Pacific Gas and Electric Company®

Barry S. Allen
Vice President, Nuclear Services

Diablo Canyon Power Plant
Mail Code 104/6
P. O. Box 56
Avila Beach, CA 93424

805.545.4888
Internal: 691.4888
Fax: 805.545.6445

May 28, 2015

PG&E Letter DCL-15-065

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

10 CFR 50.90

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 License Amendment Request 13-02, "Revision to Technical Specifications to Adopt Risk Informed Completion Times TSTF-505, Revision 1, 'Provide Risk-Informed Extended Completion Times – RITSTF Initiative 4B'"

Reference: 1. PG&E Letter DCL-13-106, "License Amendment Request 13-02, Revision to Technical Specifications to Adopt Risk Informed Completion Times TSTF-505, Revision 1, 'Provide Risk-Informed Extended Completion Times – RITSTF Initiative 4B,'" dated November 25, 2013

Dear Commissioners and Staff:

In Reference 1, Pacific Gas and Electric Company (PG&E) submitted License Amendment Request (LAR) 13-02 that proposes an amendment that would modify Technical Specification (TS) requirements to permit the use of Risk Informed Completion Times in accordance with Technical Specifications Task Force-505, Revision 1, "Provide Risk-Informed Extended Completion Times - RITSTF Initiative 4B."

On February 18, 2015, the NRC staff requested additional information required to complete the review of LAR 13-02. PG&E's responses to the staff's questions are provided in the Enclosure.

This information does not affect the results of the technical evaluation or the no significant hazards consideration determination previously transmitted in Reference 1.

This communication contains a new commitment (as defined in NEI 99-04) to be implemented following NRC approval of the LAR. The commitment is contained in Attachment 1 to the Enclosure.

If you have any questions, or require additional information, please contact Philippe Soenen at (805) 545-6984.

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

Executed on May 28, 2015.

Sincerely,

Barry S. Allen
Vice President, Nuclear Services

kjse/4328/50467285
Enclosure
cc: Diablo Distribution
cc/enc: Marc L. Dapas, NRC Region IV Administrator
Thomas R. Hipschman, NRC Senior Resident Inspector
Siva P. Lingam, NRR Project Manager
Gonzalo L. Perez, Branch Chief, California Dept of Public Health

PG&E Response to NRC Request for Additional Information Regarding License Amendment Request 13-02, "Revision to Technical Specifications to Adopt Risk Informed Completion Times TSTF-505, Revision 1, 'Provide Risk-Informed Extended Completion Times – RITSTF Initiative 4B'"

NRC Question 1:

By letter dated November 25, 2013 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13330A557), Pacific Gas and Electric Company (PG&E, the licensee) submitted a License Amendment Request (LAR) regarding Diablo Canyon Units 1 and 2 Facility Operating License. The proposed amendment would Revise Technical Specifications to Implement Technical Specification Task Force (TSTF) TSTF-505, Revision 1, "Provide Risk-Informed Extended Completion Times - RITSTF Initiative 4b." The technical review branch for instrumentation and control (I&C) has identified the need for additional information to complete the review of the LAR:

The LAR proposes adding Technical Specification (TS) Section 5.5.20, "Risk Informed Completion Time Program," to the TS, which states:

"This program provides controls to calculate a Risk Informed Completion Time (RICT) and must be implemented in accordance with Nuclear Energy Institute (NEI) 06-09, Revision 0, "Risk-Managed Technical Specifications (RMTS) Guidelines." The program shall include the following…"

The safety evaluation (SE) associated with the U.S. Nuclear Regulatory Commission approval of NEI 06-09, Revision 0 (ADAMS Accession No. ML063390639) qualified the approval of NEI 06-09, Revision 0 and is included in NEI 06-09 (Revision 0) –A (ADAMS Accession No. ML12286A322). For example, the NRC qualifications includes:

"Regulatory Guide (RG) 1.200, Revision 1, was issued in January 2007, which endorsed the updated standard applicable for internal events PRA [probabilistic risk analysis] models. The NRC staff takes exception to the reference to RG 1.200, Revision 0, currently listed throughout TR NEI 06-09, Revision 0. The NRC staff will require an assessment of PRA technical adequacy using the revised RG 1.200, Revision 1, and the updated PRA standard."

It is understood that the "-A" version was not referenced because TSTF-505 did not reference it. Please explain how the "qualifications" in the SE are incorporated.

PG&E Response:

The LAR 13-02 for Diablo Canyon to adopt TSTF-505 was developed consistent with the NRC SE which is included in NEI 06-09, Revision 0-A. By Pacific Gas and

Electric (PG&E) Letter DCL-15-007, dated February 5, 2015, in response to a previous NRC request for additional information (RAI) dated November 13, 2014, PG&E responded to RAI number 8 changing the reference in the proposed Diablo Canyon TS 5.5.20 from "NEI 06-09, Revision 0," to "NEI 06-09, Revision 0-A."

