KAPL, Inc.
Knolls Atomic Power Laboratory
Post Office Box 1072 Schenectady, N.Y. 12301-1072
Telephone (518) 395-4000 Facsimile (518) 395-4422

LOCKHEED MARTIN

SPP-67610-0008
October 20, 2005
Page 1

The Manager
Schenectady Naval Reactors Office
United States Department of Energy
Schenectady, New York

Subject: Space Power Program, Instrumentation and Control System Architecture, Preconceptual Design, for Information (U)

References: See page 7.

Enclosures: See page 7.

Dear Sir:

Purpose:
The purpose of this letter is to forward the Prometheus preconceptual Instrumentation and Control (I&C) system architecture (Enclosure (1)) to NR for information as part of the Prometheus closeout work.

Summary:
The preconceptual I&C system architecture was considered a key planning document for development of the I&C system for Project Prometheus. This architecture was intended to set the technical approach for the entire I&C system. It defines interfaces to other spacecraft systems, defines hardware blocks for future development, and provides a basis for accurate cost and schedule estimates. Since the system requirements are not known at this time, it was anticipated that the architecture would evolve as the design of the reactor module was matured.

The reference architecture (See Figure 1) was selected from several different alternatives for its relative simplicity and fault tolerance. The selected architecture uses a 3-layer approach consisting of a supervisor, reactor controller, and actuators. Redundancy is implemented differently in each layer to achieve system fault tolerance:

Supervisor: Three Supervisor Channels, configured in a Hot/Warm/Cold or a Hot/Warm/Warm configuration, are used to provide overall system control. The Supervisor Channels perform the following functions:

- Collect diagnostic data from the Reactor Controller Channels and send this to the spacecraft flight computer for telemetry.
- Distribute and coordinate software upgrades.
- Monitor the Reactor Controller Channels and determine any changes in coincidence for output control that should be used, and communicate this coincidence change to the Slider Controllers.

Reactor Controller: Four Reactor Controller Channels in a channel coincidence configuration provide sensing and control of the reactor. The Reactor Controller Channels perform the following functions:

- Monitor plant parameters via sensors and interface cards.
- Provide control actions to maintain the reactor in proper control bands.
- Provide telemetry data back to the Supervisor Channels.
- Provide and receive data directly to/from the Power Conditioning and Distribution (PCAD) system for command and monitoring purposes.

Sensors and interface cards are provided to measure temperature, pressure, flow, position of reactivity and flow control devices (sliders, valves, and safety rod(s)), and neutron flux. These sensors were chosen to provide the necessary parameters for reactor plant control and handling of reactor plant casualties. In all cases except for continuous slider position indication, and discrete position sensors (sliders, valves, and safety rod(s)), there is an independent set of sensors for each Reactor Controller Channel to maintain channel independence and resilience to sensor failure.

During normal operation all four Reactor Controller Channels are operating. The Reactor Controller Channels monitor sensor inputs, execute algorithms, and send outputs through coincidence circuits to control the sliders. Bi-directional data links connect the Reactor Controllers to the Supervisor Channels and to the PCAD system. The PCAD system controls both the speed of the Brayton machine(s) and circuit breakers in the electric plant.

Actuators: There are twelve independent slider control channels, each corresponding to one of the twelve (assumed) sliders used for reactivity control. The Slider Controllers have the following functions:

- Apply coincidence logic to the Reactor Controller Channel outputs to determine if a slider should be moved.
- Control the slider's motion by controlling a three phase stepper motor drive.
- Interface with slider position sensors to determine slider position.
- Detect potential errors and communicate errors as well as slider position, error, fault, and status information back to the Reactor Controller Channels.

Separate controllers are provided for actuation of valves (if needed) and the safety rod(s). These controllers are redundant to provide single fault tolerance. These controllers provide both actuation and position feedback.

The selected architecture can be implemented with approximately 45 circuit cards and a total mass of approximately 320kg including sensors, cables, and electronics.

