DETERMINATION OF THE ALLOWABLE OPERATING ENVELOPE FOR THE POINT LEPREAU SPECIAL SAFETY SYSTEMS

M.K. Gay, J.D. Kendall[1], J.H. McIntosh, D.F. Rennick[2], P.D. Thompson

New Brunswick Power
Point Lepreau Generating Station
P.O. Box 10, Lepreau, NB, E0G 2H0

[1]James D. Kendall Consultants Limited
10 Davidson Drive
Ottawa, Ontario, K1J 6L9

[2]CANTECH International
2285 Dunwin Drive, Unit 18
Mississauga, Ontario, L5L 3S3

Abstract

New Brunswick Power is systematically reviewing each special safety system to ensure that reliable operation is maintained and that the system is being operated in accordance with the safety analysis and vice versa. The ECC system is the first to be reviewed by a multi-disciplinary team, known internally at Point Lepreau as the DOA team (DOA is an acronym for Design, Operation, and Analysis). This paper reports on the review and discusses findings. Major benefits to the station arise from increased awareness, improved communication, and development of the basis for both safety analysis models and the operating envelope.

1.0 INTRODUCTION

New Brunswick Power is reviewing each special safety system at the Point Lepreau Generating Station (PLGS), to ensure that the capability and reliability of each system are maintained. The objective is to review the existing design in detail and to compare it with the assumptions used in the current safety analysis. The Emergency Core Cooling System (ECC) has been chosen as the first system for detailed review by a multi-disciplinary team.

Previous attempts to correlate design and analysis started from a list of analysis assumptions. The designers were then polled for concurrence. (This process was known in the Canadian nuclear industry at the time as the Safety Analysis Data List, SADL.) Often, the assumptions represented code inputs having no physical correspondence to the installed equipment. The system designers who were asked to verify them could not easily construct an equivalence nor could they identify missing components.

We know now that some parameters important to modelling accuracy were overlooked in the SADL process. We recognize that this was a shortcoming of the process, not any attempt to minimize the importance of the parameters.

The present study systematically examined every component of the ECC system and its function. The safety analysis models were checked for consistency. A few significant safety related issues were identified in both the analysis and the ECC system equipment and operation.

At PLGS, this project is known as DOA, short for Design, Operation, and Analysis. The DOA project includes representatives from all perspectives of the plant equipment and its operation. We believe that the integrated approach described in the following sections leads to safe and reliable operation.

Section 2 describes the overall goals of project DOA. Section 3 describes our methodology. Section 4 describes typical results and the status of the ongoing program. Section 5 lists the benefits which have already accrued to the station related to the first steps taken along this path.

2.0 OBJECTIVES

Our objectives were:

- To compile a set of requirements to show:
  - that the safety analysis is compatible with the existing system;
  - that the station is being operated in accordance with the information contained in the Safety Report and Operating Licence.
- To identify deficiencies in existing system analytical models and provide a basis for constructing new models, when required.
- To document system requirements as an aid to the System Engineer in making decisions on the operation and maintenance of the system.
- To provide a database for input to the formulation of an impairments manual and the upgrading of other documentation such as the design manuals, the operating manuals, and the test frequency studies.

3.0 METHODOLOGY

The ECC Process and Control Systems were reviewed by a core team of specialists, systematically following the process flow and the logic flow, respectively. The team considered all components, but developed only those components having a specific safety-related function. The purpose, function and specification of each component or subsystem were documented in separate Information Reports for Process and Control. These IRs were subjected to a detailed peer review in meetings with the system analyst, and the system engineer, as well as specialists in impairments, equipment qualification, and test frequency studies.

In particular, the safety analysis was reviewed to confirm that the equipment models and system functions were consistent with the equipment installed and the actual system operation. LOCA analysis and other analyses such as water hammer and containment transients were considered. Significant issues were uncovered that had not been discovered by previous methods. For example, see Section 4.1.2.

The major findings and discrepancies, identified during the peer review meetings, were tracked in a separate Issues List. Those issues deemed to affect safe operation were acted upon immediately. Many were resolved at the working group level. The DOA team referred some to NB Power management for longer term action.

3.1 DOA Process

The DOA project is divided into four phases, ranging from information gathering to completion of all issues.

3.1.1 Information Gathering / Assessment

We systematically reviewed every component in the ECC system, both process and I&C. We focused on components "critical to safety" which we classified as follows:

- anything required to make the system perform its function is critical, and
- if the system is inactive (assumed poised), then anything required to keep the system poised is non-critical, provided there are alarms to annunciate its condition should it enter an impaired state; otherwise, those components are critical too. In this case, the credited annunciations and indications become critical.

We prepared a detailed data sheet for every critical component. For those which we classified as "not critical to safety", we prepared a summary data sheet explaining the basis of our judgement. As it turned out, some components which we dismissed as "not critical" early in our review were reclassified as we understood the integrated behaviour of all the systems better. (The HPECC water tanks heating circuit, described later in Section 4.1.1, is an example of a series of components which we initially dismissed, and later reclassified.)

