Florida Power & Light Company, 6501 S. Ocean Drive, Jensen Beach, FL 34957

December 14, 2011

L-2011-545
10 CFR 50.90

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

Re: St. Lucie Plant Unit 2
Docket No. 50-389
Renewed Facility Operating License No. NPF-16

Response to Balance-of-Plant Branch Request for Additional Information Regarding Extended Power Uprate License Amendment Request

References:

(1) R. L. Anderson (FPL) to U.S. Nuclear Regulatory Commission (L-2011-021), "License Amendment Request for Extended Power Uprate," February 25, 2011, Accession No. ML110730116.

(2) Email from T. Orf (NRC) to C. Wasik (FPL), "St. Lucie 1 EPU – draft RAI (Balance of Plant)," November 15, 2011.

By letter L-2011-021 dated February 25, 2011 [Reference 1], Florida Power & Light Company (FPL) requested to amend Renewed Facility Operating License No. NPF-16 and revise the St. Lucie Unit 2 Technical Specifications (TS). The proposed amendment will increase the unit's licensed core thermal power level from 2700 megawatts thermal (MWt) to 3020 MWt and revise the Renewed Facility Operating License and TS to support operation at this increased core thermal power level. This represents an approximate increase of 11.85% and is therefore considered an Extended Power Uprate (EPU).

By email from the NRC Project Manager dated November 15, 2011 [Reference 2], additional information was requested by the NRC staff in the Balance-of-Plant Branch (SBPB) to support their review of the St. Lucie Unit 1 EPU License Amendment Request (LAR). The request for additional information (RAI) identified one follow-up question to a previous FPL RAI response. In subsequent dialog with the NRC Project Manager, it was identified that this Unit 1 RAI is also applicable to the St. Lucie Unit 2 EPU LAR. The response to this RAI is provided in the attachment to this letter.

A001
NRR

This submittal does not revise any existing commitments; however, it contains a new commitment to perform testing of the turbine steam admission valves and overspeed trip system as noted below:

- Testing of the speed probes will be performed off-line at refueling intervals;
- Testing of the speed detector modules will be performed off-line at refueling intervals;
- Testing of the testable dump manifolds will be performed on-line at quarterly intervals;
- Testing of the turbine control system controller overspeed logic will be performed at refueling intervals; and
- Testing of the steam admission valves will occur at 6-month intervals.

In accordance with 10 CFR 50.91(b)(1), a copy of this letter is being forwarded to the designated State of Florida official.

This submittal does not alter the significant hazards consideration or environmental assessment previously submitted by FPL letter L-2010-259 [Reference 1].

Should you have any questions regarding this submittal, please contact Mr. Christopher Wasik, St. Lucie Extended Power Uprate LAR Project Manager, at 772-467-7138.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed on December 14, 2011

Very truly yours,

Richard L. Anderson
Site Vice President
St. Lucie Plant

Attachment

cc: Mr. William Passetti, Florida Department of Health

Response to NRC Balance-of-Plant Branch Request for Additional Information

The following information is provided by Florida Power & Light (FPL) in response to the U. S. Nuclear Regulatory Commission's (NRC) Request for Additional Information (RAI). This information was requested to support the Extended Power Uprate (EPU) License Amendment Request (LAR) for St. Lucie Unit 2 that was submitted to the NRC by FPL via letter (L-2011-021) dated February 25, 2011 (Accession Number ML110730116).

In an email dated November 15, 2011 from T. Orf (NRC) to C. Wasik (FPL),"St. Lucie 1 EPU – draft RAI (Balance of Plant)," the NRC requested additional information to support their review of the St. Lucie Unit 1 EPU LAR. In subsequent dialog with the NRC Project Manager, it was identified that this Unit 1 RAI is also applicable to the St. Lucie Unit 2 EPU LAR; FPL identified this as RAI SBPB-6. The request for additional information (RAI) identified one follow-up question to a previous FPL RAI response. The response to this RAI is provided below.

SBPB-6 (Number assigned by FPL.)

