Ms. Annette L. Vietti-Cook
Secretary of the Commission
United States Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: 2.206 Petition on Current Operating Nuclear Power Plants – Open Phase Conditions in Electric Power System Which Lead to Loss of Safety Functions of Both Offsite and Onsite Power Systems (NRC Bulletin 2012-01)

I. SPECIFIC ACTIONS REQUESTED

Pursuant to 10 C.F.R. § 2.206, we are submitting this Petition to the United States Nuclear Regulatory Commission (NRC) requesting immediate enforcement actions against the licensees of current operating nuclear power plants. Specifically, we are requesting either (i) the NRC **issue Orders** which require immediate corrective actions including compensatory measures to address the operability of electric power systems in accordance with their Plant Technical Specifications, and to implement plant modifications in accordance with current NRC regulatory requirements and staff guidance provided in the references below; **or** (ii) **issue Orders** to immediately shutdown the nuclear power plants that are operating without addressing the significant design deficiency identified in NRC Bulletin 2012-01, "Design Vulnerability in Electric Power System," since the licensees are not in compliance with their Technical Specifications 3.8.1 (typical) requirements related to onsite and offsite power systems.

II. BACKGROUND

Based on the Byron Station operating event, the staff issued U.S. Nuclear Regulatory Commission (NRC), Information Notice 2012-03, "Design Vulnerability in Electric Power System," dated March 1, 2012. On July 27, 2012, the staff issued NRC Bulletin 2012-01, "Design Vulnerability in Electric Power System," to confirm that licensees comply with Title 10 of the Code of Federal Regulations, (10 CFR) Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," General Design Criterion (GDC) 17, "Electric Power Systems," or principal design criteria specified in the updated final safety analysis report, 10 CFR 50.55a(h)(2), and 10 CFR 50.36. Specifically, the NRC requested licensees to provide information by October 25, 2012, regarding (1) the protection scheme to detect and automatically respond to a single phase open circuit condition or high impedance ground fault condition on offsite power circuits, and (2) the operating configuration of engineered safety features (ESF) buses at power. The NRC staff has reviewed the information that NRC licensees provided and the details of this review is documented in a Summary Report dated February 26, 2013. The staff determined that all nuclear facilities are susceptible to this design vulnerability except one plant and recommended that NRC takes prompt regulatory action.

III. SAFETY SIGNIFICANCE

At Byron, a failure to design the electric power system's protection scheme to detect the loss of a single phase between the transmission network and the onsite power distribution system resulted in degraded and unbalanced voltage conditions on redundant ESF buses. This led to tripping of equipment that is safety related and important to safety that is required for normal plant operation and controlled safe shutdown. The lack of an adequate detection scheme for open phase condition(s) allowed the degraded offsite power system to remain connected to ESF buses and prevented the onsite AC sources from starting and powering the safety related buses. As a consequence, neither the onsite (emergency diesel generators) nor the offsite electric power system was able to perform its intended safety functions (i.e., to provide electric power to the ESF buses with sufficient capacity and capability to permit functioning of structures, systems, and components (SSCs) important to safety) to support safe shutdown of the plant.

The Byron event identified a vulnerability in the design of US and international operating plants. The current design requires an accident signal to automatically connect the emergency core cooling systems to the preferred power source to mitigate the consequences of a design basis event. As such, if the preferred power source has an undetected open phase condition, redundant trains of electrical equipment (electric motors that drive the pumps and valves) could burn out in few minutes and therefore will not be available for safe shutdown, even after restoration of an operable power source. In some cases, individual protective schemes for specific loads may isolate the load. In such cases, manual actions, outside of control room, may be required to reset the protective device(s) and start the specific loads, thereby delaying the response time assumed in accident analysis. Since a common degraded offsite power source can potentially degrade or disable both trains of the emergency core cooling system, the protection scheme must automatically initiate isolation of the degraded offsite power source and transfer the safety buses to the onsite or back up power source within the time period assumed in the accident analysis in accordance with codes and standards specified in NRC requirements 10 CFR 50.54 (jj) and 10 CFR 50.55a(h)(2) or 10 CFR 50.55a(h)(3).

To-date, thirteen open phase events have been identified over the last fourteen years (both US and international). The most recent events occurred at Oconee Nuclear Station in December 2015 where two separate transformers required for safe shutdown of three operating nuclear units were identified with open phase conditions. Since the transformers are common to one onsite and one offsite power source, both, power sources were rendered inoperable indicating that the lessons learned and manual compensatory actions implemented after the Byron Event were ineffective.