For each component, we adopted a "back to first principles" approach. We developed our information from elementary drawings, manufacturer's drawings and specifications, and actual operating documentation such as instrument calibration sheets and their technical bases documents.

As mentioned above, we divided the review into two disciplines, Process, and Instrumentation and Control. This suited the experience of the two people (Rennick and Kendall respectively) who did a significant portion of the detailed information gathering. This was appropriate because we could better recognize the important ingredients. Additional issues surfaced when these ingredients were presented to the peer group meetings, usually monthly.

Also, this subdivision of the review was appropriate because of the functions of the equipment. Generally, process components were amenable to a process flow component by component review, while I&C components were more suited to a logic flow "subsystem" approach.

3.1.1.1 Process Components

For process components, we divided the system into five sections: a) High Pressure ECC (HPECC), b) Medium Pressure ECC (MPECC), c) Low Pressure ECC (LPECC), d) Gravity Injection from the dousing tank, and e) auxiliary systems. For HPECC, we followed the flowsheet from the air compressors right to the reactor headers, and constructed data sheets for each component. We then did the same for MPECC, LPECC, and Gravity Injection. Often, the paths overlapped. Finally, we included all the auxiliary systems which performed an ECC function, e.g. Main Steam Safety Valves (MSSVs) and loop isolation.

For each component, we listed all the physical attributes it could possibly have. Then, we evaluated the importance of those parameters to the safety function of the component and divided them into two main groups: Process Variables and Non-variant parameters. The "Process Variables" were ones which the system engineer could measure and/or control (e.g. pressure, temperature, etc.); the non-variant parameters were ones which the system engineer could not control on a day to day basis but would be important for system changes or replacement part orders (e.g. tank volume, material properties, etc.). For each of these we reviewed the safety analysis models and assumptions to determine their importance to safety. We also reviewed the Operating Procedures for possible effects.

A standard format for each data sheet (by component type) was followed as far as possible to minimize chances of overlooking important elements of the component's function. The categories treated are as shown in the inset.

Attachment 1 is an extract from a typical component data sheet for the HPECC gas tank, 3432-TK2. It follows the format described above. Early in the process, we attempted to separate the safety analysis aspects from those the system engineer would control. Afterwards, we found that describing the safety analysis assumptions with the parameter being discussed to be more effective and more in keeping with philosophy of DOA: closely linking Design, Operation and Analysis.

1. TITLE

2. FUNCTION
A statement of the purpose of the component.

3. DESCRIPTION
A description of the physical attributes of the component such as size, type, manufacturer, failure mode, air/water/power source and requirements, etc.

4. LOCATION
This section describes the physical location of the equipment. This assists in setting environmental requirements for the component.

5. PARAMETER SUMMARY
This is a summary of the parameters which are likely to be affected by the component, or which it is exposed to. It is a summary only, each of the headings is expanded in Sections 6 and 7.
The section is subdivided into two additional categories:
a) Process Variables:
- These are parameters which vary with time, and usually can be monitored with time.

b) Non-variant Parameters:
- These parameters do not vary with time and are of most interest to the safety analyst, or to the system engineer should he wish to replace the component.

Items which are critical to safety, and which will set the requirements on the component are tagged with a bolded "**(critical)**".

6. SAFETY REQUIREMENTS

This section develops and discusses the importance to safety of the parameters enumerated in Section 5. For each critical component, we define the range of allowable operating values.

7. OTHER CONSIDERATIONS

This section deals with other items over which the system engineer has no immediate control. He would be interested in these parameters for equipment changes or system operating changes. Typical examples would be code class, environmental qualification, seismic qualification, periodic inspection requirements, availability requirements.

Standard Format for Process Component Data Sheets

3.1.1.2 Instrumentation and Control Components

We used a similar process for I&C components. I&C subsystems were divided into four general categories: Initiation Channels, Voting Channels, Control Channels, and Annunciation and Indications. Typically, the initiating signals provide inputs to voting channels which combine the signals from three channels including conditioning parameters. The outputs from the voting channels fan out to many control functions. The Control Channel Data Sheets included operation of solenoid valves, pneumatic valves, and motors. Annunciation and Indication, which monitor critical variables, were included because the operator must have clear indications of failures of critical equipment during normal and abnormal operation.

We followed the logic path from the initiating signal to the eventual operation of the device, describing every power supply, transmitter, relay, current alarm unit and motor control centre along the way. We paid particular attention to function, timing, drift, and accuracy specifications for each.

1. TITLE

2. FUNCTION
A statement of the function(s) of the I&C loop or sub-system. This is a summary statement, aimed mainly at what a safety analyst might want to know. A detailed analysis of the function appears in Section 8.