Section 4.0 of the NRC SE of NEI 06-09 identifies the limitations and conditions applicable for adoption of RMTS. Four specific "qualifications" are identified, as well as plant-specific information requirements:

> *As part of its review and approval of a licensee's application requesting to implement the RMTS, the NRC staff intends to impose a license condition that will explicitly address the scope of the PRA and non-PRA methods approved by the NRC staff for use in the plant-specific RMTS program. If a licensee wishes to change its methods, and the change is outside the bounds of the license condition, the licensee will need NRC approval, via a license amendment, of the implementation of the new method in its RMTS program. The focus of the NRC staff's review and approval will be on the technical adequacy of the methodology and analyses relied upon for the RMTS application.*

PG&E is not proposing to use any non-PRA methods in the Diablo Canyon plant-specific RMTS Program.

> *The NRC staff interprets TR NEI 06-09, Revision 0, as requiring consideration of risk management actions (RMAs) whenever the redundant components are considered to remain operable, but the licensee has not completed the extent of condition evaluations, and additionally, as required by a followup prompt operability determination.*

The Diablo Canyon program is consistent with NEI 06-09, Revision 0-A, and procedures being developed for implementation include consideration of RMAs (risk management actions) whenever redundant components remain operable pending the completion of extent of condition evaluation and followup prompt operability determination.

> *The NRC staff takes exception to the reference to RG 1.200, Revision 0, currently listed throughout TR NEI 06-09, Revision 0. The NRC staff will require an assessment of PRA technical adequacy using RG 1.200, Revision 1, and the updated PRA standard.*

Attachment 6 of the Diablo Canyon LAR 13-02 documents the evaluation of PRA technical adequacy using RG 1.200, Revision 2, which is the current revision in effect.

> *The NRC staff further interprets the guidance to evaluate the PRA using RG 1.200, Revision 1, and the ASME standard for capability Category II as a*

requirement that the licensee's PRA for internal events must satisfy all requirements of the ASME standard, and achieve at least capability Category II where the standard provides unique requirements. Because of the significant role of the PRA models in this application, exceptions to the requirements of the standard are generally not acceptable, and any exceptions must be identified and justified.

Attachment 6 of the Diablo Canyon LAR 13-02 documents the evaluation of PRA technical adequacy using RG 1.200, Revision 2, which is the current revision in effect. For the Diablo Canyon PRA for internal events, Attachment 6 of LAR 13-02 justifies that the applicable requirements of the American Society of Mechanical Engineers (ASME) standard are satisfied and achieve at least capability Category II where the standard provides unique requirements, or are dispositioned in terms of their impact on the RICT Program.

Licensees should provide the following plant-specific information in support of their LAR. ...

Attachments 1 and 5 through 16 of the Diablo Canyon LAR 13-02 provide the required plant-specific information identified in the NRC SE, items 1 through 13.

NRC Question 2:

The SE associated with NEI 06-09, Revision 0 states:

"PRA Modeling. TR NEI 06-09, Revision 0, specifically applies the RMTS only to those SSCs [Systems Structures or Components] which mitigate core damage or large early releases. Where the SSC is not modeled in the PRA, and its impact cannot otherwise be quantified using conservative or bounding approaches, the RMTS are not applicable, and the existing frontstop CT would apply."

It is understood that part of the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) functions described in TS Tables 3.3.1-1 and 3.3.2-1 are implemented in four cabinets of Eagle 21 equipment.

(a) Please describe the PRA model for the RTS, and any conservative or bounding approaches for parts of the RTS that are not modeled. Please be sure to include a description of how equipment shared between RTS functions is modeled in the PRA.

(b) Please describe the PRA model for the ESFAS and any conservative or bounding approaches for parts of the ESFAS that are not modeled. Please be sure to include a description of how equipment shared between ESFAS functions is modeled in the PRA.

(c) Please describe how any equipment shared between RTS and ESFAS functions is modeled in the PRA.

PG&E Response:

(a) Revision 2 of RG 1.200 was issued in March 2009, which endorsed the updated standard applicable for internal events, internal flooding, seismic and fire PRA models. The technical adequacy of the Diablo Canyon internal event, internal flooding, seismic and fire PRA models which support the RICT Program have been evaluated against Revision 2 of RG 1.200 using the current endorsed ASME/American Nuclear Society (ASME/ANS) standard RA-Sa-2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addendum A to RA-S-2008." Attachment 6 of the Diablo Canyon LAR 13-02 provides information supporting consistency with Revision 2 of RG 1.200 and the current endorsed standard ASME/ANS RA-Sa-2009.

The RTS trips the reactor on a signal from either the Solid State Protection System (SSPS) or the plant operator initiating a manual reactor trip. There are two redundant reactor protection system (RPS) trains (A and B) that react to reactor trip signals. Train A consists of an under voltage (UV) trip coil 52(UV)/RTA, a shunt trip coil 52(SHTR)/RTA and reactor trip breaker RT52A; likewise Train B consists of an under voltage trip coil 52(UV)/RTB, a shunt trip coil 52(SHTR)/RTB and reactor trip breaker RT52B. For each RPS train to fail, the respective reactor trip breaker must fail or the UV trip coil AND shunt trip coil must both fail. Only one RTS train is required for RTS success. If both RTS trains fail, then manual reactor trip initiated by the plant operator must be successful in order for the RTS to not fail.