The NRC's Accident Sequence Precursor analysis for the Byron event indicated the risk, Conditional Core Damage Probability (CCDP), as 1×10^{-4}.

Operating experience indicates that open phase condition is a highly probable event with high consequence that results in common cause failures of multiple accident mitigation systems and barrier integrity systems. It is a significant safety concern since a design basis event concurrent with an open phase condition would in most cases result in the plant exceeding criteria specified in Title 10 of the Code of Federal Regulations (10 CFR) 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors."

III. BASIS AND JUSTIFICATION

The NRC has established regulations that require performance based criteria such as Appendix A to Part 50—General Design Criteria for Nuclear Power Plants. For example, the Introduction section states, in part, that "Under the provisions of § 50.34, an application for a construction permit must include the principal design criteria for a proposed facility. The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for SSCs important to safety; that is, SSCs that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

The GDC establish minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have been issued by the Commission. The GDC are also considered to be generally applicable to other types of nuclear power units and are intended to provide guidance in establishing the principal design criteria for such other units."

GDC 17 establishes requirements for the electric power system design of nuclear power plants for which a construction permit application was submitted after the Commission promulgated the GDC in 1971. Specifically, Criterion 17, "Electric power systems," states:

> An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.
>
> The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their safety functions assuming a single failure.
>
> Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. --------- One of these circuits shall be designed to be available within a few seconds following a loss-of-coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.
>
> Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies.

Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Electric Power (NUREG-0800 (Formerly NUREG-75/087), Chapter 8), provides NRC staff review and acceptance criteria for verifying NRC regulations that are applicable to electric power systems. Accordingly, the NRC staff reviews (1) an applicant's description of the offsite power system with regard to the interrelationships between the nuclear unit, the utility grid, and the interconnecting grids; (2) the applicant's description of the onsite power systems with regard to the availability of sufficient power to mitigate design-basis events given a loss of the offsite power system and a single failure in the onsite power system; (3) the applicant's description of the capability to withstand and recover from a station blackout event of a specified duration; and (4) the acceptance criteria to be implemented in the design of the above systems.

SRP Section 8.2, "Offsite Power System," Section 8.3.1, "A-C Power Systems (Onsite)," Section 8.3.2, "D-C Power Systems (Onsite)," and Section 8.4, "Station Blackout," contain the specific review contain interfaces for each SRP section. In addition, Table 8-1 of this SRP section lists the acceptance criteria the staff applies to electric power systems. Implementation of these criteria in accordance with applicable regulatory guides and branch technical positions (BTPs) will provide assurance that systems will perform their design safety functions when required in accordance with GDC 17.

For current operating nuclear power plants designed before the promulgation of GDC 17, the principal design criteria specified in the plant UFSAR for both offsite and onsite power systems sets forth criteria similar to GDC 17, which requires, among other things, that plants have an offsite and an onsite electric power system with adequate capacity and capability to ensure the functioning of SSCs important to safety in the event of anticipated operational occurrences and postulated accidents.

The following electrical design criteria were used for licensing of nuclear power plants by Atomic Energy Commission (AEC). They represent the Atomic Industrial Forum (AIF) version of proposed criteria issued by the AEC for public comments. The specific criteria specified in the plant UFSAR for electric power system requirements are:

> AIF- Criterion 21
>
> Sufficient normal and emergency sources of electrical power must be provided to assure a capability for prompt shutdown and continued maintenance of the reactor facility in a safe condition under all credible circumstances.
>
> AIF- Criterion 24
>
> In the event of loss of all offsite power, sufficient alternate sources of power shall be provided to permit the required functioning of the protection systems.
>
> AIF- Criterion 39
>
> An emergency power source shall be provided and designed with adequate independency, redundancy, capacity, and testability to permit the functioning of the engineered safety features and protection systems required to avoid undue risk to the health and safety of the public. This power source shall provide this capacity assuming a failure of a single active component.

