March 25, 2008

Mr. Keith Paulson
Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146

SUBJECT: MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC. - REQUEST FOR ADDITIONAL INFORMATION ON US-APWR TOPICAL REPORT MUAP-07006-P, "DEFENSE-IN-DEPTH AND DIVERSITY"

Dear Mr. Paulson:

By letter dated July 3, 2007, Mitsubishi Nuclear Energy Systems, Inc. (MNES) submitted for NRC staff review Topical Report MUAP-07006-P, "Defense-in-Depth and Diversity." The NRC staff has reviewed this topical report and has determined that the following information is needed for the NRC staff to complete its review. The NRC staff plans to schedule a non-public (proprietary) meeting with MNES in order to discuss the response to this request for additional information.

Sincerely,

/RA/

Stephen Raul Monarque
USAPWR Projects Branch
Division of New Reactor Licensing
Office of New Reactors

Docket No. 52-021

Enclosure: As stated

cc: See next page

Mr. Keith Paulson
Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146

SUBJECT: MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC. - REQUEST FOR ADDITIONAL INFORMATION ON US-APWR TOPICAL REPORT MUAP-07006-P, "DEFENSE-IN-DEPTH AND DIVERSITY"

Dear Mr. Paulson:

By letter dated July 3, 2007, Mitsubishi Nuclear Energy Systems, Inc. (MNES) submitted for NRC staff review Topical Report MUAP-07006-P, "Defense-in-Depth and Diversity." The NRC staff has reviewed this topical report and has determined that the following information is needed for the NRC staff to complete its review. The NRC staff plans to schedule a non-public (proprietary) meeting with MNES in order to discuss the response to this request for additional information.

Sincerely,
/RA/
Stephen Raul Monarque
USAPWR Projects Branch
Division of New Reactor Licensing
Office of New Reactors

Docket No. 52-021

Enclosure: As stated

cc: See next page

DISTRIBUTION:

PUBLIC		
NMIP R/F	RidsNroPMJCiocco	JDonoghue, NRO
RidsNroPMSMonarque	RidsRGN2MLesser	TFord, NRO
RidsOgcMailCenter	RidsNroPMJChung	JBongarra, NRO
LBurkhart, NRO	RidsNroDsraSRSB	RBeacom, NRO
RidsNroLAPCoates		

ADAMS ACCESSION No. ML080790297 NRR-088

OFFICE	DNRL/NMIP/PM/jnt	NRO/DNRL/NMIP/LA	NRO/DNRL/NMIP/BC
NAME	SMonarque	PCoates	LBurkhart
DATE	03/25/2008	03/ 25 /2008	03/ 25 /2008

OFFICIAL RECORD

DC Mitsubishi - US APWR Mailing List (Revised 03/18/2008)

cc:

Mr. Glenn H. Archinoff
AECL Technologies
481 North Frederick Avenue
Suite 405
Gaithersburg, MD 20877

Ms. Michele Boyd
Legislative Director
Energy Program
Public Citizens Critical Mass Energy
and Environmental Program
215 Pennsylvania Avenue, SE
Washington, DC 20003

Mr. Ray Ganthner
Senior Vice President
AREVA, NP, Inc. 3315
Old Forest Road
P.O. Box 10935
Lynchburg, VA 24506-0935

Mr. Paul Gaukler
Pillsbury, Winthrop, Shaw, Pittman
2300 N Street, NW
Washington, DC 20037

Masayuki Kambara
Mitsubishi Nuclear Energy Systems, Inc.
2300 Wilson Blvd.
Suite 300
Arlington, VA 22201-5426

Masahiko Kaneda
Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-Chome, Minato-Ku
Tokyo, 108-8215 JAPAN

Shinji Kawanago
Mitsubishi Nuclear Energy Systems, Inc.
2300 Wilson Blvd.
Suite 300
Arlington, VA 22201-5426

Sirirat Mongkolkarn
Office Administrator
Mitsubishi Nuclear Energy Systems, Inc.
2300 Wilson Boulevard, Suite 300
Arlington, VA 22201-5426

Dr. Masanori Onozuka
Mitsubishi Nuclear Energy Systems, Inc.
2300 Wilson Blvd.
Suite 300
Arlington, VA 22201-5426

Dr. C. Keith Paulson
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146

Mr. Robert E. Sweeney
IBEX ESI
4641 Montgomery Avenue
Suite 350
Bethesda, MD 20814

Mr. Ed Wallace
General Manager - Projects
PBMR Pty LTD
P. O. Box 9396
Centurion 0046
Republic of South Africa

Mr. Gary Wright, Director
Division of Nuclear Facility Safety
Illinois Emergency Management Agency
1035 Outer Park Drive
Springfield, IL 62704