Automatic reactor trip by either RTS Train A or B is only credited in the PRA model if the SSPS system is successful. The SSPS reactor trip signal is generated when sensed and calculated process and nuclear parameters fall outside preset safe limits. However, the PRA model only models the following reactor trip functions generated from the SSPS: Containment High Pressure (Safety Injection), Pressurizer Low Pressure, Steam Line Low Pressure (Safety Injection) and Steam Generator (SG) Low-Low Level. It is noted that the RTS does not monitor the steam line pressure or containment high pressure signals; these are monitored by the ESFAS to initiate safeguards actuations which in turn would cause a reactor trip signal.

Since not all of the RTS functions are modeled in the SSPS, the automatic RTS function is evaluated for the RICT Program using a bounding evaluation, as described in the LAR 13-02 Table A5-1, Note 2. Generic logic will address failure of the automatic trip function (RTS Trains A and B) when two of two generic RTS signals fail. The inoperability of any one or more channels of a RTS function will be assumed to result in unavailability of that function as an input to the automatic RTS actuation. For the RICT Program, the risk for one or

more inoperable instrument channels for one trip function will be evaluated assuming that one of the two generic RTS function is unavailable, and crediting only one remaining function for automatic reactor trip for all initiating events. If two or more RTS functions have inoperable instrument channels, then no credit will be taken for the automatic RTS function, essentially failing RTS Trains A and B and requiring manual reactor trip for RTS success. As noted in the LAR 13-02, this modeling approach is conservative because: (1) inoperability of any single instrument channel for any RTS function is evaluated as causing the loss of that RTS function even if the remaining channels could actuate a reactor trip; (2) inoperability of any RTS signal is assumed to impact mitigation of all transient and accident conditions, even though only a subset of all initiating events would be impacted; and (3) no credit is taken for automatic RTS actuation for more than two RTS signals for any initiator.

Support equipment shared between RTS functions include SSPS Train A, SSPS Train B, 125 Volt (V) direct current (DC) Bus 1-1, 125 V DC Bus 1-2 and alternating current (AC) Instrument Channels I, II, III, IV. This equipment is in the PRA model and will be taken out of service to track risk in the RMTS program. Split fractions have been developed for the RTS and SSPS corresponding to permutations of support equipment logic failures. Split fraction logic rules have also been developed, which assign split fractions based on preceding equipment failures. For example, if SSPS Train A is taken out of service, then in the PRA model RTS split fraction RT4A (one SSPS trip signal Train A is failed and all power is available) would be used for RTS unless another support equipment fails randomly. If a 125 V DC Bus 1-2 randomly fails with SSPS Train A taken out of service, then RTS split fraction RT5A (one SSPS trip signal Train A is failed, and DC power Train B is lost to the shunt trip coil) would be used. Split fraction RT5A has a higher failure probability of RTS than RT4A since it also includes loss of 125 V DC Bus 1-2.

(b) The ESFAS System is modeled in the PRA as the SSPS, which monitors key sensed and calculated process and nuclear parameters to ensure safe operating conditions exist at all times. In case the parameters exceed preset safe limits, the SSPS will produce activation signals as required for the following systems:

Reactor Protection System
Turbine Trip
Generator Trip
Auxiliary Feed Water System Actuation
Feed Water Isolation
Safety Injection
Main Steam Isolation
Containment Vent Isolation
Containment Isolation Phase A
Containment Isolation Phase B

Containment Spray
Control Rod Withdrawal Block

ESFAS is actuated from either automatic signals generated from the SSPS or the plant operator initiating a manual safety injection, containment isolation and auxiliary feedwater actuation. There are two redundant SSPS trains (A and B) that provide ESFAS signals and are independent to the degree that only one train is required to initiate necessary safety functions. However, if there is a failure of one train, some safety system components will not receive automatic start signals, e.g., only 2 out of 3 auxiliary feed water (AFW) pumps will start if only 1 of the 2 SSPS trains produces signals. The system equipment boundary for the SSPS, including the process and control instrumentation system, starts at the parameter transmitters in the analog sensor channels. All necessary logic cabinets, transmitters, bi-stables, and input relays are modeled. The PRA models the following signals initiated by the SSPS: Containment High pressure (2 out of 3), Pressurizer Low Pressure (2 out of 4), Steam Line Low Pressure (2 out of 3 per line for 1 out of 4 lines), Containment High-High Pressure (2 out of 4) and SG Low-Low Level (2 out of 3 per SG for 1 out of 4 SG). Since not all initiating events require the same ESFAS signals six different sets of SSPS criteria have been developed based on the corresponding accident or transient: General Transient, Large Loss-of-coolant (LOCA), SG Tube Rupture, Steam Line Break Inside Containment, Steam Line Break Outside Containment and Small LOCA.