Background:
The NRPCT developed a notional I&C system architecture, defined in Enclosure (4), to provide a basis for developing project planning estimates for manpower and hardware development. The notional I&C system architecture was intended to be evolved as mission and system requirements were developed. As the project continued, trade studies were identified to begin the refinement of salient architecture features. The preconceptual I&C system architecture (Enclosure (1)) selected is the result of 9 trade studies performed on I&C system attributes and applied to the notional architecture. Enclosure (3) discusses the basis for the trade studies. The notional architecture provided the basis for Reference (a), which documents the Space Reactor Planning Estimate – Basis for Estimate. Included as part of Reference (a) is the circuit card and card rack summary and the sensor cost summary, which were used to provide cost estimates and assumptions for the preconceptual I&C system architecture as well as the trade studies.

The notional architecture provided a basis for project planning and for discussions with other spacecraft design agents to develop interface specifications between the Reactor I&C Segment and the Command & Data Handling and Power Conditioning & Distribution subsystems.

The basic aspects required to fully specify an I&C system are:

- Sensors/Interfaces
- Actuators
- Monitoring and Control Algorithms
- Design Events
- Required Fault Tolerance.

The I&C system sensors and actuators are considered to be sufficiently defined for the selection of the preconceptual I&C system architecture. Although a monitoring and control scheme is not defined at this time, key plant parameters forming the basis of candidate control schemes are sufficiently defined and included in this preconceptual I&C system architecture. The computational nodes within the I&C architecture are identified herein but the specific monitoring and control algorithms would have been specified in the next design phase. Algorithm development would not be anticipated to impact the I&C system architecture as a basis set of information (plant sensors) required by the algorithms is provided.

The preconceptual I&C system architecture is considered to support all potential control strategies for the reactor plant, including a control band strategy. The control strategies would be specified in a future design phase. In a control band strategy, the following must hold true:

- The control band must be greater than the total accuracy of the controlling parameter's sensor.
- The margin between the design limits and the control band limits must be greater than half of the total sensor accuracy of the controlling parameter(s).

The above two requirements result in a parameter (e.g., coolant temperature) design limit range that is greater than twice the total instrumentation accuracy. For example, if the instrumentation error is +/- 5K (total instrumentation accuracy is 10K), the control band must be greater than 10K and the design limit range must be greater than 20K. This range applies to either single channel or multiple channels with coincidence architectures. Therefore, accuracy and control band were not determining factors in the architecture selection. However, the impact on the system parameter design range and feedback on plant component sizing emphasizes the need to minimize instrumentation errors in any control architecture.

The preconceptual reactor design concept has sufficient reactivity margin for design lifetime with a single slider fully inserted or fully withdrawn as established in Reference (b) and it is a goal to maximize power capability with this condition. The design of the preconceptual I&C system architecture for the Prometheus project postulated that slider casualties (including mechanical failures such as a stuck or frozen slider) are credible design events. Therefore, the I&C system must be designed to preclude multiple slider casualties originating from a single failure in the I&C system. A single slider casualty may require actuation of the remaining 11 sliders in response to the reactivity transient. This design event drove the preconceptual I&C system design toward single slider control, as well as single valve control (if isolation valves are required). It is anticipated that additional design events, such as casualties emanating from the Energy Conversion Segment, Heat Rejection Segment, or single event upsets (SEUs) in electronic components, should be identified in the future but will only impact the algorithms (system requirements) and not impact the preconceptual I&C system architecture. The single failure criterion was a major design driver and was considered to provide sufficient fault tolerance in the preconceptual I&C system.

Discussion:
The I&C system architectures described in Enclosures (1), (4), and (5) are considered to be preconceptual. In some cases, design details are given for illustrative purposes only. Specific design details would be evaluated during the design phase of the project. The trade studies listed herein (Enclosures (6) through (14)) encompass some (but not all) of the evaluations needed to achieve a robust control system which would ensure continuity of reactor power to the spacecraft's energy conversion system. Enclosures (4) through (15) are summarized as follows:

- Enclosure (4) describes the notional architecture. The notional architecture was the planning baseline for Reference (a). The notional architecture uses four hot reactor controller channels to control the slider controllers based on independent sensor inputs. The supervisor channels are in a hot/warm/cold configuration and are used to perform diagnostic testing and pass telemetry data to ground control. The notional architecture uses a separate coincidence logic module as well as coincidence within each slider controller to pass commands from the reactor controller channels. The design of the notional architecture does not require microcontrollers for coincidence, but is flexible enough to include them if desired.