DC Mitsubishi - US APWR Mailing List

Email

APH@NEI.org (Adrian Heymer)
awc@nei.org (Anne W. Cottingham)
bennettS2@bv.com (Steve A. Bennett)
bob.brown@ge.com (Robert E. Brown)
BrinkmCB@westinghouse.com (Charles Brinkman)
chris.maslak@ge.com (Chris Maslak)
ck_paulson@mnes-us.com (C Keith Paulson)
ckpaulson@aol.com (C.K. Paulson)
craig.conklin@dhs.gov (Craig Conklin)
CumminWE@Westinghouse.com (Edward W. Cummins)
cwaltman@roe.com (C. Waltman)
david.hinds@ge.com (David Hinds)
david.lewis@pillsburylaw.com (David Lewis)
DeLaBarreR@state.gov (R. DeLaBarre)
Dennis.Buschbaum@txu.com (Denny Buschbaum)
dlochbaum@UCSUSA.org (David Lochbaum)
dwoodla1@txu.com (Donald Woodlan)
erg-xl@cox.net (Eddie R. Grant)
frankq@hursttech.com (Frank Quinn)
gcesare@enercon.com (Guy Cesare)
greshaja@westinghouse.com (James Gresham)
JAC3@nrc.gov (Jeff Ciocco)
james.beard@gene.ge.com (James Beard)
jcurtiss@winston.com (Jim Curtiss)
jgutierrez@morganlewis.com (Jay M. Gutierrez)
jim.riccio@wdc.greenpeace.org (James Riccio)
JJNesrsta@cpsenergy.com (James J. Nesrsta)
John.O'Neill@pillsburylaw.com (John O'Neill)
Joseph_Hegner@dom.com (Joseph Hegner)
kcrogers@aol.com (K. C. Rogers)
KSutton@morganlewis.com (Kathryn M. Sutton)
kwaugh@impact-net.org (Kenneth O. Waugh)
maria.webb@pillsburylaw.com (Maria Webb)
mark.beaumont@wsms.com (Mark Beaumont)
masahiko_kaneda@mhi.co.jp (Masahiko Kaneda)
masanori_onozuka@mnes-us.com (Masanori Onozuka)
masayuki_kambara@mhi.co.jp (Masayuki Kambara)
matias.travieso-diaz@pillsburylaw.com (Matias Travieso-Diaz)
media@nei.org (Scott Peterson)
mike_moran@fpl.com (Mike Moran)
MSF@nei.org (Marvin Fertel)
mwetterhahn@winston.com (M. Wetterhahn)
nirsnet@nirs.org (Michael Mariotte)
patriciaL.campbell@ge.com (Patricia L. Campbell)

DC Mitsubishi - US APWR Mailing List

paul.gaukler@pillsburylaw.com (Paul Gaukler)
Paul@beyondnuclear.org (Paul Gunter)
pshastings@duke-energy.com (Peter Hastings)
RJB@NEI.org (Russell Bell)
RKTemple@cpsenergy.com (R.K. Temple)
roberta.swain@ge.com (Roberta Swain)
sandra.sloan@areva.com (Sandra Sloan)
sfrantz@morganlewis.com (Stephen P. Frantz)
shinji_kawanago@mnes-us.com (Shinji Kawanago)
steven.hucik@ge.com (Steven Hucik)
Tansel.Selekler@nuclear.energy.gov (Tansel Selekler)
tgilder1@luminant.com (Tim Gilder)
tjh2@nrc.gov (Thomas Herrity)
tmatthews@morganlewis.com (T. Matthews)
tom.miller@hq.doe.gov (Tom Miller)
trsmith@winston.com (Tyson Smith)
Vanessa.quinn@dhs.gov (Vanessa Quinn)
VictorB@bv.com (Bill Victor)
vijukrp@westinghouse.com (Ronald P. Vijuk)
Wanda.K.Marshall@dom.com (Wanda K. Marshall)
waraksre@westinghouse.com (Rosemarie E. Waraks)
whorin@winston.com (W. Horin)

Request for Additional Information Based on the Review of Topical Report MUAP-07006-P, Rev.1, "Defense-in-Depth and Diversity"