3. RELATED DOCUMENTS
A listing of relevant drawings, specifications, and instrument calibration sheets.

4. EQUIPMENT
A description of the equipment which makes up the loop or subsystem. This includes equipment manufacturer, and all relevant specifications. Typical specifications are its physical attributes, its location, and its environmental and seismic qualification.

4. POWER SUPPLY
This section describes the power supply requirements, the location and the qualification of the power supply.

5. TIMING SPECIFICATION

This section develops the net timing response of the loop or sub-system, based on the manufacturer's specification, or on PLGS bench test results where available.

6. ACCURACY SPECIFICATION
This section develops the overall accuracy of the loop or sub-system based on the RMS combination of the individual contributors. The elements to accuracy are a) inherent accuracy, b) drift, and c) calibration error.

7. COMPONENT STATES
This section analyses all the possible component states the sub-system can have, based on its inputs.

8. SPECIFIC FUNCTIONS
This section describes the detailed function of every component.

Standard Format Items for I&C Component Data Sheets

Again, a standard format was followed as shown in the accompanying inset.

Attachment 2 is an example of a typical I&C Data Sheet, for the control of the valves in the line from the Dousing Tank to the ECC Pump(s).

3.1.1.3 Relationship between Process and I&C Requirements

Generally, the response required from the process components set the requirements for each of the I&C subsystems. For example, a subsystem might operate with a 200 ms response time according to its design and specification of equipment, but if the process equipment's mission required only a 5 s response, it would be unnecessarily restrictive to set a 201 ms criterion for an unsafe fault. On the other hand, an action criterion of 250 ms for a safe fault might be reasonable because it would provide a system health monitoring function while leaving some margin for rational operation.

Referring back to the sample of the Process Component Data Sheet, notice that instrument and control values have been summarized. This enables the safety analysts to see what ranges to expect on process parameters, and what alarms and indications the plant operator would have in managing the accident.

3.1.1.4 Relationship to the PLGS Impairments Manual

If a component fails to meet its requirements, the component is considered to be in a faulted state and a system impairment may result. The DOA team deliberately avoided defining impairment levels. Instead, we assigned up to three categories to each component as appropriate. The categories were unfaulted, safe fault, and unsafe fault.

The corresponding level of system impairment depends on redundancy, use of the system, accident analysis and operational assumptions, availability of annunciation, etc. However, a one-to-one correspondence with Fault Category does not exist in many cases. The Impairments Manual provides the interpretation of information in this context, and therefore is the authority on impairment categories.

3.1.2 Judgement of Operating Envelope

As stated in Section 2, our focus was to set requirements on the systems so that we could ensure that the safety analysis provided margin for all foreseen operating conditions of the equipment. Part 1 of this four phase process defined the systems' capabilities. However, requirements must be specified to declare a component to be in a safe or unsafe faulted state. This involves considerable negotiation between the system engineer (representing both design and operations) and the safety analyst.

3.1.3 Documentation Upgrades

In phases 1 and 2, we discovered many inconsistencies between documents, and noted that some of these reference documents have not kept pace with the equipment and operating setpoint changes. These must be addressed. Typical documents which may be affected are: Design Manuals, Operating Manuals, Impairments Manual (see Section 3.1.1.4), Testing Procedures, and Test Frequency Studies.

3.1.4 Ongoing Items

During phases 1 to 3, we maintained a tracking list. The issues divided into 4 main categories:

i) Inconsistencies or Unknowns
Generally, these were items which we did not see as an immediate issue, and which required further research, or where information was scarce.

ii) Safety Issues
Safety Issues were items which we believed would have an immediate safety impact and needed to be dealt with expeditiously.

iii) Inconsistencies between Design/Operations/Analysis.
These were minor items which we could deal with at a working group level (Design, Operation and/or Analysis)

iv) Issues for Management Attention
These were issues that involved considerable expenditure of human resources, or expense, and which may have impact on other parts of the station's operation.

In all categories, the items which were resolved were left on the list as a record of their disposition.

4.0 RESULTS

4.1 Typical Findings

There was a large number of findings, mostly of a minor nature. The following sections discuss typical results from three areas, Design, Operation, and Analysis.

4.1.1 HPECC Tank Recirculation Pump

<u>Problem</u>

The HPECC tank water must be kept at a temperature between 18.5°C and 30°C. Also, the water must be recirculated to provide mixing for chemical control reasons.