In Section 2.5.1.2.2.2.2 of the Extended Power Uprate (EPU) licensing report, the licensee states the following as the current licensing basis for turbine missile protection:

The current licensing basis relies on the structural capacity of the building structures which house safety-related equipment, as well as, the separation of redundant trains of this equipment to adequately protect the reactor coolant pressure boundary, to prevent the public's exposure to unacceptable radiological consequences and to maintain the ability to safely shut down the plant in the event of a turbine disk failure.

However, Section 3.5 of the St. Lucie Updated Final Safety Analysis Report (UFSAR) specifies that missile barrier protection is based on missiles generated by disk failure at design overspeed of 120%, which does not encompass overspeed protection system failure. The Siemens Westinghouse topical report, TR-TP-04124, provides an NRCaccepted licensing basis for failures at or below design overspeed, but the licensing report does not clearly specify this analysis as the new licensing basis for protection against failure of the replacement rotors at or below design overspeed at EPU conditions. This topical report does not include an applicable evaluation of destructive overspeed failure probability.

For overspeed protection system failures, the EPU licensing report cites WCAP-16501, which updated the WCAP-11525 analyses previously accepted by the NRC and applicable to the current St. Lucie turbine overspeed protection system. However, in the response to RAI 2.5.1.2.2 in the licensee's letter dated June 22, 2011, the licensee stated that the overspeed protection system would be replaced in conjunction with the Ovation turbine control and protection system. The response also includes statements that the Ovation system enhances control

system reliability and continued usage of the existing overspeed protection system failure probability in the overspeed analysis is conservative.

Please clarify the proposed EPU licensing basis for protection against failure at or below design overspeed and provide a detailed technical basis for the continued use of the existing overspeed protection system failure probability with the Ovation overspeed protection system. The latter response should address changes in design (e.g., elimination of mechanical overspeed trip), potential for common cause/mode failure of redundant components, potential for latent failures undetected by testing of trip paths, and commitments to turbine steam admission valve and overspeed trip system testing at frequencies necessary to support the proposed reliablility.

Response

For clarity, the response to the NRC question is divided as shown below, with portions of the NRC question repeated and shown in bolded underlined text.

> **Please clarify the proposed EPU licensing basis for protection against failure at or below design overspeed...**

Siemens Westinghouse Topical Report TP-04124 (and its associated Technical Report CT-27332, Revision 2), "Missile Probability Analysis for the Siemens 13.9 M^2 Retrofit Design of Low-Pressure Turbine by Siemens AG" forms the St. Lucie Unit 2 licensing basis for failures at or below design overspeed and for destructive overspeed. The NRC approved the methodology and issued a Final Safety Evaluation for CT-27332, Rev. 2 on March 30, 2004, under TAC No. MB7964 (ML040410360).

The Siemens TP-04124 analysis considers steam admission valve testing interval up to three (3) months (i.e., quarterly). However, a six (6) month steam admission valve testing interval is being used at St. Lucie. As indicated in response to RAI SPBP-4 (2.5.1.2.2, Turbine Generator), the turbine retrofit vendor Siemens Power Generation updated the St. Lucie turbine missile analysis to address the probability of failures at or below design overspeed and for failures at destructive overspeed conditions (above 120% of rated speed). The evaluation indicates that overspeed probability (P_{10}) is a function of the maintenance and test interval of the speed control and overspeed protection system. The evaluation conservatively assumes that the probability of turbine running to 120% of rated speed is equal to 1.0. The Westinghouse Owners Group (WOG) issued WCAP-16501-P, Revision 0 (February 2006), "Extension of Turbine Valve Test frequency Up to 6 Months for BB-296 Siemens Power Generation (Westinghouse) Turbines with Steam Chests," to its participating members to provide new conditional probabilities of destructive overspeed for longer valve test frequencies based on the latest analysis and valve failure data. This information was used to extend the surveillance test interval to six months.