RAI No.	Request for Additional Information (RAI)
Integrated Reactor Protection System (RPS) and Engineered Safety Feature Actuation System (ESFAS) with Functional Diversity	
RAI-01	Could a faulty sensor compromise the integrity of a train of RPS/ESFAS while also providing an erroneous value to the Diverse Actuation System (DAS)?
RAI-02	Provide a description (and figure if necessary) of how sensor values (or signals) are transmitted to the RPS and ESFAS systems.
RAI-03	Discuss the combining of the RPS and ESFAS into an integrated system and how it impacts the defense-in-depth philosophy and the four echelons of defense against Common Cause Failures (CCFs).
RAI-04	Clarify the type information shared between the RPS and ESFAS. In addition, please explain the operation of the ESFAS given the failure of the RPS to communicate a sensor/calculated value (i.e., will the RPS value be ignored, or will it be interpreted as a trip signal?).
RAI-05	Discuss the interconnections between the Reactor Trip System (RTS) and ESFAS and demonstrate that the functions required by the Anticipated Transient Without Scram (ATWS) rule (10 CFR 50.62) are not impaired.
RAI-06	Discuss the sensor signals, interpreted (converted) sensor values, or calculations based on sensor signals that are transmitted from the Protection and Safety Monitoring System (PSMS) to the ESFAS.
RAI-07	Provide that portion of the Defense-in-Depth and Diversity analysis that evaluates the four echelons of defense against CCFs that includes the RPS and ESFAS.
RAI-08	Discuss the collection and transmission of data to the ESFAS trains.
RAI-09	Please provide the probabilistic risk assessment (PRA) information including the process, assumptions, data, uncertainties, and types of errors and failures modeled (including maintenance, human errors, recovery factors, CCFs), and results so that the integrated RPS/ESFAS with functional diversity are adequately assessed.
RAI-10	Address the issue of a potential software CCF failing both the RPS/ESFAS at the RPS/ESFAS interface.
RAI-11	Discuss the results of functional diversity vs. separation, including the model, assumptions, data and sources, and comparison to operational experience. Also address hardware and software, such as what is shared, CCFs, etc.
RAI-12	Clarify the operation of the Power Interface (PIF) Modules and discuss input and output signals, hardware and software components, and system interfaces.

RAI No.	Request for Additional Information (RAI)
RAI-13	Provide details of how the ATWS function is actually implemented. In addition, it appears that there are too few sensors shared by too many systems, including common mode failure. For example, the isolation device(s) could compromise defense-in-depth objective of the design. Address any CCFs of the software of the isolation devices or the sensors. Is a postulated failure or series of failures of any aspect of any channel for these common devices a part of the safety basis of this design? Request you provide information to support the determination that no combination of failed sensors or artifacts of any one or combination of common sensor channels will negatively affect safety system operation due to CCF?
Conformity to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Subsection II.Q, "Defense against Common-Mode Failures in Digital Instrumentation and Control Systems," dated April 2, 1993	
RAI-14	Identify the software failure modes for the digital systems, their likelihood, and the effects of their occurrence. Specifically, please address how failure modes other than "fails to function" could impact the actuation and operation of the DAS.
RAI-14a	The staff requirements memorandum to SECY 93-087, dated July 21, 1993, states in full, "inasmuch as common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis." This is different than stating that "common mode failures are beyond design-basis events." This statement does not say that there are not any CCFs that may not need to be considered as single failures as implied by the quote portion of the sentence, but that such events "should be considered on a best-estimate basis." Please address this difference.
RAI-14b	Did the Failure Mode and Effect Analysis (FMEA) consider failure mechanisms that are recognized as being highly unlikely, but could affect multiple components? Without the FMEA table included in the topical report, it is not apparent that all components and failure modes have been considered. Does the FMEA systematically identify and evaluate the failure modes for all components and include failure modes such as loss of function, but also low or high values, timing issues, maintenance, etc.?
RAI-14c	Did the FMEA consider the coincident occurrence of otherwise single failures (i.e., multiple failures, such as software CCF, loss of all power, fire, flood)?
RAI-15	Please confirm that the DAS functions and other Defense-in-Depth and Diversity - related functions are consistent with the portions of the accident analysis that support the Defense-in-Depth and Diversity analysis.
RAI-16	Identify any and all common components between and within the RTS, ESFAS, and DAS divisions and systems. Discuss the CCF susceptibilities for these common components and address their likelihood of occurrence.
RAI-17	What measures are used to reduce or limit the potential for inadvertent actuation and challenges to the diverse instrumentation and controls safety systems?
RAI-18	Once initiated, will the ATWS mitigation logic and DAS the mitigation function go to completion?

