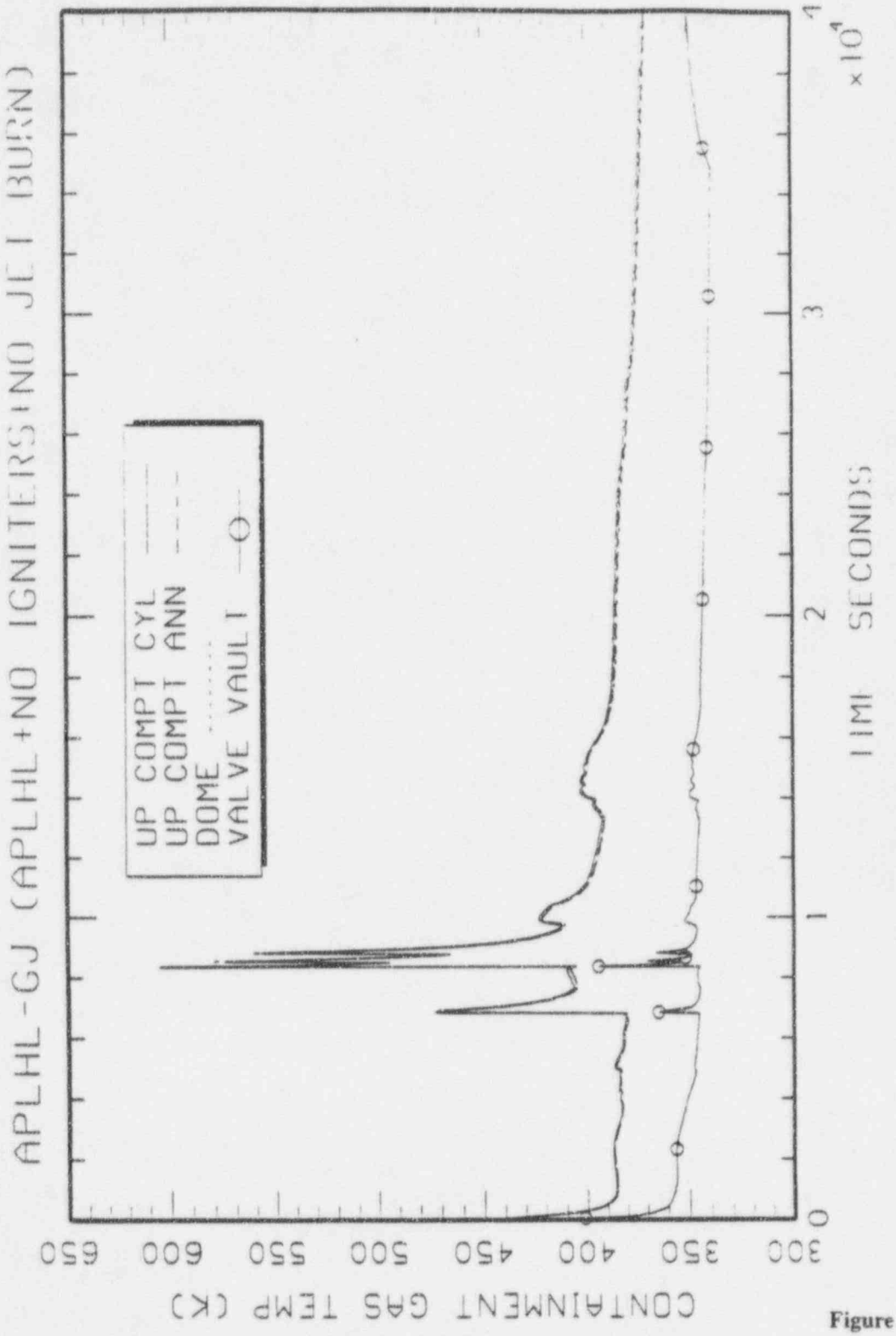



Figure D.7.1-58

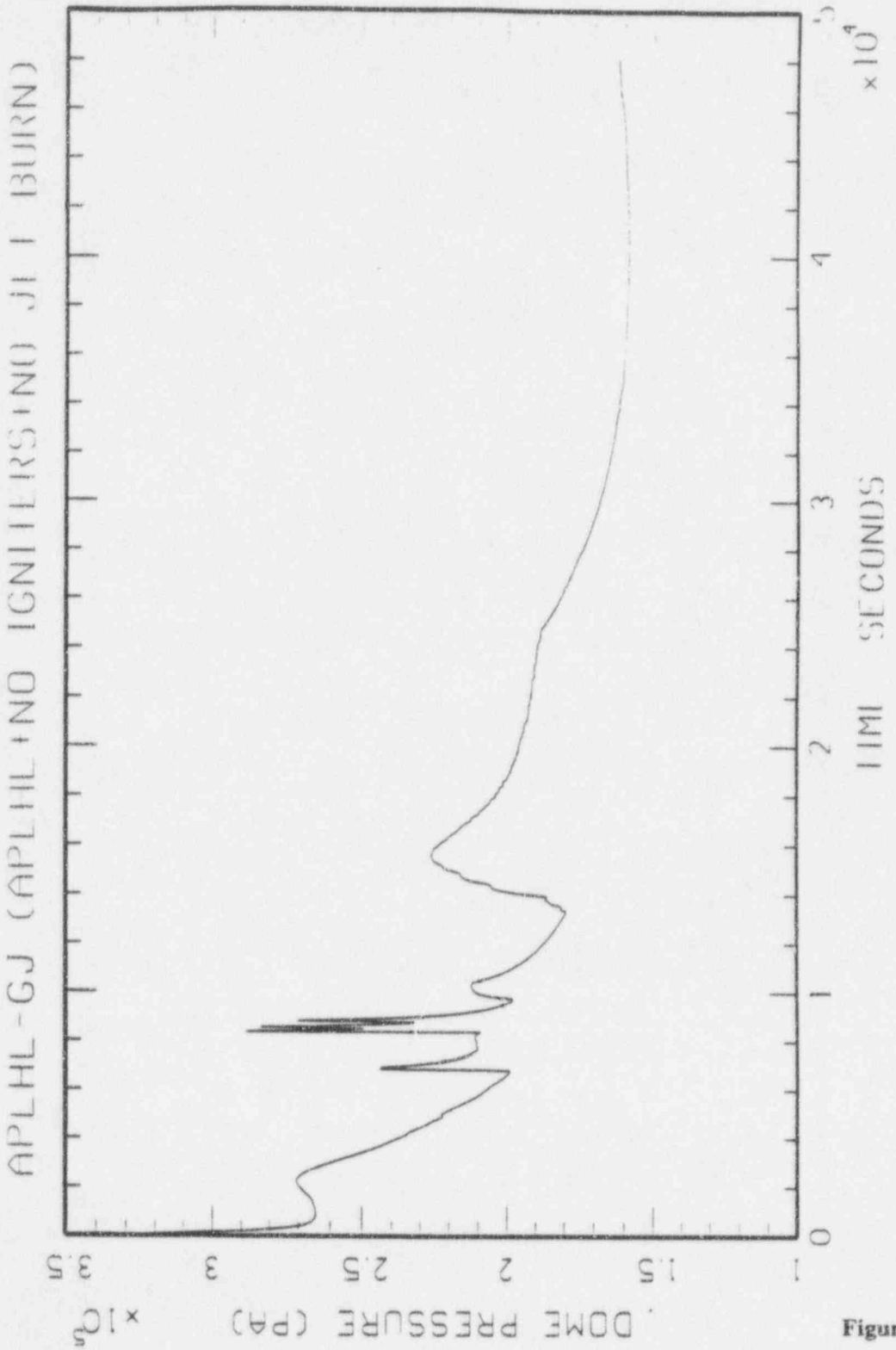



Figure D.7.1-59

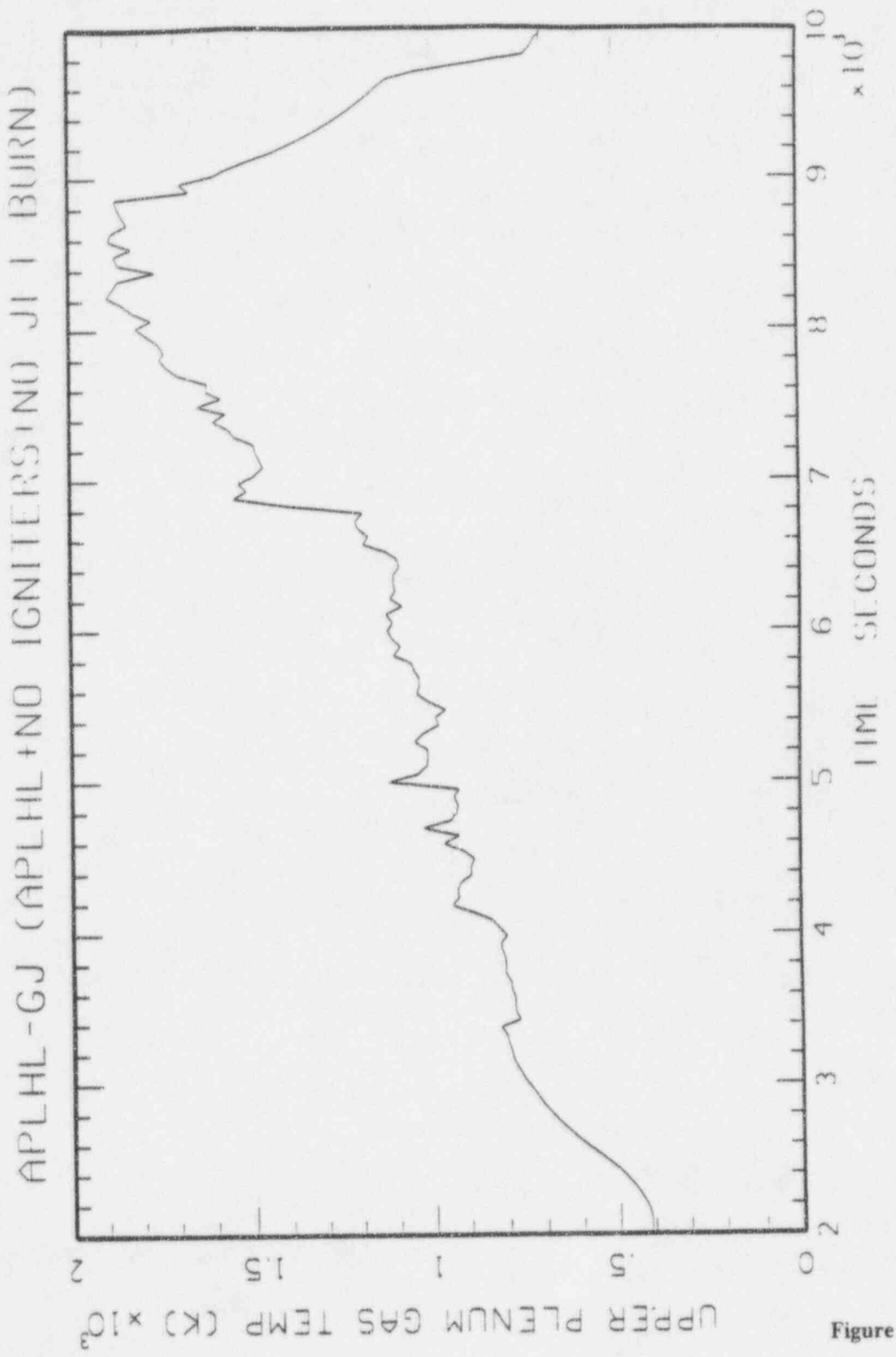



Figure D.7.1-60

## D.8 Assessment of Equipment Survivability

Since severe accidents are very low probability events, the NRC recommends in SECY-93-087, that equipment desired to be available following a severe accident need not be subject to the qualification requirements of 10CFR50.49, the quality assurance requirements of 10CFR50 Appendix B, or the redundancy/diversity requirements of 10CFR50 Appendix A. It is satisfactory to provide reasonable assurance that the designated equipment will operate following a severe accident by comparing the AP600 severe accident environments to design basis event/severe accident testing or by design practices.

### D.8.1 Approach to Equipment Survivability

The approach to survivability is by equipment type, equipment location, survival time required, and the use of severe environment experimental data.

#### D.8.1.1 Equipment Type

The various types of equipment needed to perform the monitoring activities discussed above are transmitters, thermocouples, resistance temperature detectors (RTDs), hydrogen and radiation monitors, solenoid valves, valve limit switches, containment penetration assemblies, igniters, and cables.

#### D.8.1.2 Equipment Location

Some of the in-containment equipment, i.e. transmitters, have been deliberately located to avoid the most severe calculated environments. Other equipment is located outside containment. The performance of all the equipment was judged based on the most severe postulated event for that location.

#### D.8.1.3 Time Duration Required

The monitoring requirements have been defined for each time frame, so the equipment evaluation only discusses performance during these periods. Time Frame 1 ends between 3453 seconds (0.96 hours) and 4262 seconds (1.2 hours) depending on the event. Time Frame 2 ends between 14000 seconds (3.8 hours) and 38500 seconds (10.7 hours). A limited amount of equipment has been designated for the long term (Time Frame 3) and these parameters can be monitored outside containment.