The turbine missile ejection frequencies for varying valve test intervals presented in WCAP-16501-P were calculated following the basic methodology described in the 1987 Westinghouse report WCAP-11525, "Probabilistic Evaluation of Reduction in Turbine Valve Test Frequency." WCAP-16501-P evaluation used updated BB-296 turbine valve

failure rates and an updated system separation frequency to extend the nominal test interval documented in Westinghouse report WCAP-14732, Revision 1 (June 1997),"Probabilistic Analysis of reduction in Turbine Valve Test Frequency for Nuclear Plants with Westinghouse BB-296 Turbines with Steam Chests." Accordingly, a probability analysis model from WCAP-14732 was used in the analysis with the following changes made to the model:

- Turbine valve (governor, throttle, reheat stop, and interceptor) failure rates were updated to reflect the past 10 years of operating experience.
- The time intervals for verifying operability of the components modeled were revised to reflect both 18-month and 24-month fuel cycles.
- An allowance has been justified for the missile ejection frequency contributions of design and intermediate overspeed events.
- The probability model's logic has been revised to include the failure of several manual valves in conjunction with currently modeled automatic valve failure.

The missile ejection frequency results in WCAP-11525, for BB-296 turbines, indicate that the design and intermediate overspeed failure probabilities are not major contributors to turbine missile ejection probability. Therefore, the study focuses on calculation of the destructive overspeed probability, consistent with the approach in WCAP-14732. Generic values for the probability of design and intermediate overspeed are based upon the results for BB-296 models presented in WCAP-11525.

Although TP-04124 (CT-27332, Rev. 2) considers valve testing intervals up to quarterly, the turbine retrofit vendor applied the 6-month test interval data for conditional probability of destructive overspeed assuming an 18-month refueling cycle.

...provide a detailed technical basis for the continued use of the existing overspeed protection system failure probability with the Ovation overspeed protection system.

WCAP-16501-P indicated that the conditional overspeed probability evaluation bounds turbines using the Ovation fault tolerant turbine control system (TCS) such as that planned for implementation on St. Lucie Unit 2. As a part of the plant change process guided by 10 CFR 50.59, an evaluation of the Ovation TCS and replacement of the mechanical overspeed trip system was performed. The reliability and fault tree analysis completed by the vendor provides the basis that the Ovation TCS, considering the St. Lucie specific application, has a low probability of failure to trip on demand.

The current value for the annual conditional probability of destructive overspeed at a 6-month turbine valve test interval is 2.58×10^{-6} (including speed sensing, trip logic and turbine valves). The Ovation TCS design (including speed sensing and trip logic) for St. Lucie Unit 2 has a probability of failure (to trip) on demand (PFD) of 7.00×10^{-10} (assuming a mean time to repair (MTTR) of 8 hours) at a quarterly test interval (the PFD is 8.77×10^{-10} when a MTTR of 72 hours is considered). Thus, effect of the Ovation TCS on the conditional probability of destructive overspeed is negligible.

To further support the conclusion that the contribution to the overall probability of failure from the replacement Ovation TCS is negligible, valve failure rates from WCAP-16501-P

were reviewed. Failure rates of the governor valves, throttle valves, reheat stop valves, interceptor valves, 20/ET solenoid valve, 20-1/OPC solenoid valve and 20-2/OPC solenoid valve are substantially greater and range from about 1.0E-07 to 1.0E-05 per hour.

The probability of destructive overspeed for the 6-month valve test interval used in the missile analysis is 1.39×10^{-7} per annum when system separation frequency is considered [this correlates to $P_{10} = 1.59 \times 10^{-6}$ for a 100,000 hour inspection interval]. Based on the updated probability data, the total probability of an external missile (P_1) for the unit at 100,000 hours inspection interval is 1.88×10^{-6} which is less than the NRC acceptance criteria of 11.42×10^{-5} (i.e., the NRC limit value for 100,000 hours). Therefore, the system reliability and overspeed probability are bounded by the current analysis for pre and post-EPU conditions.

... address changes in design (e.g., elimination of mechanical overspeed trip), potential for common cause/mode failure of redundant components, potential for latent failures undetected by testing of trip paths ...

The intended Digital Electro-Hydraulic (DEH) controls upgrade and mechanical overspeed elimination is discussed in EPU License Amendment Request – Attachment 5, Licensing Report Section 2.5.1.2.2.2.2 (Description of Analyses and Evaluations) and associated RAI Response Letter L-2011-406 dated October 12, 2011, from Richard L. Anderson to US Nuclear Regulatory Commission, "Response to NRC Balance-of-Plant Branch Request for Additional Information Regarding Extended Power Uprate License Amendment Request," (ML11287A039).

