



**Pacific Gas and
Electric Company®**

James R. Becker
Site Vice President

Diablo Canyon Power Plant
Mail Code 104/5/601
P. O. Box 56
Avila Beach, CA 93424

805.545.3462
Internal: 691.3462
Fax: 805.545.6445

August 12, 2010

PG&E Letter DCL-10-099

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

Docket No. 50-275, OL-DPR-80
Docket No. 50-323, OL-DPR-82
Diablo Canyon Units 1 and 2

Response to NRC Request for Additional Information Regarding Diablo Canyon
Topical Report, "Process Protection System Replacement Diversity & Defense-in-
Depth Assessment"

- References:
1. NRC Standard Review Plan Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth In Digital Computer-Based Instrumentation and Control System," Revision 5, dated March 2007.
 2. PG&E Letter DCL-10-030, "Review of Diablo Canyon Topical Report, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment," dated April 9, 2010.

Dear Commissioners and Staff:

Pursuant to Reference 1, Pacific Gas and Electric Company (PG&E) requested in Reference 2 approval of the Diablo Canyon Power Plant (DCPP) Topical Report, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment," Revision 0.

On July 12, 2010, the NRC staff requested additional information required to complete the review of the DCPP Topical Report, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment," Revision 0. PG&E's responses to the staff's questions are provided in Enclosure 1.

PG&E is currently planning the replacement of the DCPP Eagle 21™ reactor trip system (RTS) and engineered safety feature actuation system (ESFAS) in 2014 for Units 1 and 2. PG&E plans to use the Invensys Tricon PLC Version 10



described in Reference 1 and the CS Innovations, LLC, Advanced Logic System for the Eagle 21™ RTS and ESFAS digital based instrumentation and control (I&C) replacement. The Reference 2 PG&E Topical Report contains the diversity and defense-in-depth assessment of the proposed Eagle 21™ RTS and ESFAS replacement. PG&E currently plans to submit a License Amendment Request for a digital upgrade of the DCPD Eagle 21™ RTS and ESFAS system by May, 2011.

The PG&E response to the staff request for additional information contained in Enclosure 1 contains information proprietary to PG&E. Accordingly, Enclosure 2 includes an affidavit signed by PG&E, the owner of the proprietary information. The affidavit sets forth the basis on which the information may be withheld from public disclosure by the Commission, and it addresses with specificity the considerations listed in paragraph (b)(4) of 10 CFR 2.390 of the Commission's regulations. PG&E requests that the PG&E proprietary information be withheld from public disclosure in accordance with 10 CFR 2.390. A nonproprietary version of the PG&E response to the staff request for additional information is contained in Enclosure 3.

Correspondence with respect to the proprietary aspects of the application for withholding related to the PG&E proprietary information or the PG&E affidavit provided in Enclosure 2 should reference PG&E Letter DCL-10-099 and be addressed to James R. Becker, Vice President, Pacific Gas and Electric Company, Diablo Canyon Power Plant, P. O. Box 56, Avila Beach, California 93424.

PG&E makes no regulatory commitments (as defined by NEI 99-04) in this letter. This letter includes no revisions to existing regulatory commitments.

If you have any questions, or require additional information, please contact Tom Baldwin at (805) 545-4720.

I state under penalty of perjury that the foregoing is true and correct.

Executed on August 12, 2010.

Sincerely,

James R. Becker
Site Vice President



kjse/4328 SAPN 50271918

Enclosures

cc: Gordon Clefton, Senior Project Manager, Nuclear Energy Institute
Diablo Distribution

cc/enc: Elmo E. Collins, NRC Region IV
Michael S. Peck, NRC, Senior Resident Inspector
Alan B. Wang, Project Manager, Office of Nuclear Reactor Regulation
Bill Kemper, NRC, Chief, Instrumentation and Controls Engineering Branch

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

_____)	Docket No. 50-275
In the Matter of)	Facility Operating License
PACIFIC GAS AND ELECTRIC COMPANY)	No. DPR-80
)	
Diablo Canyon Power Plant)	Docket No. 50-323
Units 1 and 2)	Facility Operating License
_____)	No. DPR-82