- Enclosure (5) describes Architecture 2. This is an evolution of the notional architecture documented in Enclosure (4) based on the outcomes of the trade studies. Some advantages of Architecture 2 over the notional architecture are as follows:
  - Utilizes bidirectional serial interfaces for communication between architecture layers, to improve reliability, extensibility, diagnostics, and allows for remote software upgrades at all levels of the architecture.
  - Eliminates an architecture "layer" by performing coincidence at the slider and valve controllers instead of using a separate layer for coincidence. This results in fewer interconnections, improved response time, and a lower card count.
  - Made several changes to improve fault tolerance (e.g., utilizing more "point-of-use" power supplies, providing improved separation of slider indication circuitry), while reducing card count, cost, and system mass.

- Enclosure (6) provides the result of a comparison trade study for a secondary electronics vault. It shows that implementing a secondary electronics vault closer to the reactor, for the purpose of multiplexing signals to reduce cable mass, is not practical. The increase in mass for shielding the secondary vault outweighs the increase in cabling required without multiplexing signals.

- Enclosure (7) evaluates the pros and cons of one power supply versus two power supplies used in each Reactor Controller Channel (RCC) and each Reactor Supervisor Channel (RSC). The trade study recommends using one power supply per Reactor Controller Channel, and one power supply per Supervisor Channel if the probability of failure of a power supply card is not much greater than other cards.

- Enclosure (8) evaluates the use of three bus options for communication within card racks. Versa Module Eurocard bus (VMEbus) is traded against Compact Peripheral Component Interface bus (cPCI bus) and against using a serial data bus. The three options trade commonality, numbers of cards allowed per card rack, flexibility, and bandwidth. This trade study recommends using the cPCI bus due to the advantages associated with using common hardware and should mitigate any bandwidth concern.

- Enclosure (9) evaluates using discrete or serial data links for communication between reactor controller channels and coincidence logic. Using serial links provides more mass savings, flexibility, and extensibility to the system. The same trade also evaluates the pros and cons of locating coincidence logic on a separate card or integrating it with the slider or drum controllers. This trade study concluded that serial data links had more pros than discrete data. This trade study found the two options to be approximately equal in terms of pros and cons for the location of the coincidence logic.

- Enclosure (10) evaluates using two slider motor windings versus using a single motor winding. The outcome of this trade centers around differences in architecture for the two options and an increase in fault tolerance is traded with increased mass, cost, and volume. This trade study found the two options to be approximately equal in terms of pros and cons for the use of two slider motor windings and using a single motor winding.

- Enclosure (11) evaluates the advantages and disadvantages of implementing a single control tier versus two control tiers for reactor supervisors and reactor controllers. It also evaluates the advantages and disadvantages of using the spacecraft flight computer as the reactor module's supervisor instead of having a separate supervisor computer within the reactor module. The trade for a single control tier provides savings in mass, cost, and volume with the possible decrease in fault tolerance and reliability. This trade concluded that using a two control tier has more advantages than using a single control tier.

- Enclosure (12) evaluates the advantages and disadvantages of the slider controller level of programmability. Designing the slider controllers to have the capability of software modification post launch could provide more system flexibility. Designing a system that does not allow modification of software may provide less fault tolerance, but the deletion of programming circuitry may offset this disadvantage and may increase system reliability. This trade was inconclusive and further evaluation would need to be done for future missions.

- Enclosure (13) evaluates the advantages and disadvantages for having independent Reactor Controller Channels (RCCs) versus cross-connecting the RCCs. Cross-connected channels may have more fault tolerance, but with an increase in complexity. This trade study found the two options to be approximately equal in terms of pros and cons for the use of cross-connected channels and independent channels.

- Enclosure (14) evaluates three options for a reactor controller channel redundancy configuration including one hot backup channel, one cold backup channel, and no backup channels. An increase in backup channels may increase fault tolerance, and reliability while sacrificing simplicity, mass, cost, and volume. This trade study concluded that having a hot backup channel had more pros than the other options.