#### D.8.1.4 Severe Environment Experiments

The primary source for performance expectations of similar equipment in severe accident environments is EPRI NP-4354, "Large Scale Hydrogen Burn Equipment Experiments". This information is supplemented by NUREG/CR-5334, "Severe Accident Testing of Electrical Penetration Assemblies." These programs tested equipment types that had previously been qualified for design basis event environmental conditions. The temperature in the chamber

for the first program was in the 700 - 800°F range for ten to twenty minutes during the continuous hydrogen injection tests. Although the conditions at the equipment would be somewhat less severe, the chamber conditions envelop all of the longer duration profiles indicated for the AP600 events. The equipment in this program was also exposed to significant hydrogen burn spikes that are also postulated for the AP600. The same equipment was exposed to and survived several events, both pre-mixed and continuous hydrogen injection which provides confidence in its ability to survive a postulated severe accident. The second program tested containment penetrations to high temperatures for long durations. The Westinghouse penetration was tested under severe accident conditions simulated with steam up to 400°F and 75 psia for ten days. The results indicated that the electrical performance of the penetration would not lead to degraded equipment performance for the first four days. The mechanical performance did not degrade (no leaks) during the entire test.

### D.8.2 Equipment Located in Containment

The exposure to elevated temperatures as a direct result of the postulated severe accident or as a result of hydrogen burning is the primary parameter of interest. Pressure environments will not exceed the design basis event conditions for which the equipment has been qualified. Radiation environments also will not exceed the design basis event conditions throughout Time Frames 1 & 2.

#### D.8.2.1 Differential Pressure and Pressure Transmitters

The functions defined for severe accident management that utilize in-containment transmitters are IRWST water level, reactor coolant system pressure, steam generator wide range water level and containment pressure. Most of these transmitters that provide this information are located in the valve rooms where the environment is limited to short duration temperature transients. These transients exceed ambient design basis temperature conditions but should not impact the transmitter performance since the internal transmitter temperature will not increase significantly above that experienced during design basis testing. EPRI NP-4354 documents transmitter performance during several temperature transients with acceptable results. The IRWST water level transmitters are located in the lower compartment and are only required during Time Frame 1. The environment during Time Frame 1 will not exceed the design basis qualification parameters of the transmitters. Reactor system pressure and steam generator wide range water level are required through the second time frame. The only long term application is the containment pressure transmitter which may eventually be impacted by the severe accident radiation dose, but containment pressure could also be measured outside containment if necessary.

#### D.8.2.2 Thermocouples

The functions defined for severe accident management that utilize thermocouples are core exit temperature and containment water level. The core exit temperature (located in the upper plenum) is only required during Time Frame 1 and the containment water level (located in the steam generator 1 compartment and the cavity) is required through Time Frame 2. The

temperatures to which the thermocouples are exposed during the defined time frames do not exceed the thermocouple design.

### D.8.2.3 Resistance Temperature Detectors (RTDs)

Both hot and cold leg temperatures are defined as parameters for severe accident management in Time Frame 1. RTDs are utilized for these measurements and will perform until their temperature range is exceeded. The hot leg RTDs could fail as the temperature increases well above the design conditions of the RTDs but the cold leg RTDs should perform throughout Time Frame 1.

### D.8.2.4 Hydrogen Monitors

Containment hydrogen is defined as a parameter to be monitored throughout the severe accident scenarios. Early in the accident, the hydrogen will be monitored by a design basis event qualified device that operates on the basis of catalytic oxidation of hydrogen on a heated element. The hydrogen monitors are located in the main containment area. The design limits of this device may be exceeded after the first few hours (2 to 3 hours) of some of the postulated accidents and performance will be uncertain. If the device fails, hydrogen concentration will be determined through the post-accident sampling function.

### D.8.2.5 Radiation Monitors

Containment radiation is defined as a parameter to be monitored throughout the severe accident scenarios. The containment radiation monitors are located in the main containment area. Early in the accident, the design basis event qualified containment radiation monitor will provide the necessary information until the environment exceeds the design limits of the monitor (2 to 3 hours for some events). If the device fails, containment radiation will be determined through the post-accident sampling function.