AFFIDAVIT

James R. Becker, of lawful age, first being duly sworn upon oath states as follows:

- (1) I am Site Vice President, of Pacific Gas and Electric Company (PG&E), and as such, I have been specifically delegated the function of reviewing the confidential information sought to be withheld from public disclosure in connection with nuclear power plant licensing and rulemaking proceedings, and am authorized to apply for its withholding on behalf of PG&E.
- (2) I am making this affidavit in conformance with the provisions of 10 CFR 2.390 of the Commission's regulations and in conjunction with the PG&E application for withholding accompanying this affidavit.
- (3) I have personal knowledge of the criteria and procedures utilized by PG&E in designating information as confidential.
- (4) Pursuant to the provisions of paragraph (b)(4) of 10 CFR 2.390 of the Commission's regulations, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.

In order to conform to the requirements of 10 CFR 2.390 of the Commission's regulations concerning the protection of proprietary information so submitted to the NRC, the information which is proprietary in the proprietary versions is contained within brackets, and where the proprietary information has been deleted in the nonproprietary versions, only the brackets remain. The information so designated as proprietary is indicated in both versions by means of a lower case letter "a" located as a superscript immediately following the

brackets. This lower case letter refers to the types of information PG&E customarily holds in confidence identified in this affidavit pursuant to 10 CFR 2.390(b)(1).

- (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by PG&E.
- (ii) The information is of a type customarily held in confidence by PG&E and not customarily disclosed to the public. PG&E has a rational basis for determining the types of information customarily held in confidence by it and, in that connection, utilizes a system to determine when and whether to hold certain types of information in confidence. The application of that system and the substance of that system constitutes PG&E policy and provides the rational basis required.

Under that system, information is held in confidence if the unauthorized disclosure, modification, or destruction of this information would adversely impact PG&E or could subject it to legal action and penalties. Generally, this information is intended for use only within PG&E and access to it is restricted to authorized individuals and entities. This information is considered confidential because it falls into one the following types:

- (a) Proprietary information is information in which PG&E has property rights which can be protected via a patent, a copyright, or other legal action as in the case of trade secrets.
- (b) A trade secret is information that: (1) derives independent economic value, whether actual or potential, from being unknown to the public in general or to persons who can obtain economic value from its disclosure or use, and (2) is the subject of efforts to maintain its secrecy that are reasonable under the circumstances. Examples include formulas and processes, designs, plans, and strategies, computer software and databases, methods and expertise that produce a desired result in a manner unknown to others in the trade ("know-how"), operational information, customer lists, and market information.
- (iii) The information is being transmitted to the Commission in confidence and, under the provisions of 10 CFR 2.390, it is to be received in confidence by the Commission.
- (iv) The information sought to be protected is not available in public sources or available information has not been previously employed in the same original manner or method to the best of our knowledge and belief.

- (v) The confidential information sought to be withheld in this submittal is that which is marked by lower case letter "a" in Enclosure 1.

This information addresses matters which will enable PG&E to license a digital upgrade of the reactor trip system and engineered safety features actuation system.

Further, this information has substantial commercial value. It consists of technical design details that support a robust design for a digital upgrade of the reactor trip system and engineered safety features actuation system. Use of the technical design details by a competitor would reduce their expenditure of resources in licensing a similar digital upgrade to the reactor trip system and engineered safety features actuation system.

Public disclosure of this confidential information is likely to cause substantial harm to the competitive position of PG&E because it would enable others to use the information to meet NRC requirements for licensing documentation for digital upgrades without purchasing the right to use the information.

The development of the design details for the digital upgrade of the reactor trip system and engineered safety features actuation system is the result of applying the results of many years of experience in an intensive PG&E effort and the expenditure of a considerable sum of money.

In order for competitors of PG&E to duplicate this information, similar technical design details would have to be developed and a significant manpower effort, having the requisite talent and experience, would have to be expended.

I state under penalty of perjury that the foregoing is true and correct.

Executed on August 12, 2010.

Sincerely,



James R. Becker
Site Vice President

Affidavit on behalf of Pacific Gas and Electric Company.
Affidavit consists of 3 pages total.