A small pump recirculates water in a heating/chemical addition loop, taking suction from near the top of the HPECC tanks, pumping through a thermostatically controlled heater, through an underground line connecting to the main ECC pipe near the reactor building wall, and back through the ECC pipe to the bottom of the tanks. See pump P3 in Figure 1. In the event of a LOCA, channel K of the ECC signal trips the pump. There are three potential problems associated with this configuration:

a) During a LOCA, the suction to the pumps would be uncovered relatively early in the transient. (The location of the suction shown on the schematic is not representative; it is actually located very near the top of the straight section of the tank.) If the recirculation pump fails to trip, there is a potential to inject gas, N_2 and air, into the ECC line near the reactor building wall, and hence into the reactor core. For certain break sizes, this would have detrimental effects on system function. Even if the pump did trip, for large breaks there could be a race between the 2" line emptying, and the tank emptying.

b) P3 has only one trip signal, provided from channel K.

c) The water in the tanks contains hydrazine for corrosion control reasons. When hydrazine is heated, it can release small quantities of gas, and the bubbles are introduced at a point in the main ECC piping where they can rise into the piping leading to the isolation valves. Any gas which bubbles up the pipe will form gas pockets at the high points, causing potential problems with waterhammer if the HPECC system is activated (these high points are vented annually, and there are no records of significant amounts of gas coming out).

An associated problem is that the safety analysis model does not include this piping. Otherwise, we would have been aware of the impending problem earlier, or dismissed it. Our judgement was that it would be easier to implement the following design solution than revise the safety analysis model and repeat a significant amount of analysis.

<u>Solution</u>

NB Power is evaluating reversing the flow direction of the P3/HTR3 combination as a potential solution. This will address all three situations simultaneously. The check valve on the pump discharge would be re-oriented to prevent gas blowing into the reactor [points a) and b)], and any bubbles which formed would be discharged into the water tanks and rise to the top, where there is already a free surface.

If no offsetting problems arise from the assessment of this design solution, there will not be a need to include it in the safety analysis model.

4.1.2 HPECC Gas/Water Tank Modelling Enhancements

Problem

The detailed review of system operation raised several points related to the current modelling.

The current FIREBIRD representation does not model the HPECC tanks explicitly. A pressure/enthalpy boundary condition node is used where the integrated flow to the reactor is tracked to calculate the gas expansion, and derive an isentropic pressure rundown. There is also a rudimentary calculation of the variation of hydrostatic pressure variations as the tanks empty. There are three points related to this simplification.

a) Because only one virtual tank is used, the expected differential level between the tanks related to differences in flow resistance of the piping cannot be tracked. The actual instrumentation for shut-off uses different levels for each tank to account for the differential flow. The current model does not permit simulation of this effect. This means the actual shutoff of the injection valves cannot be timed properly and the calculated inventory injected is not quite accurate.

b) The polytropic expansion coefficient will be a function of break size. That is, for the fast transients associated with large breaks, the pressure rundown of the ECC driver gas will be close to isentropic; for small breaks, it will be closer to isothermal. This affects calculation of flow delivery to the reactor, plus the timing of change-over to medium pressure ECC (MPECC).

c) The shutoff of the valves is based on volume discharged, not on the pressure. When the pressure is not properly calculated, the changeover to MPECC cannot be modelled. We expect that for some break sizes, the change over will occur before all the available inventory has been discharged and for some time, water will be injected to the core as a blend from MPECC and HPECC. When the system transfers from MPECC to LPECC, (taking suction from the reactor building floor instead of from the dousing tank), there will be a pressure drop in the delivery from the ECC pumps, and more water could come from the HPECC tanks at this time. An additional consideration is that there could be a pressure regain in the HPECC driver gas. The reason is as follows. For a fast transient, the isentropic expansion of the driver gas lowers its temperature to around -80°C. Then as heat transfers from the piping and tank walls, the gas temperature will regain to approximately 16°C. Using the perfect gas law, the driver gas will repressurize to about 150% of its pressure at the end of the fast transient. This, too, will affect the blend of water flow from HPECC, MPECC, or LPECC until the valves are shut on tank level. None of this has been modelled.

Solution

NB Power has already commissioned AECL to upgrade the ECC accident analysis models, and these factors are being included.

4.1.3 Handswitch Operation in the SCA

Problem

Each of the logic trains was checked from the elementary diagrams. During the review of the handswitches in the SCA, we discovered that the handswitches for the main gas valves, 3432-PV81 & PV82, would not open the valves unless the handswitches to close the vent valves PV83/PV84 had been operated first. Obviously, these interlocks were deliberately installed to prevent depressurizing the gas tank through the vent valves, but this idiosyncrasy was not described in the Design Manual. While this would not pose a significant problem if the operator followed the procedure of operating the vent valve handswitch first, gas valve second, it would be confusing if, unaware, he operated the PV81 or PV82 handswitch first and waited for the EMI to change state before proceeding with further actions.

Solution

The DOA team advised PLGS Operations. The draft generic Emergency Operating Procedure for the SCA already included this sequence.

4.1.4 Pressure Transmitter PT-26

The ECC water tanks are continuously pressurized for two reasons. First, a pressurized vessel will provide leak detection, both visibly and through monitoring pressure. Second, to prevent draindown of the column of water up to the H_2O isolation valves in the reactor building, an overpressure must be applied to the free surface of the HPECC water tank. For the elevations at PLGS, the minimum overpressure is on the order of 60 kPa(g). The operating range is 160 to 260 kPa(g), but it is controlled manually based on pressure alarms.