- Enclosure (15) documents the formal decision process followed and the conclusions reached. The decision process was performed on the notional architecture (Enclosure (4)) against Architecture 2 (Enclosure (5)), and also against cross-connected versions of each architecture as described in Enclosure (13).

Conclusion:

A decision process was performed rating the notional architecture against Architecture 2, and also against cross-connected versions of each architecture. Architecture 2 rated the most favorable in reliability and cost, and was tied for the best rating in other categories such as mass, flexibility, extensibility, simplicity, testability, response time, and troubleshooting. Following the decision process, Architecture 2 was modified to include more operational detail for the configuration management, valve and safety rod control systems, and other minor changes. This version of Architecture 2 was renamed to be the preconceptual I&C system architecture and, as described in Enclosure (1), is the architecture selected for further evaluation for a deep space nuclear propulsion mission extensible to surface missions.

Future Work:
Future trade studies that would be required if this space reactor work is resumed are outlined in Enclosure (3). Additional trades would need to be performed to support a future submittal of a final architecture once mission requirements are developed and the reactor and plant designs are sufficiently mature. These include, but are not limited to:

- Impact of sensor accuracy on control band
- Multiple position sensors vs. a Single position sensor per slider actuator
- Continuous or Step control for Slider/Drum actuation
- Static versus Dynamic Slider/Drum selection
- Asynchronous versus Synchronous Communication
- Two channel versus three channel Coincidence Logic
- Hot/Warm/Cold versus Hot/Warm/Warm Supervisor Channel Configuration
- Separation of Control versus Limitation Functions

The most significant of these is the Separation of Control versus Limitation Functions trade study. This trade study would evaluate the advantages and disadvantages of a system architecture that uses the Supervisor Channel for operational control of the sliders and uses the Reactor Controller Channels (with coincidence) to provide a protective (limiting) action with the sliders to maintain the plant within operating limits. All architectures considered during the KT (described in Enclosure (15)) combined control and limitation functions in the Reactor Controller Channels. Potential advantages of separating the control and limitation functions are:

- Provides functional diversity mitigating common mode failures by providing a second echelon which must be breached before a loss of mission occurs.
- Simplifies individual single slider selection for control due to removal of coincidence.
- Simplifies the application of coincidence logic to limitation actions since it is only applied to slider movement and not slider selection if bank slider motion is used.

A major disadvantage is that a separate set of Reactor plant sensors would be required, which increases mass of the system.

Requested Action:
This letter is provided to NR for information. No NR action is requested.

Concurrence:
This letter and its enclosures have been reviewed and concurred to by the Manager of KAPL SPP Space Electrical Systems (K. Loomis), the Manager of KAPL Space Power Plant Systems (H. Schwartzman), the Manager of KAPL Space Energy Conversion (J. Ashcroft), the Manager of KAPL Space Reactor Engineering (D. McCoy), the Manager of Bettis Space Reactor Engineering (C. Eshelman), the Manager of Bettis Space Plant Systems (D. Hagerty) and the Engineering Manager of BPMI-P Technical Assurance and Development Department (S. Gazarik).

Very truly yours,

Jessica Ross

Jessica N. Ross, Engineer
Space Electrical Systems
Space Power Program

Approved by:

Matthew Ryan

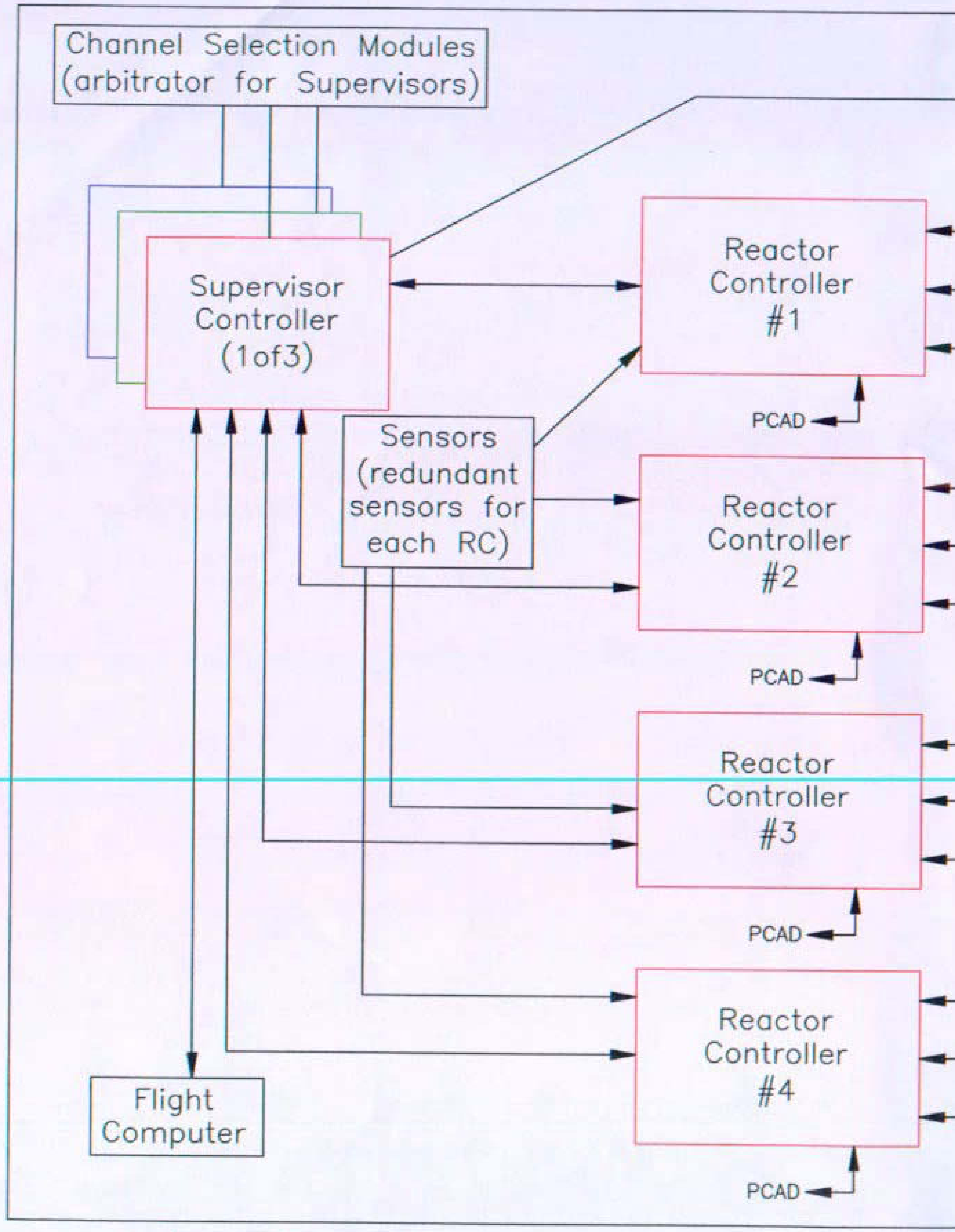
Matthew Ryan, Manager
Space Electrical Systems-Systems and Software Design
Space Power Program

References:

(a) SPP-67610-0003 Space Reactor Planning Estimate – Basis for Estimate, dated 20 May 2005
(b) SPP-67410-0008 Space Reactor Program, Pre-Conceptual Prometheus Space Reactor Nuclear Design Basis, for NR Information, dated 30 June 2005