As described in the LAR 13-02 Table A5-1, and as permitted by NEI 06-09, the following bounding conservative approaches have been applied in applying RICTs to the following T.S. 3.3.2 Limiting Condition for Operation (LCO) Condition functions for the parts of ESFAS that are not modeled in the PRA:

- Function 1.a – Safety Injection – Manual Initiation: The operator action for failure to take manual action in response to a loss of automatic SSPS actuation is used as a conservative surrogate for a manual safety injection channel inoperable
- Function 2.a – Containment Spray (CS) – Manual Initiation: Unavailability of the CS system is used as a conservative surrogate for a manual CS channel inoperable
- Function 3.a(1) – Phase A Isolation – Manual Initiation: The operator action for failure to take manual action in response to a loss of automatic SSPS actuation is used as a conservative surrogate for a manual Phase A isolation channel inoperable
- Function 3.b(1) – Phase B Isolation – Manual Initiation: The operator action for failure to take manual action in response to a loss of automatic SSPS actuation is used as a conservative surrogate for a manual Phase B isolation channel inoperable
- Function 4.a – Steam Line Isolation - Manual Initiation: The operator action for failure to take manual action in response to a loss of automatic

SSPS actuation is used as a conservative surrogate for a manual steam line isolation channel unavailable.

- Function 5.b - Feedwater Isolation – SG Water Level – High-High: Unavailability of the associated SG low level actuation of AFW is used as a bounding surrogate for feedwater isolation actuation on SG water level – high-high
- Function 6.g - Reactor Coolant Pump (RCP) UV AFW Start: Unavailability of the turbine driven AFW pump is used as a conservative surrogate for the RCP UV AFW start
- Function 7 – Refueling Water Storage Tank (RWST) Low Level Residual Heat Removal (RHR) Pump Trip: Unavailability of aligning an RHR pump for recirculation is used as a conservative surrogate for the RWST Low Level RHR pump trip
- Support equipment shared between ESFAS functions includes SSPS Trains A and B and AC Instrument Channels I, II, III, and IV. This equipment is in the PRA model and will be taken out of service to track risk in the RMTS program. Split fractions have been developed for the SSPS corresponding to permutations of support equipment logic failures. Split fraction logic rules have also been developed, which assign split fractions based on preceding equipment failures. For example, if Instrument AC channels II and III are out of service, then in the PRA model split fraction SA6 would be used.

(c) Equipment shared between the RTS and ESFAS functions includes SSPS Trains A and B, AC Instrument Channels I, II, III, and IV and instrumentation channels including Pressurizer Pressure, Containment Pressure, Steam Line Pressure and SG level. This equipment is in the PRA model and will be taken out of service to track risk in the RMTS program. Taking this equipment out of service impacts the SSPS fault tree, which results in split fractions with higher failure probabilities. This directly impacts the ESFAS SSPS system in the PRA model and results in the RTS being assigned a higher failure probability by split fraction logic rules due to its dependence on the SSPS system.

NRC Question 3:

The single failure criterion requires that a system which is designed to perform a defined safety function must be capable of meeting its objectives assuming the failure of any major component within the system or in an associated system which supports its operation.

The LCO in the TS allows a limited period of operation in a condition where the single failure criterion is not met. That is, given that a single failure has occurred, a plant is allowed a limited time of operation in this configuration (i.e., a configuration that could not tolerate a second failure). During this limited time, the plant must either establish a plant configuration that can tolerate another failure, or transition to an operating mode where the safety function is not required.

A plant is never allowed to operate in a configuration where a protection system or a safety system is unable to perform its required safety functions.

For the specific case where a protection system and a control system share components, there are additional regulatory requirements that must be considered. These additional requirements are sometimes referred to as the "separation of protection and control criterion," and include:

GDC 24 "Separation of protection and control systems. The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system..."

IEEE 279-1971 "4.7 Control and Protection System Interaction."

"4.7.3 Single Random Failure. Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.

Provisions shall be included so that this requirement can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel."

For the RTS and ESFAS, please identify all of the instances where equipment or information is shared between protection and control systems.

PG&E Response:

(PG&E notes that it is the TS Conditions, Required Actions, and their associated Completion Times which specify the limited period of operation where the single failure criterion is not met; the LCO specifies the minimum equipment requirements for unlimited continued operation. Further, PG&E notes that NEI 06-09 Revision 0-A implemented by TSTF-505 provides a method acceptable to the NRC for determination of this limited time, as an alternative to the fixed times in the Standard TS.)

The RTS and ESFAS functions within the scope of the RICT Program of TS 3.3.1 and 3.3.2 that use the same instrumentation inputs for one or more control functions is contained in Table 1.