Furthermore, the AEC published in Federal Register, Vol 32, No.132 -Tuesday, July 11, 1967, the following the proposed rule:

> The Atomic Energy Commission has under consideration an amendment to its regulation, 10 CFR Part 50."Lcensing of Production and Utilization Facilities," which would add an Appendix A, "General Design Criterion, for Nuclear Power Plant Construction Permits." The purpose of the proposed amendment would be to provide guidance to applicants in developing the principal design criteria to be included in applications for Commission construction permits. These General Design Criteria would not add any new requirements, but are intended to describe more clearly present Commission requirements to assist applicants in preparing applications.
>
> The proposed amendment would complement other proposed amendments to Part 50 which were published for public comment in the Federal Register on August 16, 1966

(31 F-R. 10891). The proposed amendments to Part 50 reflect a recommendation made by a seven-member Regulatory Review Panel, appointed by the Commission to study:

(1) The programs and procedures for the licensing and regulation of reactors and (2) the decision-making process in the Commission's regulatory program. The Panel's report recommended the development, particularly at the construction permit stage of a licensing proceeding, of design criteria for nuclear power plants. Work on the development of such criteria had been in process at the time of the Panel's study.

As a result, preliminary proposed criteria for the design of nuclear power plants were discussed with the Commission's Advisory Committee on Reactor Safeguards and were informally distributed for public comment in Commission Press Release H-252 dated November 22, 1965. In developing the proposed criteria set forth in the proposed amendments to Part 50, the Commission has taken into consideration comments and suggestions from the Advisory Committee on Reactor Safeguards, from members of industry, and from the public... The Commission expects that the provisions of the proposed amendments relating to General Design Criteria for Nuclear Power Plant Construction Permits will be useful as interim guidance until such time as the Commission takes further action on them......

The criteria are designated as General Design Criteria for Nuclear Power Plant Construction Permits to emphasize the key role they assume at this stage of the process. The criteria, have been classified as Category A or Category B. Experience has shown, that more definitive information is needed at the construction permit stage for the Items listed in Category A than for those in Category B.

Applicable electric power system GDCs are:

Criterion 21-Single Failure Definition (Category B). Multiple failures resulting from a single event shall be treated as a single failure.

Criterion 24-Emergency Power for Protection Systems (Category B). In the event of loss of all offsite power, sufficient alternate sources of power shall be provided to permit the required functioning of the protection systems.

Criterion 39-Emergency Power for Engineered Safety Features (Category A). Alternate power systems shall be provided and designed with adequate independency, redundancy, capacity, and testability to permit the functioning required of the engineered safety features. As a minimum, the onsite power system and the offsite power system shall each, independently, provide this capacity assuming a failure of a single active component in each power system.

The AEC published the final rule that added 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," in the Federal Register (36 FR 3255) on February 20, 1971, with the rule effective on May 21, 1971.

In addition, other GDCs such as 33, 34, 35, 38, 41, and 44 and equivalent Principle Design Criteria require that offsite power supplies including electrical distribution systems be available (for onsite electric power system operation assuming offsite power is not available and for offsite electric power system operation, assuming onsite power is not available, the system safety function can be accomplished, assuming a single failure) for reactor coolant makeup during small breaks, residual heat removal, emergency core cooling, containment atmosphere cleanup, and cooling water for SSCs important to safety during normal and accident conditions.

We note that the NRC staff's interpretation of the of the GDC 17 requirements or equivalent principal design criteria, as specified in SRP Section 8.1, Table 8.2, is described below:

Both an offsite and onsite power system shall be provided, each independent of the other and capable of providing power for all safety functions. The offsite and onsite power systems considered together must meet the single failure criterion on a system basis without losing the capability to provide power for all safety functions, i.e., the two systems considered together must be capable of sustaining a complete loss of offsite power and a single failure in onsite system, without losing the capability to provide power for the minimum required safety functions.

The complete onsite electric power system (Class 1E) must be capable of sustaining a single failure without loss of capability to provide power for the minimum required safety function. This means that the licensees must follow the single failure, redundancy, and independence requirements in accordance with the design criteria provided in Institute of Electrical and Electronic Engineers (IEEE) Standards 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE 603 "Standard Criteria for Safety Systems for Nuclear Power Generating Stations" as endorsed by RG 1.153, "Application of the Single-Failure Criterion to Safety Systems," provides criteria to evaluate all aspects of the electrical portions of the safety-related systems and onsite power system, including basic criteria for addressing single failures in accordance with its licensing basis to comply with the requirements specified in 10 CFR 50.55a(h)(2).

The onsite power system must be capable of performing its safety function assuming a single failure. For onsite power system, IEEE Standards 279 and 603 require that the protection systems must automatically initiate appropriate protective actions whenever a condition monitored by the system reaches a preset level. Once initiated, protective actions should be completed without manual intervention to satisfy the applicable requirements delineated in IEEE standards.