**PG&E Response to NRC Request for Additional Information Regarding
Topical Report, “Process Protection System Replacement Diversity & Defense-in-
Depth Assessment,” Revision 0**

NRC Question 1:

By letter dated April 9, 2010 (Agencywide Documents Access & Management System (ADAMS) Accession No. ML101100646), Pacific Gas and Gas and Electric Company (PG&E), the licensee for Diablo Canyon Power Plant, Unit Nos 1 and 2 (DCPP), requested approval of the DCPP Topical Report, “Process Protection System Replacement Diversity & Defense-in-Depth Assessment,” Revision 0 (LTR).

Section 2.3.2 of the LTR states that “The diverse ALS [Advanced Logic System] portion of the proposed replacement PPS [Process Protection System] is a logic-based platform that does not utilize a microprocessor and therefore has no software component required for operation of the system”. The staff understands that the FPGA [Field Programmable Gate Array] technology used does not utilize software during operation, however, it is also understood that software based development tools are used extensively during the design, implementation, and testing of these FPGA devices. Therefore, the characterization that no software component is required for operation of the system does not seem to be consistent with the actual system development lifecycle. Please provide clarification to this statement to include a discussion of the software that is relied upon for the design and development of the FPGA-based system.

PG&E Response:

The FPGA is a hardware realization of a logic structure; that is, it is a programmable hardware logic device. An FPGA-based system does not use software in the traditional sense when it is in operation; however, its logic structure is generated (i.e., it is “programmed”) in a manner similar to traditional software program development, with the same versatility and the same potential weaknesses.

The CS Innovations, LLC ALS application program development is structured to follow a traditional waterfall life cycle that includes a top-down requirement and specification development, design implementation, and a bottoms-up Verification and Validation (V&V) effort at each level of integration. The ALS program development utilizes proprietary software tools that have been subject to assessment and qualification. In-process quality assurance efforts are executed integral to the development stages, and a separate V&V team examines the outputs of each stage.

The CS Innovations tool assessment and qualification meets the intent of IEEE 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Section 5.3.2, Software Tools. The tool assessment and qualification ensures the proper tool is used for a particular activity in the Design Development Process. The tool assessment and qualification identifies how the output of a particular activity is assessed within the V&V activities, resulting in an independent verification of the tool output.

NRC Question 2:

Section 2.3.2 of the LTR states that “A software-related CCF that disables ALS protective functions is not considered credible...”. Because software based tools which could be susceptible to failure are utilized in the FPGA design and development process for all four protection sets, the staff considers that a software CCF could be credible in this case. Please provide additional information to support this claim or provide an explanation of how software based development tools which may have the potential to introduce faults into all protection sets will be accounted for in the PPS system design.

PG&E Response:

As noted in the response to Question 1, the software tools used in ALS development are assessed and qualified to meet the intent of IEEE 7-4.3.2. The tool assessment and qualification ensures the proper tool is used for a particular activity in the Design Development Process, and identifies how the output of a particular activity is assessed within the V&V activities, resulting in an independent verification of the tool output.

In addition, the section has been rewritten to better describe the measures taken to address software software common cause failure (CCF) in the ALS. The response to Question 6 addresses this concern.

NRC Question 3:

In Figure 2-8, a class I to class II isolation boundary is shown in the ALS block. The staff would like to have a better understanding of the nature of this boundary. Please provide a description of the components that comprise this isolation boundary and of how the electrical, physical, and data isolation characteristics of this boundary are achieved in the PPS system design.

PG&E Response:

The isolation functions shown in Figure 2-8 are performed by Class I components powered from Class 1 power sources. The “isolation section” shown in the subject figure can also be referred to as a termination area for the Class II signals.

Discussions with Westinghouse after the Diversity & Defense in Depth (D3) Assessment was submitted have led to simplification of the ALS scope, and the subject figure is being revised. The 4-20 mA (milliampere) process control and analog output signal isolation functions will be performed by qualified Class I isolation devices separate and independent from both the Tricon and the ALS, similar to what is shown for the anticipated transient without scram (ATWS) mitigation system actuation circuitry (AMSAC) signals. Reactor coolant system (RCS) flow signals will be isolated by the ALS due to the requirement to normalize the scaling periodically. Refer to Figure 1 in this Enclosure.