The planned TCS upgrade, which is being implemented and evaluated under the 10 CFR 50.59 plant change process, replaces the mechanical overspeed protection system and overspeed protection controller (OPC), overspeed trips, associated components and auto stop oil system, with (two) independent electronic overspeed trip systems that dump system hydraulic fluid to rapidly close the steam admission valves. These electronic overspeed trips are generated by employing multiple, diverse trip schemes via triple redundant logic channels that include triple redundant passive and active sensing elements (i.e., speed probes). The fault tolerant, diverse trip schemes provide high assurance that an overspeed trip can be produced when potentially damaging overspeed conditions are sensed.

The installation of the DEH replacement system will provide two sets of electronic overspeed trips (each using separate sensors with different technology per redundant set). The digital upgrade is implemented under the FPL/Nextera Energy Software Quality Assurance (SQA) program. The TCS application software was developed using the vendor's (i.e., Westinghouse) quality assurance process. Aspects of the digital upgrade are evaluated pursuant to the guidance in Regulatory Issue Summary (RIS) 2002-22, Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule". The replacement overspeed trip design is evaluated relative to the original (mechanical and electronic) overspeed trip design to demonstrate that comparable or improved safety margin is provided by the replacement overspeed trip design.

The replacement DEH control system is an Emerson Ovation Turbine Control System (TCS) Logic Platform similar to the platform integrated into the AP1000 Advanced Light Water Reactor (ALWR) standard design that was evaluated and accepted by the NRC in NUREG-1793, Supplement 2, "AP1000 Design Certification Amendment, Advanced Final Safety Evaluation Report, Chapter 10 - Steam and Power Conversion" (ML100910522). In the St. Lucie application, the Ovation speed detector modules (SDMs) are credited with providing an independent and diverse trip relative to the overspeed trip provided by the redundant Ovation controllers (see Figure 1 for a depiction of the St. Lucie overspeed trip system configuration).

The Ovation TCS employs a fail-safe design in that loss of power will produce a trip for the turbine trip devices. The SDMs are capable of producing overspeed trips independently. The speed detection algorithm is a simple recursive algorithm that monitors speed of the turbine and processes a trip command if turbine speed is excessive when compared to the programmed trip setpoint. The new TCS provides annunciation of equipment failures to allow timely maintenance and repair of degraded conditions; equipment redundancy and modular design are features that support on-line maintenance activities without adverse impact to TCS performance.

The turbine trip devices called Testable Dump Manifolds (TDMs) have a common design that employs solenoid valves configured to produce a two-out-of-three hydraulic trip configuration. The TDMs are of a simple design that is on-line testable and use fail-safe (de-energize to trip) configuration for the overspeed protection function.

Item 2.a; of NUREG-0800 (Standard Review Plan (SRP)) 10.2 (Revision 2/July 1981), Turbine Generator, Section III (Review Procedures) states that the defense-in-depth provided by the turbine generator protection system to preclude excessive overspeed should include diverse protection means.
The current EHC system design has overspeed trip redundancy and diversity by employing the following:

- Two parallel OPC solenoid valves to dump governor and interceptor valve emergency trip fluid to force closure of interceptor and governor valves to reduce turbine speed without a full turbine trip (at a setpoint of 103% rated speed [1854 rpm]). The extraction steam non-return valves are also closed via a fluid operated air pilot valve (the non-return valves are closed to prevent reverse flow from the extraction steam lines and feedwater heaters).
- The mechanical overspeed dumps the auto stop oil to initiate a turbine trip on overspeed setpoint (111% rated speed [1998 rpm]); this trip closes the governor, throttle, interceptor and reheat stop valves. The governor and interceptor valves are closed via the actuation of a diaphragm interface valve.
- The OPC controller also senses overspeed conditions (111.5% rated speed setpoint) and actuates a dump of the auto stop oil by energizing the 20/AST trip solenoid.

This planned TCS upgrade installs 3 active speed probes (associated with the Operator Automatic/Overspeed Protection Controller (OA/OPC) logic) and 3 passive speed probes (associated with the Emergency Trip System (ETS) controller protection logic.

The replacement system also includes an installed spare passive and an active probe that enable on-line replacement of a failed (passive and or active) probe.