The accuracy specification of the instrument, 63432-PT26 in Figure 1, on which the associated alarms are based was near the range being monitored/controlled. The range of this transmitter is 0 to 7.5 MPa(g). This range is required because the transmitter also measures pressure during the full pressure tests (annually) and these pressures are up to approximately 5.0 MPa(g).

Thus, there are two problems. First, there is a loss of annunciation on an important parameter if the transmitter or its loop fails. Second, the inherent accuracy is nearly the same as the process variable being measured.

<u>Solution</u>

The proposed solution is to add a second pressure loop with a lower range to provide good accuracy during normal operation (i.e., except when the annual pressure test is performed, and the reactor is shut down for this test). The current transmitter would be left as-is, providing the indication during the annual test, and a backup for the lower range meter during normal operation.

4.2 Status

The assessment of Design, Operations and Analysis is a continuous process. Occasionally, not all of the rationale for certain design parameters could be recovered. In these cases, the team made judgments, and recorded these judgements in the two reports. The reports have been produced in magnetically readable format so that they can be easily updated, if new information becomes available. In summary, the DOA reports on ECC are intended to be a living document.

As stated in Section 3.1, the process has four stages. We have essentially completed stage 1 for ECC. Followup of the issues will require further consideration and analytic effort, including further assessments of the relative importance of the issues. We have also addressed parts of the remaining three items, but as suggested, this will be an ongoing process.

4.3 Future Work

Based on the experience and benefits from the ECC DOA process, NB Power intends to continue with its plan to review the remaining special safety systems, followed by reactor core parameters, safety support systems (such as Boiler Makeup Water, Emergency Water Supply, Emergency Power Supply), the utilities (electrical power, service water, and instrument air), and the remainder of the process systems. The review of Containment Systems has already started.

5.0 BENEFITS

The benefits to the station and station personnel were:

- For Analysts:
  - declaration of implicit assumptions;
  - improved understanding of equipment being modelled;
  - improved understanding of functional operation;
  - improved code and plant model (eg:, two tanks, non-condensibles, AMADs, instrumentation uncertainty, input of actual field values).
- For Operators, Maintainers and System Engineers:
  - heightened awareness of accident analysis assumptions, (part of an on-going program);
  - specification of items which should be monitored;
  - establishment of requirements for replacement of components;
  - improved understanding of the allowable plant operational envelope.
- For the Station as a Whole:
  - reduction of avoidable impairments;
  - improved auditability of safety analysis;
  - improved communications between safety analysts and system operators.

Acknowledgement
The authors of this paper made up the core DOA team. The following people also contributed to the DOA process regularly:

Steve Uhlman	System Engineer
Norm Boucher	Problems and Issues Resolution
Derek Mullin	Test Frequency Study Assumptions
Keith Scott	Impairments Interpretation
Malcolm Callister	Environmental Qualification & General I&C Issues
Mark A. Wright	Safety Analysis
Andrés Galia	Safety Analysis
Leslie Fernandez	Process Resource
Mike Soulard	AECL Designer Input
Joe Sobolewski	Overall Comments on the Information Reports