Specifically, IEEE 279-1971, Section 4.2, "Single Failure Criterion," states:

> Section 4.2 of IEEE Std. 279-1971 states, in part, that "any single failure within the protection system shall not prevent proper protective action at the system level when required." and "Note: "Single Failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables." Section 4.7.2 "Examples of credible failures include short circuits, open circuits, grounds, and application of maximum credible ac or dc potential. A failure in an isolation device is evaluated in the same manner as failure of other equipment in the protection systems." Section 4.6 ".... Shall be independent and physically separate to accomplish decoupling of the effects of unsafe environmental factors, electric transients, ...reduce the likelihood of interactions between channels during .... or in the event of channel malfunction."

IEEE No 279, August 1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," states:

> Section 4.1 - General Functional Requirement. The nuclear power plant protection

system shall, with precision and reliability, automatically initiate appropriate protective action whenever a plant condition monitored by the system reaches a preset level.

Section 4.2 - Single Failure Criterion. Any single failure within the protection system shall not prevent proper protection system action when required.

Note: "Single failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. ....

Section 4. 7 - Control and Protection System Interaction. Where a plant condition that requires protective action can be brought on by a failure or malfunction of the control system, and the same failure or malfunction prevents proper action of a protection system channel or channels designed to protect against the resultant unsafe condition, the remaining portion of the protection system shall independently meet the requirements of paragraphs 4.1 and 4.2.

Regulatory Guide (RG) 1.53, "Application of the Single-Failure Criterion to Safety Systems," Revision 3, states that conformance with the requirements of IEEE Std 379-2000, provides methods acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.

RG 1.75, "Physical Independence of Electric Systems," Revision 1, states that the guidance in IEEE Std. 384-1974, "IEEE Trial-Use Standard Criteria for Separation of Class IE Equipment and Circuits," dated, March 15, 1974, is generally acceptable to the NRC staff and provides an adequate basis for complying with IEEE Std. 279-1971 and the Commission's GDC 3, 17, and 21 of Appendix A to 10 CFR Part 50 with respect to the physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.

IEEE Std. 603-1991 states:

- Section 5.1, "Single-Failure Criterion," states: The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std. 379-1988 provides guidance on the application of the single failure criterion.

- Section 5.2, "Completion of Protective Action," states: The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal.

In addition to the above guidance, Section 4.5 of IEEE Std. 308-2001, "Power Quality," which is endorsed by RG 1.32, requires that variations of voltage, frequency, and waveform (including endorsed by RG 1.32, requires that variations of voltage, frequency, and waveform (including the effects of harmonic distortion) in the Class 1E power systems during any mode of plant operation shall not degrade the performance of any safety system load below an acceptable level. The NRC staff position has always been that power quality issues caused by any event or condition that could affect redundant ESF buses and loads must have features such as physical separation, electrical isolation, independence, redundancy, and meet qualification requirements. These features shall be included in the design to aid in preventing a mechanism by which a single design basis event could cause redundant equipment within the plants' Class 1E power system to be inoperable.

Further, the earliest version of this standard, IEEE Std. 308-1971 (Safety Guide 32), principal design criteria's for Class IE electric systems require that systems be designed to assure that any design basis event (i.e., single equipment malfunction) will not cause a loss of electric power to a number of engineered safety features, surveillance devices, or protection system devices sufficient to jeopardize the safety of the station. Even with subsequent revision to this standard (i.e., 308-1974 thru 308-2012) this fundamental principal design criteria has not changed.

In short, these IEEE Standards state that the protection systems must automatically initiate appropriate protective actions whenever a condition monitored by the system reaches a preset level. Once initiated, protective actions should be completed without manual intervention to satisfy the applicable requirements delineated in IEEE standards.

In addition, NRC Safety Guide 6, "Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems," March 10, 1971, states that:

> General Design Criterion 17 requires that onsite electrical power systems have sufficient independence to perform their safety functions assuming a single failure. This safety guide describes an acceptable degree of independence between redundant standby (onsite) power sources and between their distribution systems...... Common mode failures as well as random single failures should be considered in the analysis.

The draft versions of Safety Guides 6 and 32 have been used by the AEC staff as guidance for verifying compliance with the above AEC principal design criteria requirements for electric power system.