Each (in-service) speed probe (sensing element) is hardwired directly to its associated SDM that provides signal conditioning and simple command logic that compares the process signal to the pre-established setpoint and actuates an integral relay that provides the individual channel trip signal. The simple signal comparison algorithm in the SDM is developed using a simple microcontroller. The SDM provides a hard-coded signal comparison - setpoint. The SDM is capable of detecting an open circuit in its associated speed probe wiring. The SDM design also allows the raw speed signal to be "passed through" to the associated redundant system controller for fault-tolerant two-out-of-three (2oo3) trip logic voting. The SDMs and redundant controllers (ETS and OA/OPC) separately and independently sense and command individual channel trips to rapidly actuate a turbine trip signal on overspeed conditions via output relay contacts. Each SDM channel is directly wired to its associated triple redundant trip solenoid (see attached figure). The normally-closed contact of the SDM output relay is employed to provide a channel trip signal. Wiring for the passive probes is routed in separate conduit from the active probes to minimize the possibility of common cause failures, particularly from electromagnetic interference.

The porting (or dumping) of hydraulic fluid is now performed using redundant and (on-line) testable dump manifolds (TDMs). TDMs are designed to rapidly de-pressurize a turbine trip header. Triple redundant solenoids with dual shuttle valves form a valve logic configuration that requires 2oo3 solenoid actuation to produce flow (i.e., actuate a turbine trip). The overspeed protection trip TDMs are fail-safe in that a loss of power or open circuit results in a trip.

- The OPC overspeed control (103% rated speed setpoint [1854 rpm]) is performed using energize to trip valves and 125 VDC control power. The process input to this logic is from the triple redundant active speed probes and logic from the redundant OA/OPC controller actuates triple redundant output relays. Each relay's normally open output contact energizes (i.e., closes) to actuate its associated TDM-3 solenoid (OPC-A, OPC-B or OPC-C). The OPC overspeed control dumps fluid from the OPC fluid header that controls the Governor and Intercept valves. The OPC fluid header is isolated from the ETS header by a check valve to preclude operation of the Throttle and Reheat Stop Valves.

- The overspeed protection trip (111% rated speed setpoint [1998 rpm]) is performed using a de-energize to trip 2oo3 solenoid valve logic configuration to dump hydraulic fluid. There are two redundant electronic overspeed trip systems that use separate TDMs, with each TDM solenoid actuated by 24 VDC power (via the SDM module) from either the ETS Remote I/O (RIO) cabinet TU002CAB or the OA/OPC RIO cabinet TU001CAB.

    - TDM-1 (de-energize to trip) is powered from TU002CAB. The process input to this logic is from the triple redundant passive speed probes. Each speed probe is connected (i.e., hardwired) to its respective SDM which is capable of processing a channel trip independently of the

redundant ETS controllers. The SDMs use simple microcontroller logic versus programmable logic function blocks used by the ETS controller (a real-time operating system is used in the redundant controllers) based on its internal logic and integral output relay. The speed signal is also passed through to the ETS controller TU102CAB in the Control Room for 2oo3 voting logic processing and actuation of output relays.

- TDM-2 (de-energize to trip) is powered from TU001CAB. The process input to this logic is from the triple redundant active speed probes. The SDM and redundant control configuration is as described above; however the trip logic is processed by the redundant OA/OPC controllers in cabinet TU103CAB that actuate separate output relays.

In addition to generic analyses completed by the vendor (Westinghouse) as supporting documentation for the Ovation platform, St. Lucie application specific Failure Modes and Effects Analysis, Software Hazards Analysis and Reliability/Fault Tree Analysis were completed to evaluate the acceptability of the DEH Controls Upgrade and to support the conclusion that the software and control system have a low probability of causing hazards, and provides adequate defensive measures in the design to minimize exposure to upsets resulting from individual component failures or unauthorized access. Aspects of the digital upgrade software lifecycle and verification and validation process are described in the Software Lifecycle, Configuration Management and Verification & Validation Plan. Also, these evaluations (both qualitatively and quantitatively) support the conclusion that the annual probability of an unsafe overspeed condition post-upgrade remains bounded by the current analyses for the St. Lucie Unit 2 Siemens Power Generation / Westinghouse turbine (with upgraded HP and LP rotors) where semi-annual valve testing is performed. It is also noted that governor valve failures are the dominant contributors to destructive overspeed probability and that individual elements of the electro-hydraulic system (including trip system) have a smaller impact.