Additional information is provided in the response to Question 4.

NRC Question 4:

Figure 2-8 shows an input line titled "Process Inputs (4-20 mA)" that provides input to the TRICON system, the ISLN system and the ALS system. Please provide additional details on these input signals. The staff would like to have a better understanding of what these signals are as well as how and why these signals are shared among the systems.

PG&E Response:

The depiction of the input signals in Figure 2-8 is conceptual.

The "Process Inputs" are the analog input signals that are used to perform the required trip and actuation protection functions. These include RCS flow, steam generator level, pressurizer level and pressure, containment pressure, steamline pressure, etc. Refer to Figure 1 in this Enclosure, which clarifies Figure 2-8.

The pressurizer pressure signal is used by the ALS to generate the diverse pressurizer pressure high and low trips and the pressure-low safeguards functions. It is also input to the Tricon because it is used to calculate the Overpower Delta T (OPDT) Overtemperature Delta T (OTDT) trip setpoints. Since the signals are shared at the transmitter (4-20 mA analog) output, a failure in either ALS or Tricon cannot affect the other. AMSAC shares steam generator level and turbine impulse pressure with the Tricon. The signals are shared at the transmitter (4-20 mA analog) output and meet 10 CFR 50.62 diversity requirements. A Tricon failure cannot affect the AMSAC and an AMSAC failure cannot affect the Tricon.

The D3 Assessment explains that the ALS will also provide Class IE signal conditioning for the RCS narrow range resistance temperature detector (RTD) inputs to the OPDT and OTDT thermal trip functions due to its improved ability to process 200 ohm RTD inputs. Otherwise, it would be necessary to provide dedicated, individual signal conditioners, use of which creates issues in meeting Westinghouse specifications for stability and accuracy. The temperature information is not used by the ALS to perform safety functions and is passed from the ALS to the Tricon via analog signals to address concerns regarding software-based communication between redundant or diverse processors. The ALS provides additional benefits such as self-diagnostics, which individual isolators do not. The Nuclear Instrumentation System (NIS) provides diverse automatic protection should a failure in either the ALS or Tricon disable the OPDT and OTDT trip functions.

NRC Question 5:

Figure 2-8 shows a Class II Data link to the process plant computer. The staff would like to have a better understanding of the nature of this Class I to Class II boundary. Please provide a description of the components that comprise this isolation boundary and of how the electrical, physical, and data isolation characteristics of this boundary are achieved in the PPS system design.

PG&E Response:

The current concept for connecting the Class I Tricon and ALS to the Class II Plant Process Computer (PPC) and workstation was developed after the first Process Protection System (PPS) replacement Phase Zero meeting based on feedback from NRC. However, the concept

is not fully developed at this time, and may change as the Tricon and ALS designs develop. As currently envisioned, the ALS data link isolation function is performed by the Class I ALS Communications Board. The ALS link to the PPC Gateway computer is one-way. It broadcasts data to the Class II PPC Gateway, which is common to all four protection sets, and does not receive any data or instructions from the PPC Gateway.

The Tricon will be isolated from the PPC Gateway by a qualified Class I Triconex Communications Module (TCM). Fiber optic cable electrically isolates the Tricons from external Class II devices. An additional data isolation device such as a network port aggregator tap permits two-way communications between the Maintenance Video Display Unit (MVDU) belonging to a specific protection set and the Tricon in that protection set, yet ensures only one-way communication to the PPC gateway.

NRC Question 6:

The inherent internal diversity of the ALS system is referenced and relied upon throughout the LTR as a means of addressing the diversity requirements for the three events requiring exception as described in section 1.0 of the LTR. The approval of the Wolf Creek MSFIS [Main Steam and Feedwater Isolation System] SER [Safety Evaluation Report] is referenced in section 2.3.2 as a basis for this inherent internal diversity, however, the Wolf Creek SER points out that the safety determination was specific to the MSFIS design and that future more complex uses of the ALS platform, such as for a system receiving sensor signals and making trip or actuation determinations may require additional design diversity. As this appears to be the case for the proposed PPS, the staff requests that the applicant provide a description of any additional design diversity measures that are being taken for the PPS system to ensure that this inherent internal diversity will meet the requirements of Interim Staff Guidance (ISG) Number 2, issue 5, staff position 1.