Table 1
Reactor Trip System and Engineered Safety Features Actuation System Functions Within the scope of the Risk Informed Completion Time Program that Use the Same Instrumentation Inputs for One or More Control Functions

RTS/ESFAS Function	Control Function
Power Range Neutron Flux - High (RTS Function 2.a) Power Range Neutron Flux - Low (RTS Function 2.b) Power Range Neutron Flux - High Positive Rate (RTS Function 3)	Control Rod Speed and Direction
Overtemperature ΔT (RTS Function 6) Overpower ΔT (RTS Function 7)	Control Rod Speed and Direction Steam Dumps (T_{avg} mode)
Pressurizer Pressure - High (RTS Function 8.a) Pressurizer Pressure - Low (RTS Function 8.b) Pressurizer Pressure - Low (ESFAS Function 1.d)	Pressurizer Pressure Control
Pressurizer Water Level - High (RTS Function 9)	Pressurizer Level Control and Let-down Isolation
SG Water Level - Low-Low (RTS Function 14.a) SG Water Level - High-High (ESFAS Function 5.b) SG Water Level - Low-Low (ESFAS Function 6.b)	SG Level Control for AFW and Main Feedwater (MFW)
SG Pressure - Low (ESFAS Function 1.e(1) and 4.d(1))	SG Level Control and MFW Pump Speed Control

NRC Question 4:

Protection systems and safety systems have two or more redundant elements, and these elements are arranged in typical voting arrangements, for example:

1 out of 2 (e.g., Manual Reactor Trip)
2 out of 3 (e.g., Pressurizer Water Level-High)
2 out of 3 (per loop) (e.g., Reactor Coolant Flow-Low)
2 out of 4 (P&C) (e.g., See response to Question No. 3 above)
2 out of 4 (no P&C)

For each RTS & ESFAS voting arrangement, please state the minimum number of redundancies that must be functional (i.e., TS Operable and/or "PRA Functional"), so the RTS and ESFAS system can still perform their required safety functions.

PG&E Response:

For an RTS or ESFAS function to be considered PRA Functional in order to permit the use of the RICT Program, the number of OPERABLE and/or PRA Functional channels must be such that the RTS or ESFAS signal will actuate when the actual plant parameter exceeds the RTS or ESFAS setpoint. For manual actuations, where a 1-of-2 redundancy is provided, at least one channel must be OPERABLE or PRA Functional. For automatic actuations involving either a 2-of-3 or 2-of-4 redundancy, at least two channels must be OPERABLE or PRA Functional. This may include an inoperable channel which is in the trip condition.

Refer also to the responses to RAI numbers 5 and 7, below, for additional considerations for control functions.

NRC Question 5:

LAR Enclosure Attachment No. 5. Table A5-2 contains RICT estimates for some conditions, for example:

The first row addresses "Condition B, one of two manual reactor trip channels inoperable," and identifies the calculated RICT. It is assumed the RICT is calculated based on the inoperable channel being "PRA Functional," because a RICT is not applicable for a loss of function.

(a) Is the "single failure criterion" met in each of these conditions? Please explain.

(b) Please state if the "separation of protection and control criterion" is applicable, and if so, how it is met in each of these conditions.

PG&E Response:

(a) (PG&E notes that, consistent with NEI 06-09 Rev. 0-A and TSTF-505, the RICT Program is not applicable if both manual reactor trip channels are inoperable and non-functional. The RICT Program may be applicable when a single channel is inoperable and non-functional, provided the remaining channel is either OPERABLE or PRA Functional, such that the function of manual reactor trip remains available.)

The "single failure criterion" may be met depending upon the specific arrangement of the instrument channel logic and the failure mode of the instrument channel (high or low).

For RTS or ESFAS functions with two redundant channels, an inoperability of one channel would result in a 1-of-1 logic, so "single failure criterion" would not be met while the TS LCO is not met and the Required Action is in effect.

For RTS or ESFAS functions with three redundant channels and a 2 of 3 actuation arrangement, an inoperability of one channel may still maintain "single failure criterion," if the channel fails in a manner which actuates the RTS or ESFAS function for that channel, and the logic becomes 1-of-2. If the channel fails and does not actuate the RTS or ESFAS function, then the logic becomes 2-of-2, so "single failure criterion" would not be met while the TS LCO is not met and the Required Action is in effect.

For RTS or ESFAS functions with four redundant channels and a 2-of-4 actuation arrangement, an inoperability of one channel would still maintain "single failure criterion," since the arrangement would become either 2-of-3 or 1-of-3, depending upon the failure mode of the inoperable channel.

(b) Refer to NRC Question 3 response above which identifies the plant-specific RTS and ESFAS functions which share protection and control functions using the same instrumentation channels in Table 1. For each of the functions in Table 1, the discussion below identifies the plant response to a single additional channel failure while a TS Required Action is in effect for one inoperable channel, and the impact on the associated RTS or ESFAS functions. The discussions below demonstrate that for each configuration where protection and control functions use common inputs, either the associated RTS or ESFAS function will still actuate properly, or the resulting transient condition does not require or credit the affected RTS or ESFAS function. Note that the discussions below assume that the inoperable channel is also not PRA Functional per the RICT Program; otherwise there would not be any impact on the channel's capability to perform its RTS or ESFAS functions.

Power Range Neutron Flux

Four power range neutron flux channels input to 2-of-4 RTS signals for Overtemperature ΔT, Overpower (high and low range), and High Positive Rate, while the auctioneered high signal inputs to the Rod Control System.

If one channel is out-of-service, the remaining three channels would be in a 1-of-3 or 2-of-3 logic, depending upon the status of the inoperable channel. A failure of any single additional channel cannot therefore result in failure of the RTS functions.

Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function from the remaining channels.