RAI No.	Request for Additional Information (RAI)
RAI-19	Provide a listing of Anticipated Operational Occurrence (AOO)s and Postulated Accident (PA)s considered in the design of the diverse instrumentation and control systems and identify the potential concurrent CCFs that can disable or cause erratic or erroneous operation of the PSMS and PCMS. Discuss the effects of those failures.
RAI-19a	The coping analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to de-energized or energized state).
Conformity to NUREG/CR-6303, "*Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994*	
RAI-20	Identify and discuss those cases where functional diversity does not exist within the PSMS for each AOO and PA.
RAI-21	Identify and discuss those events where the signal used to produce a reactor trip is not diverse from the signals for ESF actuation.
RAI-22	Provide or discuss the Defense-in-Depth and Diversity Coping Analysis, along with a reference. Include a listing and explanation of events under each category of "equivalent protection," expertly judged," and "analyzed."
RAI-23	Discuss the ability to detect and mitigate each AOO or PA using the DAS for Type 1, 2, and 3 Failures, including a discussion of sensor diversity withing the PSMS for each AOO and PA.
RAI-24	Discuss the operating experience of the PSMS, PCMS, and DAS, including, but not limited to, identifying any failures, detectable failures, diagnostics, failure modes.
RAI-24a	Please discuss whether the failure mode "disables" is limited to "fails" such that no signal is generated or does it include false signals.
RAI-25	This does not account for the transmittal of a faulty signal or value. Because of the shared PIF modules, are there any postulated CCFs that could prevent the proper operation of the PSMS and PCMS and impact the DAS?
RAI-25a	The only failure mode evaluated in the coping analysis is "fail as is." Please discuss that other failure modes are not considered. .
RAI-26	Identify and explain any differences and changes with an explanation on why the change is appropriate from the Chapter 15 analysis compared with the best estimate analysis for each AOO.
RAI-27	Identify and explain any differences and changes with an explanation on why the change is appropriate from the Chapter 15 analysis compared with the best estimate analysis for each PA.
RAI-28	Did the Defense-in-Depth and Diversity coping analysis evaluate CCFs, disabling the two separate scenarios; the reactor trip functions and then the ESFAS functions, that cause spurious actuations as well as preventing actuations? Did this assume that, by providing a diverse means of protection, this did not effect the DAS?

RAI No.	Request for Additional Information (RAI)
RAI-29	Please identify all shared hardware and software between the RPS/ESFAS and the DAS (including the PIF Modules) and discuss the effects of its failure, including CCF susceptibilities. Discuss whether other failure modes besides "disable" were addressed. If not, please discuss why "disable" is the only failure mode addressed and the appropriateness of this assumption.
Task Working Group #2: Diversity and Defense-in-Depth Issues	
RAI-30	In those cases where plant response analysis shows that the protective action is not required for at least 30 minutes, the protective action may be performed by manual operator actions. Demonstrate that sufficient information and controls (safety or non-safety), independent and diverse from the RPS, are provided in the main control room, and that the information displays and controls are not subject to the same CCF. For those events where manual operator actions are required before 30 minutes, please demonstrate that sufficient information and controls are provided, and discuss any possible conflicts in training and procedures for evaluating when to take action prior to 30 minutes.
Conformity to SECY 93-087, Subsection II.D, "Leak Before Break"	
RAI-31	Containment level sump level and airborne particulate radioactivity monitoring are diverse methods of detecting a reactor coolant pressure boundary leak. What third methods are under consideration?
Common PIF Modules for PSMS/PCMS and DAS	
RAI-32	Provide justification on why the PIF Module is not susceptible to a CCF.
RAI-33	Please clarify the definition "higher level in the system architecture."
RAI-34	Does the statement "safety signals from within the PSMS always have priority over signals from all non-safety equipment, with the exception of DAS which uses state based priority" mean that other nonsafety signals (besides the DAS) transmit/receive data, communicate, or interface with the PSMS?
RAI-35	Please discuss why it is ok to use the same sensors for PSMS/ESFAS and DAS, with all signals then being transmitted to a common PIF Module.
RAI-36	Is there a communication independence between the PSMS and the DAS?
RAI-37	Please address handshaking or communication that would compromise functional independence of the PSMS and DAS.
RAI-38	Please discuss the "conventional" hardware of the PIF Module.
RAI-39	Show that the "conversion to discrete signal" and "switching of control circuit" are easily verifiable steps. Is there any self-testing or diagnostic running within the PIF Module? What is the format of the digital signal from the "Control signal from CPU"?
RAI-40	The topical report states that the PIF Modules are described in the *MELTAC Digital Platform Topical Report*; this report does not provide any more information than the topical report under review. Please describe the PIF Modules in detail in this topical report or the *MELTAC Digital Platform Topical Report*. A simple device might best be shown with a schematic.

RAI No.	Request for Additional Information (RAI)
RAI-40a	Is the Output Module in Topical Report MUAP-07004, "Safety I&C System Description and Design Process," July 2007, the same component as the PIF Module in Topical Report MUAP-07006? If not, please explain the differences and clarify the uses of each component.
RAI-41	A PIF Module combines normal control, manual, auto safety, and auto DAS. What examples of "these components" that are used in nuclear plants are referred to in Point 4 (page 51 of the topical report)? Describe the similarities and differences.
	Compliance with 10 CFR Part 50, Appendix A
RAI-42	Outline how leak detection (i.e., leak-before-break) will be used in the defense-in-depth and diversity strategy and how it will comply with 10 CFR Part 50, Appendix A, General Design Criterion 4 and the NRC's guidance for use of leak-before-break analysis?