PG&E Response:

The MSFIS SER states that it is a unique application, and that "... future ALS applications, such as a reactor protection system (RPS) or engineered safety feature actuation system (ESFAS) that receives input signals and makes trip decisions, may require additional design diversity such as independent development of diverse application code for each core."



Concern for ALS software CCF is addressed by incorporating additional design diversity within a hardware system using qualified design practices and methodologies to develop and implement the hardware. Therefore, the proposed PPS provides sufficient diversity to adequately address Staff Position 1 of ISG-02 without operator action.

Westinghouse is expected to provide the detailed information necessary for NRC to determine that the ALS possesses adequate design diversity in the ALS Topical Report. Additional information is provided in the response to Question 8.

A revision to Section 2.3.2 of the D3 Assessment is as follows:

“... future ALS applications, such as an RPS or ESFAS that receives input signals and makes trip decisions, may require additional design diversity.

Concern for ALS software CCF is addressed through incorporating additional design diversity in the FPGA based hardware system and using qualified design practices and methodologies to develop and implement the hardware. The diverse ALS cannot be affected by a CCF that affects the Tricon. The proposed PPS provides sufficient design diversity to automatically mitigate Diablo Canyon Final Safety Analysis Report Update (FSARU) Chapter 15 events where previous evaluations credited operator action should a CCF occur concurrent with the event. Therefore, the proposed design addresses Staff Position 1 of ISG-02 adequately.”

NRC Question 7:

The discussion in the second paragraph of section 2.0 of rack sets, redundant process channels, and logic racks (trains) is confusing. The only definition provided is for Process Channel. Please provide definitions for each of these terms as well as a clear description or illustration of how these separation schemes are applied to the PPS architecture.

PG&E Response:

Section 2.0 of the D3 Assessment has been rewritten to include definitions of the protection set and logic train and a more detailed architecture description.

The protection system is designed to provide two, three, or four process channels for each protective function and redundant (two) logic trains, as shown in Figure 2-1. Each individual process channel is assigned to one of four channel designations, e.g., Channel I, II, III, or IV. Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each separate channel.

Redundant process equipment is separated by locating electronics in different protection rack sets. The four separate and redundant PPS rack sets (i.e., “Protection Sets”) are comprised of Protection Racks 1-16.

Separation of the redundant process instrumentation channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and process protection racks

and then to the four solid state protection system (SSPS) input chassis of the two redundant SSPS logic racks ("Trains").

A protection set is defined as a physical grouping of process channels with the same channel designation. Each of the four redundant protection sets is provided with a separate and independent power feed and process instrumentation transmitters. Thus, each of the four redundant protection sets is physically and electrically independent from the other sets [FSARU Section 7.2].

A logic train is defined as one of the two sets of equipment that comprise the SSPS. As shown in Figure 2-1, each of the two redundant and independent SSPS logic trains contains a logic cabinet and four separate input cabinets that receive trip signals from the PPS. Electronics in the logic cabinets perform coincident logic functions that actuate reactor trip and engineered safety system equipment based upon the PPS trip signals.

NRC Question 8:

The last sentence in section 2.3.1 correctly states that Triconex has submitted an updated platform LTR which is currently under review by the NRC staff. Please state if the proposed PPS system will be based upon the Version 10 Tricon system or if the PPS system will be based upon the previous approved version of Tricon. If version 10 is to be used, then completion of the safety evaluation for this LTR under review would be required prior to approval of the proposed PPS system.

PG&E Response:

The proposed PPS system will be based upon the Version 10 Tricon system. PG&E understands that approval of the Triconex Version 10 Topical Report is required before the proposed PPS can be approved. PG&E suggests that the Safety Evaluation Report (SER) for the D3 Assessment be issued conditionally; that is, pending successful safety evaluations for the Version 10 Tricon system Topical Report and the ALS Topical Report. Additional information on the ALS design is provided in the response to Question 6.