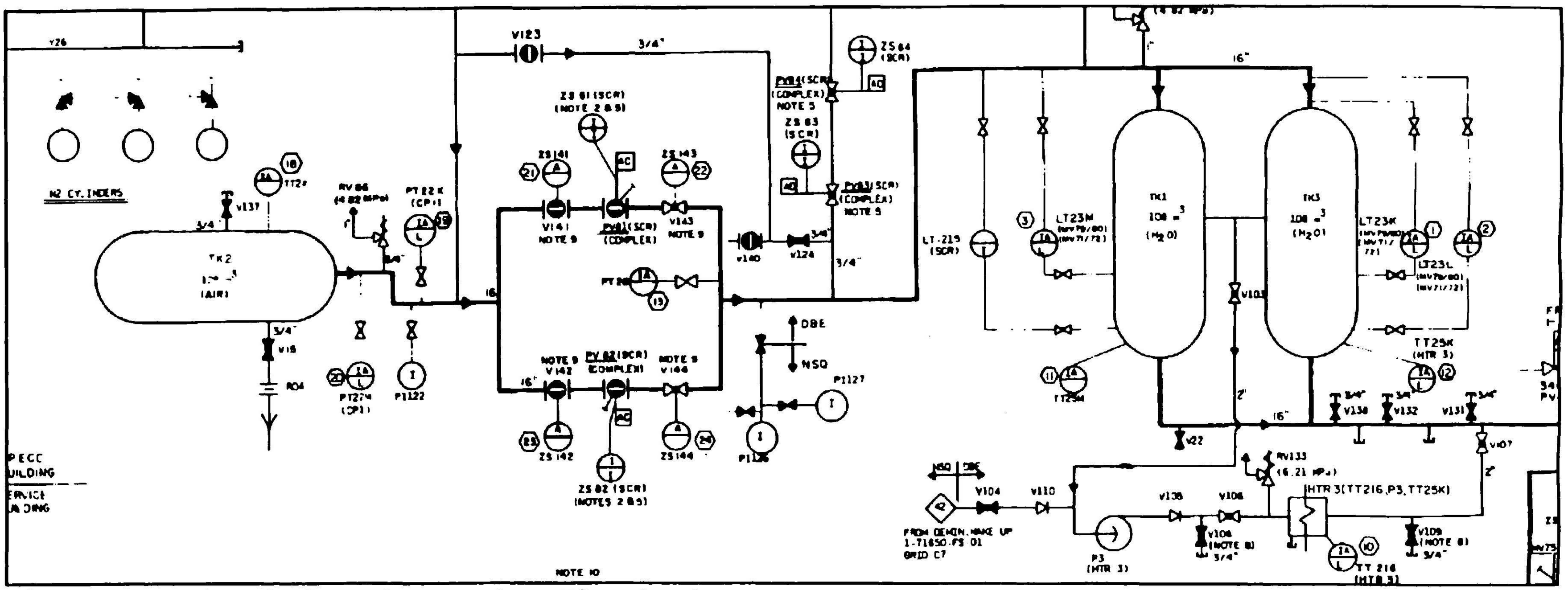

Figure 1   Extract from ECC System Flowsheet

EXTRACT FROM TYPICAL
PROCESS SYSTEM COMPONENT DATA SHEET

COMPONENT: 1-3432-TK2

1. TITLE: HPECC Gas Tank

2. FUNCTION:

- Contents of tank provides the source of energy required to drive the HPECC water contained in the two accumulator tanks, TK1 & TK3, into the PHTS.

3. DESCRIPTION:

- Cylindrical body 12'4" diameter and 24'4" long with truncated hemispherical head and oriented horizontally. Fabricated by Dominion Bridge of unlined carbon steel ASME-SA-516 Gr. 70 (Drwg: 87-34324-9002-1-DD Rev. 15). Shell is 4" thick; head is 2.5" thick. Tank contains 107.6 m^3 of an air/N_2 mixture supplied by air compressor 1-3432-CP 1 and backed up by an array of N_2 bottles (see 87-3432-2001-FS-E, Rev. 14)
- The tank is sloped slightly to allow water (if any) accumulation to be drained via the drain valve, V15.
- The exterior surface of the tank is painted for corrosion control, and is not insulated.
- SCN: 583L1831 (see 87-34324-9003-1-DD-D Rev. 5)

4. LOCATION:

- ECC Building (E-101) (see 87-20030-2001-21-GA-E, Rev. 2)
- See drwgs:
  - 87-34320-56-1-GA-E Rev. 10
    for general layout detail. Note this drawing is not up to date in some details (eg. location of PV81/PV82 and associated piping).
  - 87-34320-2004-01-GA-E Rev. 1
    for pictorial view. Note this drawing is also not completely up to date.

5.0 **PARAMETER SUMMARY:**

5.1 Process Variables:
- **Pressure (critical)**
- Temperature
- Composition & Chemical Purity **(critical)**
- Relative Humidity

5.2 Non-variant Parameters:
- Tank Volume
- Flow Resistance at the Nozzle

6.0 SAFETY REQUIREMENTS:

6.1 Process Variables

6.1.1 Pressure:

(a)

Unsafe Fault (USF)	Safe Fault (SF)	Operating Continuum No Fault Normal Operating Range	SF	USF

A | B Low Alarm | C Nominal | D High Alarm | E

Indicated Pressures in MPa(g)

A ≤ 4.04
B ≤ 4.33
C = 4.55
D ≥ 4.66
E ≥ 4.96

(b) Discussion:

Pressure is a critical process variable because it applies the force for displacing the HPECC water inventory, which in the event of an accident, will cool the fuel in the PHTS during the HP phase.

A low gas pressure reduces the HP injection flow rate into the core and in the extreme, causes it to not occur.

A high gas pressure may impose additional waterhammer loads on the ECC and PHT systems during activation. In principal, the overpressure safety valve RV86 limits system high pressure.

A high gas pressure discharges the water inventory from the tanks faster.

(c) Operating and Alarm Values:

The unsafe fault limit on low tank pressure (≤4.04 MPa(g)) comes from reference 1 (OP&P) section 3.12.1 ii) and reference 2 pg. 9 (DM34320/63432). (see Section (f) for Additional Commentary).

The unsafe fault limit on high pressure is based on the opening pressure for RV86 (4.82 MPa(g)) plus 3% uncertainty, to yield 4.96 MPa(g).

The safe fault limit corresponds to the low and high alarm setpoints.