Overtemperature ΔT and Overpower ΔT

Three hot leg and two cold leg temperature channels in each reactor coolant system (RCS) loop input to a 2-of-4 RTS signal for Overpower ΔT and Overtemperature ΔT, while the auctioneered high signal for T_{avg} inputs to the rod control system and steam dump system (T_{avg} mode).

If one channel is out-of-service, the remaining three channels would be in a 1-of-3 or 2-of-3 logic, depending upon the status of the inoperable channel. A failure of any single additional channel cannot therefore result in failure of the RTS functions.

Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function from the remaining channels.

Pressurizer Pressure

The four pressurizer pressure instrument channels input to a 2-of-4 RTS signal for both high and low pressure, and a 2-of-4 ESFAS signal for safety injection actuation on low pressure, while the second highest signal is selected for pressurizer pressure control.

If one channel is out-of-service, the remaining three channels would be in a 1-of-3 or 2-of-3 logic, depending upon the status of the inoperable channel. A failure of any single additional channel cannot therefore result in failure of the RTS functions.

Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function from the remaining channels.

Pressurizer Water Level

The three pressurizer water level instrument channels input to a 2-of-3 RTS signal on high water level, while the median signal is selected to isolate RCS let-down and to control charging flow.

If one channel is out-of-service failed high, there is no impact since the remaining two channels would be in a 1-of-2 logic and could withstand failure of a single additional channel.

If the out-of-service channel is failed low or as-is, then the logic is 2-of-2. A failure high of one of the two OPERABLE channels would not affect the control function since the remaining channel would be the median channel. A failure low of one of the two OPERABLE channels would fail the RTS function, and would isolate let-down and increase charging flow to increase pressurizer water level.

The Pressurizer Water Level—High trip function provides a backup signal for the Pressurizer Pressure—High trip and also provides protection against water relief through the pressurizer safety valves. These valves are designed to pass steam in order to achieve their design energy removal rate. A reactor trip is actuated prior to the pressurizer becoming water solid. The level channels do not actuate the safety valves, and the high pressure reactor trip is set below the safety valve setting. Therefore, with the slow rate of charging available, pressure overshoot due to level channel failure cannot cause the safety valve to lift before reactor high pressure trip.

Based on the above discussion, there is a potential for a single additional pressurizer level channel failure to cause a control system action that results in a condition requiring protective action. However, since the Pressurizer Water Level—High trip function is only the backup function for the Pressurizer Pressure—High trip, an additional channel failure will not prevent proper action of the protection system.

SG Water Level

The three water level instrument channels in each SG input to a 2-of-3 per SG RTS signal on low level, a 2-of-3 per SG ESFAS signal for actuation of AFW on low level, and a 2-of-3 per SG ESFAS signal for feedwater isolation on high level. The median signal is selected for SG water level control for both MFW and AFW. (AFW is used only during plant shutdown, so the control function is not further considered for the RICT Program, which is only applicable in MODE 1 and 2.)

If one channel is out-of-service failed high, there is no impact on the feedwater isolation function, since the remaining two channels would be in a 1-of-2 logic and could withstand failure of a single additional channel. The RTS and ESFAS functions for low SG level would be in a 2-of-2 logic. If an additional channel then failed low, there would be no impact on the MFW control function since the remaining OPERABLE channel would be the median channel selected. If an additional channel failed high, then MFW would be isolated to all SGs on a false high SG water level signal, and the reactor would trip on an eventual actual low

SG water level on the other three SGs which would ensue due to the MFW isolation.

If the out-of-service channel is failed low, there is no impact on the low SG water level RTS and AFW actuation functions, since the remaining two channels would be in a 1-of-2 logic. If an additional channel then failed high, there would be no impact on the MFW control function since the remaining OPERABLE channel would be the median channel selected. If an additional channel failed low, then a reactor trip and AFW actuation would occur on a false low SG water level signal.

Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function from the remaining channels.

SG Pressure

The three SG pressure instrument channels in each SG input to a 2-of-3 per SG ESFAS signals for safety injection and steam line isolation on low pressure, while the median signal is selected for SG water level control for MFW, as well as MFW pump speed control.

Since malfunctions of the MFW control functions do not result in a transient which requires either low SG pressure safety injection or steam line isolation signals, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function designed to protect against the condition.

Also, see the response to NRC Question 7c for evaluation of two or more channels inoperable.

NRC Question 6:

The second row of Table A5-2 identifies the calculated RICT for, "(Various Conditions) one of two credited automatic RTS functions inoperable." It is assumed the RICT is calculated based on the inoperable channels being "PRA Functional," because a RICT is not applicable for a loss of function. Please describe each condition and the two credited automatic RTS functions for each.

PG&E Response:

(PG&E notes that, consistent with NEI 06-09 Rev. 0-A and TSTF-505, the RICT is not applicable if there are insufficient OPERABLE and/or PRA Functional channels to permit actuation of the RTS or ESFAS function. The RICT Program may be

applicable when one or more channels are inoperable and non-functional, provided the remaining channel(s) are either OPERABLE or PRA Functional, such that the RTS or ESFAS function remains available.)