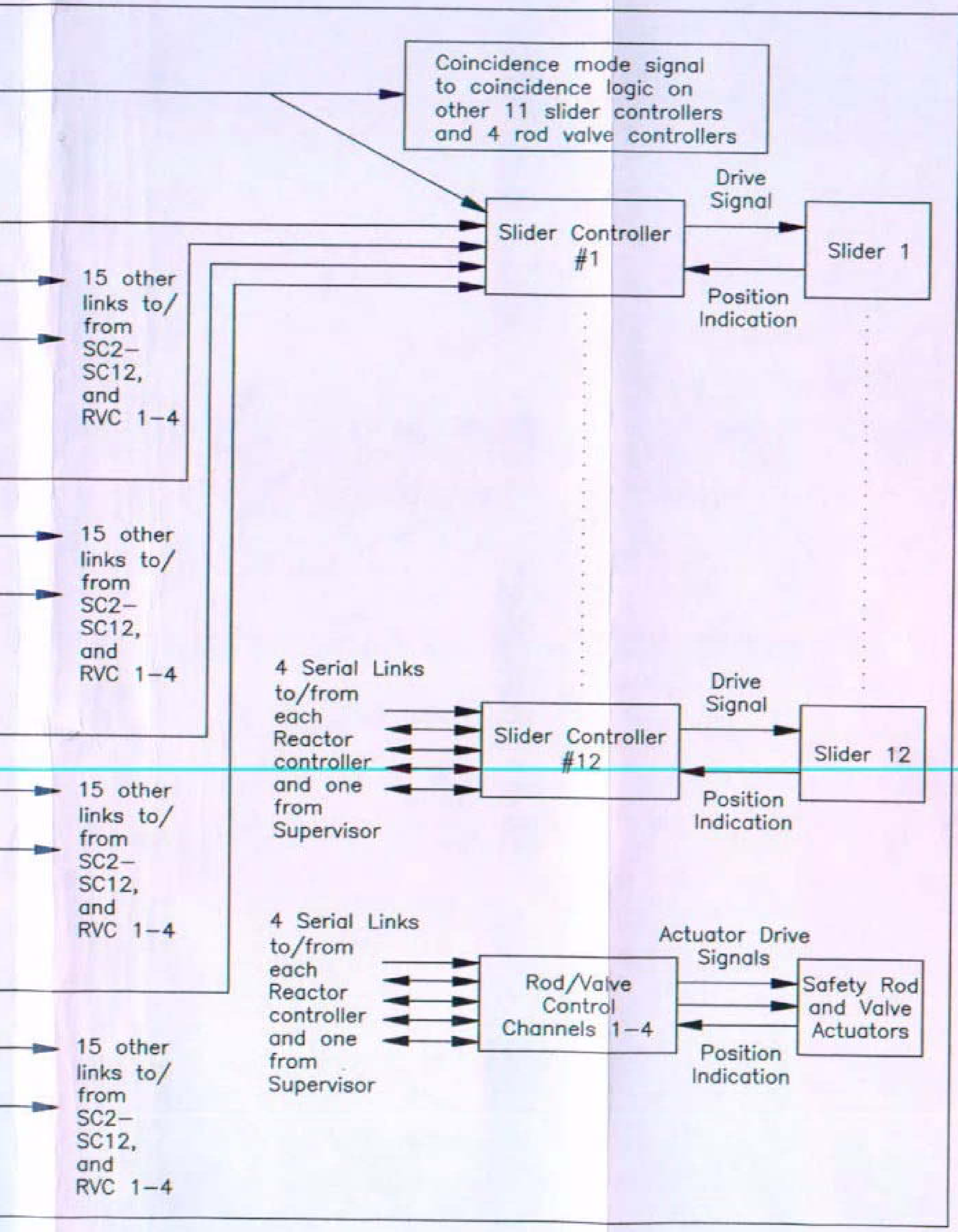
Enclosures:

(1) Preconceptual I&C System Architecture, dated 9/28/05
(2) Assumptions
(3) Definitions of Terms and Basis for Trades
(4) Notional Architecture
(5) Architecture 2
(6) Comparison Study for a Secondary Electronics Vault
(7) Reactor Controller and Supervisor Power Supply Trade Study
(8) Data Bus Evaluations for Space I&C Reactor Instrumentation & Control System
(9) Discrete versus Serial Communication with Coincidence Logic and Coincidence Logic Location Trade Study
(10) Single Winding versus Dual Winding Trade Study
(11) Single versus Two I&C Control Tiers Trade Study
(12) Slider Controller Programmability Trade Study
(13) Cross-Coupled Channels vs. Independent Channels Trade Study
(14) Reactor Controller Architecture Trade Study
(15) Kepner Tregoe (KT) Evaluation Process



Key:
Red— Hot
Green— Warm

Figure 1: Preco
Arc



nceptual I&C System
hitecture

CONCURRENCE/DESIGN CHECK FORM FOR DOCUMENT NO. SPP-67610-0008 **Date:** 10/20/05

DOCUMENT TITLE: Space Power Program, Instrumentation and Control System Architecture, Preconceptual Design, for Information (U)

REFERENCES See cover sheet

ENCLOSURES: See cover sheet.