(d) Indications/Annunciations/Instrument Uncertainties:

The pressure in TK2 and the lines leading downstream to the HP gas isolation valves is measured by pressure transmitter PT22K and M, and local indication is given by PI-122. PT22K and M loops provide both visual indication as well as annunciation on high and low values, in the MCR.

Window Alarms W3-43 provide further indication to the operators:
(a) "3432 P22M ECC GAS TANK PRESS LO";
(b) "3432 P22K ECC GAS TANK PRESS LO";
(c) "3432 P22M ECC GAS TANK PRESS HIGH";
(d) "3432 P22K ECC GAS TANK PRESS HIGH";
(e) "ECC GAS 3432 TK2 TROUBLE".

Further I&C details are given in Section 7.3 of reference 3 (IR-63432-01) and Section 7.2 of reference 4 (OM 34320/63420).

The alarm is backed up by routine surveillance of the panel meters, called up weekly via OM tests 63432.39 and .40. Hence, failure of the alarm should be treated as a safe fault, provided more frequent monitoring is employed.

In the event of a complete lack of pressure indication in the MCR, tank pressure can be obtained by examining PI-122 provided this gauge has been kept in a calibrated state.[1]

Analysis which assumes a low tank pressure should include an uncertainty allowance of 56 kPa (Section 7.3.6 of reference 3) to account for measurement and indication uncertainties. This value includes allowance for the current alarm unit (even though it is assumed to fail and is not on) to cover either indication uncertainty or to provide for future flexibility.

Calibration specifications for both the transmitters and current alarm units are given in Section 7.3.6 of reference 3.

(e) Mandatory Testing:

TK2 is under continuous test since pressure (both high and low) is alarmed and checked as discussed in (d), hence there is no specific test.

As discussed previously the instrumentation verification and panel checks are performed under OM tests 63432.39, and .40, and the tank is subject to periodic inspection (see Section 7.3).

(f) Additional Commentary:

LOCA analysis performed with FIREBIRD did not explicitly model the HP gas tank and the downstream piping and valves leading to the two HP water tanks. The code applied a pressure/time boundary condition to an assumed combined set of water tanks. Details are provided in reference 5 (pg. 4-33). (See Appendix 2, Table 3 for a sample calculation of the current FIREBIRD model pressure rundown versus volume of ECC discharged).

It should be noted that the basis for the original selection of pressure in the tank, nominally 600 psia, is described in Volume 2 of this IR, section ## (memorandum, P.J.Allen to J.D.Sainsbury, "Summary of G-2 High Pressure ECC Design Assist", 78.02.09, AECL file 66-01500 to be part of IR). The selection of 600 psia was based on performance for the feeder

---

[1] Its calibration must be trustworthy because it is used as a gauge for verifying the digital readings in tests 63432.30 and a reference in OM-34320/63432 Rev. 14 in case of irrational readings of the instrument loops 63432-P22K and M.

size break. The other option considered, 800 psia, did not give perceptibly better performance for larger breaks[2], and 600 psia was adequate for small breaks.

Additionally, the value 4.04 MPa(g) was modified by 0.25 MPa following a minor misinterpretation of a requirement to have 600 psia available at the reactor headers. Reference 6 page 6 refers to SIC 5506 as the report resolving this discrepancy.

Finally, an explicit model of the gas tank and the associated valves and piping have been developed for the CATHENA code. This model (CATCIRC-PL2 and its later derivatives) will be used for future LOCA analysis.

A summary of LOCA analysis for the various events is given in the PLGS Safety Report.

Details of the potential effect of waterhammer are given in the Volume 2 of this IR, section ### ("POINT LEPREAU ECC System Documentation of Pressure Transient Analysis for ECC System Simulating (i) LOCA Conditions (ii) Dynamic Tests with Rupture Discs Bursting at 75 psid" by J.M.Francisco, 82-10-04 for geometric description. Analysis was subsequently revised for 50 psid rupture disk and transmitted under memo, Francisco to Liederman, "Routine Testing of 3432-PV81/82", 83-01-18, AECL file 87-34320-270-000).

- The characteristics assumed in the WH-NWA computer code, used in the waterhammer analysis, for the gas tanks are as follows:

P_0	Gas tank	600 psig (note that WH-NWA ignores elevation heads)
P_0	Downstream of gas valves	25 psig
V	Gas tank[3]	3820.98 ft^3 (108.20 m^3)
V_0	Downstream of gas valves	124.3 ft^3
T_0	Gas tank	70°F (21.1°C)
Valve opening time		4.0 s.
No. of gas isolation valves		2

END of EXTRACT

[2] In fact, sheath strain/fuel failures were slightly worse for large breaks because of the faster rewetting and faster depressurization of the fuel. This analysis was done with a single loop FIREBIRD model.

[3] Clearly this volume includes an allowance for the gas piping up to the isolation valves 3432-PV81/PV82, but note it is different from previously used FIREBIRD analysis.