The potential for latent failures (or latent software errors) that adversely impact the upgraded DEH system (including the overspeed trip systems) performance following design, implementation and testing is low. The Ovation TCS is a mature design. The platform history and operating experience (which includes nuclear and non-nuclear steam and feedwater pump turbine control applications) demonstrates that the platform is stable and capable of operating on demand with high reliability. The process used for the design, implementation and (verification & validation) testing of the TCS provides sufficient assurance that software errors are identified prior to commissioning and that software errors that could adversely impact protective functions are precluded. The Ovation platform software release is reviewed to evaluate the resolution of software defects. If software errors are identified prior to and during initial commissioning, these errors are documented, evaluated and resolved by the vendor under the vendor's configuration management process. The resolution of these issues would be tracked and documented under the FPL change management process. During TCS operation, system testing, change management and configuration management processes in conjunction with SQA and corrective action processes provide high assurance that latent errors (with a low likelihood of occurrence) are detected and corrected in a timely manner.

The redundancy, self-diagnosing and fault detecting defensive measures (including sensing element quality discrimination) support the high reliability claim for the TCS upgrade. The Ovation network is a robust, fault-tolerant, high-speed, communications network designed for real-time mission critical control applications. Each input is read on separate I/O cards (each on a separate communication branch in the controller) to eliminate a single point of failure in the I/O hardware. This approach is used for all critical-control and protection-input parameters.

The Westinghouse design philosophy does not rely on the network for the data used in critical control loops. Critical loops (such as those performing protective - tripping functions) are contained within a single controller, or data is shared by some other method (data may be shared via the hardwired inputs between controllers).

- Several watchdog timers (WDTs) are employed in Ovation controllers to verify normal operation and to discriminate the health of the controllers and associated I/O devices.
- Ovation controllers contain a collection of internal tests and diagnostics to verify system health, detect failed I/O modules, and validate data, alarm, and failover, if necessary.
- Ovation algorithms extensively used in the application perform validation checks to the inputs to ensure data validity before using it. Any input that does not pass the check will result in setting the point value to BAD quality. Additionally, on start-up, the Ovation controller performs numerous self-diagnostic checks to verify internal system integrity.
- All data exchanges between components utilize checksums and/or cyclic redundancy-check-based error detection mechanisms. Lost packets are recovered utilizing mechanisms that are inherent in the associated protocol(s).
- If an input or sensor has failed or is providing bad data, the controller's diagnostics and comparison programming algorithms will process the data to determine its quality. These quality propagation algorithms catalog the data into different categories.
- A failed redundant component can be replaced on-line.
- The overall Ovation control system is qualified for electro-magnetic compatibility (EMC) consistent with the guidance in Regulatory Guide 1.180 Revision 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interferences in Safety-Related Instrumentation and Control Systems.
- The diversity techniques employed in the Ovation TCS are consistent with guidance in NUREG/CR-6303 and NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems (December 2008). The Ovation TCS uses different application technologies for the development of overspeed trips provided by the speed detector modules and the Ovation controllers.
- Logical and physical access measures are employed to control unauthorized and authorized access to specific user-defined levels/accounts/roles. The TCS operates independently on its own self-contained network. Security features are utilized where communication with external devices (e.g., time synchronization) is required. However, it is noted that the Ovation TCS does not rely on external communications or network operation to perform its protective control functions such as issuing overspeed trip commands.

With implementation of the Ovation DEH controls upgrade, a higher degree of fault-tolerance and overspeed trip assurance is achieved by using dual-redundant logic controllers in each logic cabinet and by implementing cross-tripping between logic control cabinets whereby a trip signal processed in one cabinet is also hardwired using (triple redundant) isolated contact outputs to produce a contact logic - voting trip via the other cabinet trip actuation equipment. Therefore, multiple diverse trip paths are employed to provide high assurance that a turbine trip can be achieved especially on overspeed conditions or on multiple equipment failures.