1. ADSARS: PERMANENT RECORD: Yes X No ___ Repository MFLIB Corporate Author: KAPL NR PROGRAM K

Key Words: Prometheus, I&C, NRPCT, Instrumentation and Control

Need to Know Categories REP

Available Sites: PRNR

Design File Location(s)

2. DESIGN CHECK

Type of Check	Signature(s)	Comments: (Including Reference to Check Document If Appropriate)
A. No check considered necessary		
B. Check vs. previous results/issues		
C. Checked calculations made		
D. Checked computer input and/or output		
E. Computer Programs approved/qualified		
F. Performed independent audit		
G. Spot checked significant points		
H. Reviewed methods used	Allen Terrill	
I. Reviewed results for reasonableness		
J. Comparison with test data		
K. Reviewed vs. drawings		
L. Verified procedures		
M. Technical content reviewed	Allen Terrill	
N. Management verification of adequate review by others		
O. Performed Lessons Learned Search		
P. Used Measurement Uncertainty Methods		
Q. Other Checks (Describe)		

3. CONCURRENCE REQUIREMENTS: Indicate signatures required by X:

	SPP MANAGER		ADVANCED CONCEPTS		FLUID DYNAM
X	NUCLEAR ENGINEERING		SHIELDING		STRUC. ENGRG
	REACTOR TH/MECH DESIGN		REACTOR SAFETY		DRAFTING
	REACTOR EQUIPMENT		TO		QA
X	SPP MECHANICAL		RSO		OTHER
X	SPP ELECTRICAL		FSO	X	BETTIS
	FINANCE		MDO	X	BPMI
	PROJECT OFFICE		ARP	X DRS	ADMIN REVIEW
X	ENERGY CONVERSION				

Cognizant Manager ______________
(Must Be Subsection or Higher for External Letters)

4. AUTHORIZED CLASSIFIER: Reviewed By: ______________ CLASSIFICATION: UNCLASSIFIED

5. RELATED SUBJECTS:

UTRS Implication (Y/N) N

Safety Council Review (Y/N) N

Commitment Made (Y/N) N

Design Basis Info. (Y/N) N

Design Review (Y/N) N

Commitment Complete (Y/N) N

UTRS Doc. # N/A

6. Distribution:

NR	Bettis
S. Bell, 08I/8024	CD Eshelman, 36E/SE JR for CE per telecon, 10/20/05
MW Henneberger, 08K/8026, for Information	D. Hagerty, 38D/SE JR for DH per telecon, 10/20/05
SJ Kurth, 08K	M. Zika, 01C/SE
JP Mosquera, 08C/8017	D. Robare 38D/SE JR for DR per telecon, 10/20/05
CH Oosterman, 08C/8017	
	BPMI-P
KAPL	SD Gazarik JR for SG per telecon, 10/20/05
JM Ashcroft *, 132 JR for JA per telecon, 10/20/05	RF Hanson
PF Baldasaro *, 111	
CF Dempsey *, 93	
KC Loomis *, 132	**PNR**
DF McCoy *, 111 JR for DM per telecon, 10/20/05	J. Andes
H. Schwartzman *, 132 JR for HS per telecon, 10/20/05	JF Koury
SA Simonson *, 92	
MJ Wollman *, 111	**BPMI-S**
MJ Ryan *, 132	F. Barilla*
JN Ross, 132	
AA Terrill, 132	
JW Meredith, 132	
EG Johnson *, 132	
JA Boyle *, 132	
TA Hamilton *, 028	
AK Rice *, 132	
DA Schroeder *, 026	
BM Robinson *, 026	
CP Richardson *, 132	
MR Corcoran *, 132	
JM Sempsrott *, 132	
SNR	
D. Clapper, 065	
H. Miller, 065	
GM Millis, 065	RECEIVED NOV 1 2005 M.J. WOLLMAN

* Cover letter only.