In the Diablo Canyon LAR 13-02 Table A5-1, Note 2 describes a bounding evaluation used to assess a RICT for instrumentation channels input to the automatic RTS functions. The inoperability of one or more instrumentation channels is assumed (conservatively) to fail the associated RTS function (Table 3.3.1-1 of the Diablo Canyon TS). This is conservative because any single failure of an instrument channel does not fail the RTS function, and because the RICT Program is not permitted to be applied to a loss of any RTS function condition.

A generic RTS model is used for the automatic reactor trip instrumentation channel input, assuming that two trip signals are actuated for any transient or accident condition. The calculated RICT in Table A5-2 is based on the change in risk associated with having only one signal available instead of two. This RICT would be applicable to each automatic RTS function in TS Table 3.3.1-1 for which the RICT Program is applicable.

NRC Question 7:

Table A5-2 generally does not tabulate the RICT for the RTS and ESFAS functions when "Two or more…channels inoperable."

(a) Please provide tabulated RICTs for each configuration (i.e., 2, 3, or 4 channels inoperable) associated with "Two or more…channels inoperable." Please include the case where one or more channels are not PRA functional.

(b) Is the "single failure criterion" met in each of these configurations? Please explain.

(c) Please state if the "separation of protection and control criterion" is applicable, and if so, how it is met in each of these configurations.

PG&E Response:

(a) The cases where two or more channels are inoperable involve a "loss of function" condition of RTS or ESFAS. In such a case, the RICT Program is only applicable when sufficient channels remain OPERABLE or PRA Functional to ensure the associated RTS or ESFAS signal will still actuate. The PRA calculation of a RICT in LAR 13-02 Table A5-2 is based on maintaining PRA Functionality of the RTS or ESFAS function, and therefore the calculated RICT for multiple channels inoperable but still PRA Functional would be the same as identified in Table A5-2 for the single channel out-of-service cases.

(b) While the RTS or ESFAS function is always available while a RICT is in effect, the "single failure criterion" may or may not be met depending upon the specific number of inoperable and non-functional channels while the TS LCO is not met and a TS Required Action is in effect. It is additionally noted that in many situations when a TS Action is entered for TS systems and components, the LCO function cannot be performed if an additional single failure occurs in the remaining equipment that is OPERABLE.

(c) Refer to NRC Question 3 response above which identifies in Table 1 the plant-specific RTS and ESFAS functions which share protection and control functions using the same instrumentation channels. For each of the Table 1 functions, the discussion below identifies the plant response to a single additional channel failure while the TS Required Action is in effect for two or more inoperable channels, and the impact on the associated RTS or ESFAS functions. The discussions below demonstrate that for each configuration where protection and control functions use common inputs, either the associated RTS or ESFAS function will still actuate properly, or the resulting transient condition does not require or credit the affected RTS or ESFAS function. Note that the discussions below assume that the inoperable channels are also not PRA Functional per the RICT Program; otherwise there would not be any impact on the channels' capability to perform their RTS or ESFAS functions.

Power Range Neutron Flux

Four power range neutron flux channels input to 2-of-4 RTS signals for Overtemperature ΔT, Overpower (high and low range), and High Positive Rate, while the auctioneered high signal inputs to the Rod Control System.

If two or more channels are out-of-service, the remaining channels would be in a 1-of-1, 1-of-2, or 2-of-2 logic, depending upon the status of the inoperable channels.

The control function uses the auctioneered high signal input; thus only a failure high of a channel could cause the control system to respond. In such a case the failure high of the power range neutron flux channel would also actuate the RTS function for that channel. Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function.

Overpower ΔT and Overtemperature ΔT

RCS Loop Hot and Cold Leg Temperature: Three hot leg and two cold leg temperature channels in each RCS loop input to a 2-of-4 RTS signal for Overpower ΔT and Overtemperature ΔT, while the auctioneered high signal for T_{avg} inputs to the rod control system and steam dump system (T_{avg} mode).

If two or more channels are out-of-service, the remaining channels would be in a 1-of-1, 1-of-2, or 2-of-2 logic, depending upon the status of the inoperable channels.

The control functions use the auctioneered high signal input for T_{avg}; thus only a failure high of a loop temperature channel could cause the control system to respond. A high input signal can only result in control rod insertion, not in control rod withdrawal. The RTS functions of Overpower ΔT and Overtemperature ΔT do not protect against an uncontrolled rod insertion. The high input cannot actuate the steam dump valves, because an additional control signal input indicating occurrence of a load rejection is required to permit steam dumps to actuate.

Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function from the remaining channels.

Pressurizer Pressure

The four pressurizer pressure instrument channels input to a 2-of-4 RTS signal for both high and low pressure, and a 2-of-4 ESFAS signal for safety injection actuation on low pressure, while the second highest signal is selected for pressurizer pressure control.