Therefore, both GDC and pre-GDC nuclear power plants' current licensing basis require an onsite power system and offsite power system with adequate capacity and capability to mitigate design basis events, conditions, and accidents. It also requires that if the offsite (preferred) power system cannot perform its intended safety function, the plant design is required to automatically transfer the ESF buses and loads to the onsite power system within the time specified in the accident analysis (i.e., this is protective function and it has to meet the provisions of IEEE 279 or 603 as stated before). The onsite power system is Class 1E (safety-related), therefore, the current licensing basis for operating nuclear power plants requires meeting single failure, redundancy, separation, and independence criteria. Any failure that causes failure or degradation of the offsite power system such open phase, undervoltage, and degraded voltage must be monitored by the ESF bus and take automatic protective action to meet the Chapter 15 accident analysis assumptions. In addition, the onsite power system must also meet the protection system requirements specified in NRC GDCs 20-24 or equivalent principle design criteria specified in the UFSAR for pre-GDC plants.

As of this filing, the NRC has not informed licensees that they are not in compliance with applicable regulatory requirements and their licensing and design basis for electric power systems.

Therefore, the licensing bases and design bases for all U.S nuclear power plants require that both power offsite and onsite power systems must be operable and capable of supporting all design bases functions. In short, any failures in an offsite power system or onsite power system must not disable the safety functions of emergency core cooling and vital safety systems to protect the health and safety of the public. In addition, the onsite power system must be in compliance with the single failure criteria, redundancy, separation, and independence criteria in accordance with NRC requirements 10 CFR 50.55a(h)(2) or (h)(3), and the codes and standards requirements specified in 10 CFR 50.54 (jj).

The actions requested by this petition will rectify the open phase design vulnerability identified in Bulletin 2012-01 and provide reasonable assurance of public health and safety in accordance with the current NRC requirements.

Sincerely,

Roy Mathew
18837 Falling Star Rd Germantown, Maryland 20874

Sheila Ray
109 Swarthmore Ave, Gaithersburg, MD 20877

Swagata Som
18031 Wheatridge Drive, Germantown, MD 20874

Gurcharan Singh Matharu
110 Harbour Town Court, New Orleans, LA 70131

Tania Martinez Navedo
13529 Wisteria Drive, Germantown, MD 20874

Thomas Koshy
218 Lower Country Dr. Gaithersburg, MD 20877

Kenneth Miller
174 Canal Way, Shepherdstown, WV 25443

CC:
Stephen G. Burns, Chairman
William C. Ostendorff, Commissioner
Kristine L. Svinicki, Commissioner
Jeff Baran, Commissioner

References:

Information Notice 2012-03, "Design Vulnerability in Electric Power System," dated March 1, 2012 (ADAMS Accession No. ML120480170)

U.S. Nuclear Regulatory Commission, Licensee Event Report, Byron Station, Unit 1 and Unit 2, ADAMS Accession No. ML12272A358

NRC Bulletin 2012-01, "Design Vulnerability in Electric Power System," (Accession No. ML12074A115)

NRC Bulletin 2012-01, "Design Vulnerability in Electric Power System," Summary Report dated February 26, 2013 (ADAMS Accession No. ML13052A711).

U.S. Nuclear Regulatory Commission, NRC letter dated November 25, 2014, from William Dean, Office of Nuclear Reactor Regulation to Anthony Pietrangelo, Nuclear Energy Institute, ADAMS Accession Nos. ML14120A196 and ML14120A203.

U.S. Nuclear Regulatory Commission, "Status of the Accident Sequence Precursor Program and the Standardized Plant Analysis Risk Models," SECY-13-0107, dated October 4, 2013, ADAMS Accession No. ML13232A062.

U.S. Nuclear Regulatory Commission, "Open Phase Conditions in Electric Power System," Advisory Committee on Reactor Safeguards (ACRS) letter dated December 17, 2014, regarding the ACRS review of BTP 8-9, ADAMS Accession No. ML14343A485.

U.S. Nuclear Regulatory Commission, "Open Phase Conditions in Electric Power System," Staff's Response to ACRS letter dated December 17, 2014, regarding BTP 8-9, ADAMS Accession No. ML14364A348.

Institute of Electrical and Electronics Engineers, IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Stations.”

Institute of Electrical and Electronics Engineers, IEEE Std. 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations.”
ML14120A196

U.S. Nuclear Regulatory Commission, “Criteria for Power, Instrumentation, and Control Portions of Safety Systems,” Regulatory Guide 1.153.

U.S. Nuclear Regulatory Commission, “Criteria For Power Systems For Nuclear Plants.” Regulatory Guide 1.32.

U.S. Nuclear Regulatory Commission, “Availability of Electric Power Sources.” Regulatory Guide 1.93.