SAMPLE INSTRUMENTATION AND CONTROL DATA SHEET

I AND C DATA SHEET

5.3 1-3432-PV11, -PV10
Dousing Tank Isolating Valve Control
Channels K and M

5.3.1 FUNCTION

1) To open the dousing tank isolating valves automatically when the ECC Channelized Voting Logic Channel K (M) is in the ECC trip state.

2) To open and close the dousing tank isolating valves under manual control from the MCR.

3) To annunciate if:

   - the dousing tank isolating valve PV11 (PV10) is open under manual control;

   or if:

   - both the dousing tank isolating valve PV11 (PV10) and the recovery sump isolating valve PV1 (PV2) are closed under manual control.

4) To enable, when PV11 (PV10) is fully open, the automatic startup of the ECC pumps, PM1 and PM2, when they are in either AUTO or STANDBY.

5.3.2 RELATED DOCUMENTS

- Pneumatic Connection Diagram 87-63432-3-9-ED-D Rev 09.
- Schematic Wiring Diagram Control Loop for PV11 (PV10) and PV1 (PV2) 87-63432-4-73-ED-D Rev 11, (-74-ED-D Rev 11).
- Fuse Allocations: 87-55210-4-1-ED-B, Rev 03 (-5-1-ED-B Rev 03);
- Class I 48 VDC Distribution Flowsheet: 87-55212-2001-01-FS-F Rev 08.

5.3.3 EQUIPMENT

- MCR Handswitch (HS-77, HS-78):
  - type: 3 position, SCN 684L1340;
  - marking: CLOSE/AUTO/OPEN;
  - panel: 1-66110-PL-3;
  - location: S1-326 Main Control Room;
  - environmental qualification: none;
  - seismic qualification: Seismic Qualification of Instrument and Control Equipment, TS-XX-60000-005, Rev 2, 79/06/05.

- Logic relays:
  - type: 2C mercury wetted, SCN: relay 686N3353, module 686L0084;
  - panel: 63432-PL-115 (-PL-174), in module 41K (42M);
  - location: S1-328 Control Equipment Room;
  - environmental qualification: none;
  - seismic qualification: Seismic Qualification of Instrument and Control Equipment, TS-XX-60000-005, Rev 2, 79/06/05.

- Solenoid Valve:
  - type: Skinner Precision Industries Inc., Model A46HX6, SCN 545L6844, Note: existing valves are to be converted to Viton seals, as found;
  - panel: 1-63432-PL-1059 (-PL-1457);
  - location: S1-004 (S1-019);
  - environmental qualification: none;
  - seismic qualification: Seismic Qualification of Instrument and Control Equipment, TS-XX-60000-005, Rev 2, 79/06/05.

5.3.4 POWER SUPPLY

- Class I, 48 VDC.

  - Relay/solenoid valve circuits:
    - panel: 1-5521-PL-559, (-PL-560);
    - location: S1-328 Control Equipment Room;
    - environmental qualification: none;
    - seismic qualification: none.

5.3.5 TIMING SPECIFICATION

The time delay for relay RL-99K (RL-87M) is accounted for in the data sheet 1-63432, ECC Channelized Voting Logic Channels K and M.

- For opening PV11 (PV10):

  1) Solenoid valve: 15 ms.

  Total time delay: 15 ms.

5.3.6 ACCURACY SPECIFICATION

- None.

5.3.7 COMPONENT STATES

- Component's state when PV11 (PV10) is open:

  - Logic relay RL-99K (-87M), i.e. from ECC Channelized Voting Logic: energized.

- Component's state when the MCR handswitches are in the off normal position:

  - MCR handswitch HS-77 (HS-78) not in AUTO or MCR handswitches HS-73 (HS-74) not in OPEN and HS-77 (HS-78) not in CLOSE: open;

  - Annunciation relays RL-430K RL-431M: de-energized.

- Component's state when the SCA handswitches are in the off normal position:

  - MCR handswitches HS-75, HS-76 not in CLOSE: open;

  - Annunciation relays RL-430K RL-431M: de-energized.

5.3.8 SPECIFIC FUNCTIONS

1) The valve PV11 (PV10) is open if and only if:

   - ECC channelized voting logic is in the ECC trip state,

   and;

   - MCR handswitch HS-77 (HS-78) is in the AUTO position;

   or if:

- MCR handswitch HS-77 (HS-78) is in the OPEN position.

3) An audible alarm is given and the 66110-PL3 H. S. OFF NORMAL light is illuminated on panel PL-3 if:

   - the MCR handswitch HS-77 (HS-78) (i.e. dousing tank isolating valve PV11 (PV10)) is in the OPEN position;

   or if:

   - the MCR handswitch HS-77 (HS-78) (i.e. dousing tank isolating valve PV11 (PV10)) is in the CLOSE position,

   and;

   - the MCR handswitch HS-73 (HS-74) (i.e. recovery sump isolating valve PV1 (PV2)) is in the CLOSE position.