If two or more channels are out-of-service, the remaining channels would be in a 1-of-1, 1-of-2, or 2-of-2 logic, depending upon the status of the inoperable channels. A control function transient can only be initiated if an additional channel fails high, since if an instrument channel failed low, there would be no control function transient since the failed channel would not become the second highest channel. Further, if the remaining channels are in 1-of-1 or 1-of-2 logic, a high failure would result in a reactor trip signal. Therefore, the only concern would be if the logic was 2-of-2, and a channel then failed high. However since the control function uses the second highest input, the failed high channel could only cause a transient if another channel were also failed high, which is not the case when the logic is 2-of-2.

Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function from the remaining channels.

Pressurizer Water Level

The three pressurizer water level instrument channels input to a 2-of-3 RTS signal on high water level, while the median signal is selected to isolate RCS let-down and to control charging flow.

If two or more channels are out-of-service, then one of the inoperable channels would have to be in trip to maintain PRA functionality of the RTS function, and so would be in a 1-of-1 logic.

A failure high of the remaining channel would cause a reactor trip on a false high pressurizer water level signal. A failure low of the remaining channel would fail the RTS function, and would isolate let-down and increase charging flow to increase pressurizer water level.

The Pressurizer Water Level—High trip function provides a backup signal for the Pressurizer Pressure—High trip and also provides protection against water relief through the pressurizer safety valves. These valves are designed to pass steam in order to achieve their design energy removal rate. A reactor trip is actuated prior to the pressurizer becoming water solid. The level channels do not actuate the safety valves, and the high pressure reactor trip is set below the safety valve setting. Therefore, with the slow rate of charging available, pressure overshoot due to level channel failure cannot cause the safety valve to lift before reactor high pressure trip.

Based on the above discussion, for the Pressurizer Water Level—High trip function there is a potential for a single additional pressurizer level channel failure to cause a control system action that results in a condition requiring protective action. However, since the Pressurizer Water Level—High trip function is only the backup function for the Pressurizer Pressure – High trip, an additional channel failure will not prevent proper action of the protection system.

In consideration for the Pressurizer Water Level—High trip function that there is a potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action, when a RICT is in effect for one or more inoperable instrumentation channels of TS 3.3.1 Function 9, Pressurizer Water Level - High, and RMAs are required by the RICT Program of TS 5.5.20 and NEI 06-09 Revision 0-A, then additional monitoring of the pressurizer water level control function or placement of the affected plant equipment in manual control will be considered to manage the configuration risk associated with a possible control system transient initiated by any additional pressurizer water level channel failure.

SG Water Level

The three SG water level instrument channels in each SG input to a 2-of-3 per SG RTS signal on low level, a 2-of-3 per SG ESFAS signal for actuation of AFW on low level, and a 2-of-3 per SG ESFAS signal for feedwater isolation on high level. The median signal is selected for SG water level control for both MFW and AFW. (AFW is used only during plant shutdown, so the control function is not further considered for the RICT Program, which is only applicable in MODE 1 and 2.)

If two or more channels are out-of-service, then one of the channels would have to be in trip to maintain PRA functionality of the RTS function, and so would be in a 1-of-1 logic.

If the remaining channel failed high, then MFW would be isolated to all SGs on a false high SG water level signal, and the reactor would trip on an eventual actual low SG water level on the other three SGs which would ensue due to the MFW isolation.

If the remaining channel failed low, then a reactor trip and AFW actuation would occur on a false low SG water level signal.

Therefore, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system function from the remaining channels.

SG Pressure

The three SG pressure instrument channels in each SG input to a 2-of-3 per SG ESFAS signals for safety injection and steam line isolation on low pressure, while the median signal is selected for SG water level control for MFW, as well as MFW pump speed control.

Since malfunctions of the MFW control functions do not result in a transient which requires either low SG pressure safety injection or steam line isolation signals, there is no potential for a single additional channel failure to cause a control system action that results in a condition requiring protective action and also prevent proper action of a protection system channel designed to protect against the condition.

NRC Question 8:

Section 3.2.2 of NEI 06-09 Revision 0-A states:
"This guidance is intended to address separate operability and PRA functionality assessments which would allow a component to be considered both inoperable and PRA Functional based on the evaluation of the same degraded condition."

Please provide some example conditions that would allow RTS and ESFAS components to be considered both inoperable and PRA Functional.

PG&E Response:

It would not be typical for an inoperable RTS or ESFAS component to be inoperable but PRA Functional. In most cases, the inoperable channel would also be non-functional, and the RICT would be applicable only if sufficient channels remained OPERABLE such that the actuation signal could still occur. Some potential examples where RTS and ESFAS instrument channels could be inoperable and PRA functionality are the discovery of a slightly nonconservative setpoint (fraction of a percent), the discovery of the response time slightly exceeding the TS surveillance limit, or the intentional placement of an inoperable instrument channel in the trip condition.

Commitment

Commitment 1

When a risk informed completion time (RICT) is in effect for one or more inoperable instrumentation channels of TS 3.3.1 Function 9, Pressurizer Water Level - High, and risk management actions are required by the RICT Program of TS 5.5.20 and NEI 06-09, Revision 0-A, then additional monitoring of the pressurizer water level control function or placement of the affected plant equipment in manual control will be considered to manage the configuration risk associated with a possible control system transient initiated by any additional pressurizer water level channel failure.