The diversity and redundancy implemented as a part of the DEH replacement system design meets industry standard requirements based on the NRC guidance on acceptable types of diversity contained in NUREG/CR-6303. A software common cause failure that prevents overspeed protection is precluded by the use of SDMs (which use a simple microcontroller and simple signal comparison algorithm) with hard coded overspeed trip setpoint and Ovation controllers (microprocessors running a deterministic real-time operating system) using voting logic software that actuate separate relays for independent tripping in the event of an overspeed condition. The replacement system satisfies equipment diversity for tripping in the case of the SDMs and ETS or OA/OPC controllers. The redundant TDMs are of a similar design but are testable on-line and simple components comprise the TDM design. The (24 VDC) TDMs used for overspeed protection are de-energize to actuate (i.e., dump hydraulic fluid) and will generate a trip upon loss of power. The 125 VDC TDM used for OPC control action at 103% rated speed is energize to actuate. The SDMs use normally closed output contacts to provide a trip signal. Therefore, a failure of this contact may prevent an individual channel trip. However, redundancy built into the design and 2oo3 coincidence logic provides acceptable margin. Additionally, system diagnostics and health checks are designed to detect a failed SDM. The TCS can issue trip commands through median selector logic using the remaining good quality speed signal if exactly two speed signals in the set indicate bad quality. The TCS will issue an automatic trip if all six speed signals indicate bad quality.

The historical industry standard TCS overspeed trip design included an electronic overspeed and a mechanical overspeed. As the quality and reliability of digital control systems has improved and fault avoidance/fault tolerance has improved, newer TCS designs have eliminated the mechanical overspeed trip mechanism. Elimination of this device has been driven by several factors including: the imprecision of the spring mechanism, its reliability is below that of the new fault tolerant electronic TCS designs, and the maintenance costs and personnel test hazards associated with the mechanical overspeed trip system are comparatively higher than modern electronic overspeed trip systems based on studies conducted by EPRI (EPRI Technical Report 1013461, November 2006, Turbine Overspeed Trip Modernization, Requirements and Implementation Guidance). The mechanical overspeed trip provided a level of redundancy and diversity. This level of redundancy is now implemented electronically and the reliability of the electronic TCS exceeds the mechanical system. The probability of turbine overspeed following implementation of the DEH upgrade is not increased. The turbine overspeed modernization (i.e., implementation of electronic overspeed trips in lieu of mechanical overspeed trips) provides a modern fault-tolerant electronic

overspeed design that is more reliable, repeatable, and results in a system that provides low risk with respect to personnel safety and equipment damage during on-line testing.

Although different components and software are being implemented with new logic/algorithms, the failure modes assumed for the DEH system are not changed and remain bounding.

... commitments to turbine steam admission valve and overspeed trip system testing at frequencies necessary to support the proposed reliability.

Acceptance Criteria Item II.1 of SRP Section 10.2 (op. cit.) states that the overspeed protection system should meet the single-failure criterion and should be testable when the turbine is in operation. The St. Lucie overspeed protection is single-failure proof and is testable on-line. Two separate controllers and two separate sets of triple redundant speed detector modules are capable of detecting and producing a turbine trip on overspeed (refer to the attached figure). The Ovation TCS uses separate sets of triple redundant active and passive speed sensing probes. Testing of the overspeed trip system or components will be performed as follows:

- Testing of the speed probes will be performed off-line at refueling intervals. The analog signals are displayed for channel comparison. The analog signal quality discrimination is always active and an alarm occurs on speed deviation between any two of the three channels (for both passive and active probe sets).
- Testing of the Speed Detector Modules will be performed off-line at refueling intervals.
- Testing of the Testable Dump Manifolds will be performed on-line (one channel at a time) at a quarterly interval.
- Testing of the TCS Controller overspeed logic will be performed during startup at a refueling interval. This test will verify overspeed trip capability of the redundant controllers. The test will be conducted at a reduced setpoint. The setpoint is automatically returned to the overspeed trip setting following termination of the overspeed trip test. The reduced setpoint is used to minimize turbine stresses that occur during overspeed conditions.
- Testing of the steam admission valves will occur at the current 6 month interval.

The testing and test intervals described above are consistent with the assumptions of the application specific reliability analysis for the St. Lucie Unit 2 TCS upgrade.

Figure 1

Turbine Overspeed Trip System