Figure 1 PPS Concept Architecture

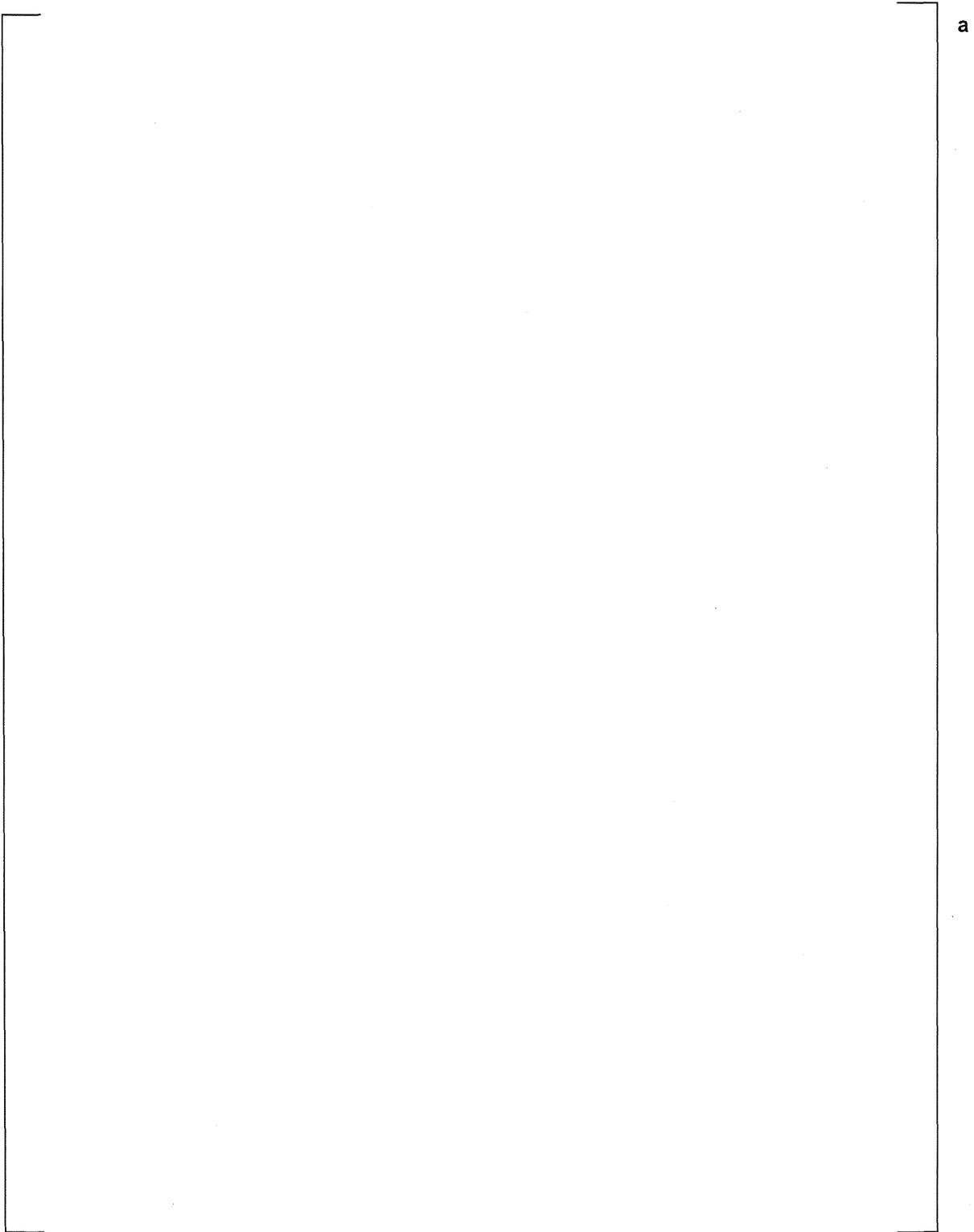


Figure 2 ALS Inherent Diversity Architecture