### D.8.2.6 Solenoid Valve

Access to the containment environment from the post-accident sampling function is through a solenoid-operated valve located in the lower compartment. The environment to which the valve will be exposed is not significantly different than the design basis event to which these devices are qualified. In addition, solenoid valves in an energized condition were included in the hydrogen burn experiments (EPRI NP-4354) and survived many transients. The application of these valves (normally deenergized) for access to the post-accident sampling function adds to the confidence that the solenoid valves will perform properly when needed following the most severe transients of the postulated accidents. The radiation exposure during Time Frame 3 will exceed the requirements for design basis event testing. Based on previous experience with qualification of solenoid valves, materials can be selected to provide confidence in valve performance for about one year following the severe accident.

### D.8.2.7 Limit Switches

Limit switches are required to monitor the position of containment isolation valves that could lead directly to an atmospheric release. These isolation valves will close early in the transient, so verification is only required during Time Frame 1. The limit switches are located in the lower compartment and the environment in this time frame will not exceed the design basis event qualification of the limit switches.

### D.8.2.8 Hydrogen Igniters

The hydrogen igniters are distributed throughout the containment and are designed to perform in environments similar to those postulated for severe accidents. The igniters transformers are located outside containment. The successful results of glow plug testing through several hydrogen burns is documented in EPRI NP-4354 and provides confidence in the performance of these devices.

### D.8.2.9 Electrical Containment Penetration Assemblies

The electrical containment penetrations are located in the lower compartment and are required to perform both electrically and mechanically throughout the severe accident. The hydrogen burn equipment experiments documented by EPRI NP-4354 included a Westinghouse penetration qualified for nuclear plants. Electrical testing on the penetration cables after all the pre-mixed and continuous injection tests concluded that most (39 of 52) of the cables passed the electrical tests while submerged in water. These tests consisted of ac (at rated voltage) and dc (at three times rated voltage) withstand tests and insulation resistance tests at 500 volts. The Westinghouse penetration was also tested under simulated severe accident conditions at 400°F and 75 psia for about 10 days (NUREG/CR-5334). The results indicated that some degradation in instrumentation connected to the penetration may occur in four days under these severe conditions. The lower compartment may experience short temperature transients above 400°F but stable temperatures are significantly less, so it is expected that the electrical performance would be maintained throughout the event. The only long term measurement utilizing these penetrations is containment pressure and this can easily be measured outside containment if necessary. There was no degradation of mechanical performance (maintaining the seal) in either test program.

### D.8.2.10 Cables

The hydrogen burn equipment experiments documented by EPRI NP-4354 included twenty-four different cable types qualified for nuclear plants. Electrical testing on these cables after all the pre-mixed and continuous injection tests concluded that all (fifty two samples) of the cables passed the electrical tests while submerged. These tests consisted of ac (at rated voltage) and dc (at three times rated voltage) withstand tests and insulation resistance tests at 500 volts. Due to the exposure to many events, some cable samples had extensive damage in the form of charring, cracking and bulging of the outer jackets and still performed satisfactorily. The cables tested are representative of cables specified for the AP600 and will

only be exposed to short single temperature transients in their respective locations. Proper performance can be expected. The only long term measurement utilizing cables is containment pressure, which can be measured outside containment if necessary.

### D.8.3 Equipment Located Outside Containment

Other functions defined for severe accident management are monitored outside containment and are not subjected to the harsh environment of the event. These include the steamline radiation monitor and transmitters for monitoring steamline pressure, the passive containment cooling system flow and tank level and the post-accident sampling function.

## D.9 Conclusions of Equipment Survivability Assessment

The equipment defined for severe accident management was reviewed for performance during the environments postulated for these events. Survivability of the equipment was evaluated based on design basis event qualification testing, severe accident testing, and the survival time required following the initiation of the severe accident. It is concluded that the equipment has a high probability of surviving postulated severe accident events and performing satisfactorily for the time required.

AP600 provides reasonable assurance that equipment, both electrical and mechanical, used to mitigate the consequences of severe accidents and achieve a controlled, stable state can perform over the time span for which they are needed.

## D.10 References

D-1 *Framework for AP600 Severe Accident Management Guidance*, WCAP-13914, Revision 1, November 1996.

D-2 AP600 Emergency Response Guidelines, Revision 3, May 1997.

D-3 Westinghouse Owner's Group Severe Accident Management Guidance, June 1994.

D-4 Letter from B. A. McIntyre, Westinghouse, to T. Quay, NRC, "AP600 Loss of Coolant Accident Source Term Model," NSD-NRC-96-4675, April 1, 1996.