[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Part 73

[Docket No. PRM-73-17; NRC-2013-0214]

Programmable Logic Computers in Nuclear Power Plant Control Systems

AGENCY: Nuclear Regulatory Commission.

ACTION: Petition for rulemaking; denial.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is denying a petition for rulemaking (PRM), filed by Mr. Alan Morris (petitioner) on March 14, 2013, as supplemented ~~through~~ most recently on December 19, 2013. The petition was docketed by the NRC on February 7, 2014, and was assigned Docket No. PRM-73-17. The petitioner requested that the NRC require that his "new-design programmable logic computers [PLCs]" be installed in the control systems of nuclear power plants to block malware attacks on the industrial control systems of those facilities. In addition, the petitioner requested that nuclear power plant staff be trained "in the programming and handling of the non-rewriteable memories" for nuclear power plants. The NRC is denying the petition because the petitioner did not ~~failed to~~ present any significant new information or arguments that would support the requested changes, nor has he demonstrated that a need exists for a new regulation ~~provision~~ requiring the installation of his new-design PLCs in the control systems of NRC-licensed nuclear power plants.

DATES: The docket for the petition for rulemaking PRM-73-17 is closed on **[INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Please refer to Docket ID **NRC-2013-0214** when contacting the NRC about the availability of information regarding this petition. You may obtain publicly-available documents related to the petition using any of the following methods:

- **Federal Rulemaking Web Site:** Go to http://www.regulations.gov and search for Docket ID **NRC-2013-0214**. Address questions about NRC dockets to Carol Gallagher; telephone: 301-415-3463; e-mail: Carol.Gallagher@nrc.gov. For technical questions, contact the individual listed in the FOR FURTHER INFORMATION CONTACT section of this document.
- **NRC's Agencywide Documents Access and Management System (ADAMS):** You may obtain publicly-available documents online in the ADAMS Public Documents collection at http://www.nrc.gov/reading-rm/adams.html. To begin the search, select "ADAMS Public Documents" and then select "Begin Web-based ADAMS Search." For problems with ADAMS, please contact the NRC's Public Document Room (PDR) reference staff at 1-800-397-4209, 301-415-4737, or by e-mail to pdr.resource@nrc.gov. The ADAMS accession number for each document referenced in this document (if that document is available in ADAMS) is provided the first time that a document is referenced. In addition, for the convenience of the reader, the ADAMS accession numbers are provided in a table in the section of this document entitled, Availability of Documents.
- **NRC's PDR:** You may examine and purchase copies of public documents at the NRC's PDR, Room O1-F21, One White Flint North, 11555 Rockville Pike, Rockville, Maryland 20852.

FOR FURTHER INFORMATION CONTACT: Natreon Jordan, Office of Nuclear Reactor Regulation, telephone: 301-415-7410, e-mail: Natreon.Jordan@nrc.gov, U.S. Nuclear Regulatory Commission, Washington DC 20555-0001.

I. The Petition

Section 2.802 of ~~title~~ Title 10 of the *Code of Federal Regulations* (10 CFR), "Petition for rulemaking," provides an opportunity for any interested person to petition the Commission to issue, amend, or rescind any regulation. A § 2.802 petition was filed by the petitioner on March 14, 2013, ~~as~~ and was supplemented several times through December 19, 2013. (ADAMS Accession No. ML14016A458). On February 7, 2014, (79 FR 7406), the NRC published a notice of receipt of PRM-73-17. The petitioner requested that the NRC amend its regulations that protect digital computer and communication systems and networks. The petitioner requested that the NRC specifically require that ~~his~~ "new-design programmable logic computers," with his patented write-once, read-many (WORM) media, be installed in the control systems of nuclear power plants in order to "block malware attacks on the industrial control systems of those facilities." The petitioner also requested that nuclear power plant staff "be trained to maintain and secure records of all memory programming," and recommended "maintenance in secure storage of programmed memories, as specified in this petition, which may be again employed, as the control systems of critical facilities are essentially steady-state." The petitioner stated that the proposed action would "[r]educe impact on quality of the natural and social environments by stopping disastrous events at critical facilities."

The NRC staff sent a letter to the petitioner on June 12, 2014 (ADAMS Accession No. ML14120A006), asking the petitioner to provide additional information. Staff specifically asked the petitioner:

- To indicate the inadequacies that he identified in the NRC's current regulatory approach (i.e., performance-based, programmatic) and framework (i.e., NRC's cyber security rule at § 73.54 and Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities") that would be remedied by the proposed rulemaking. Specifically, what cyber threat or vulnerability is not addressed by the current NRC regulations and guidance?
- If one of the PLCs with his patented ~~write-once, read-many (~~WORM~~)~~ media has been installed in any operating facility (nuclear or non-nuclear)? Are these PLCs alone sufficient to protect against cyber threats? What other cyber controls may be required at nuclear power plants if a PLC with his patented WORM media is installed?

The petitioner responded to the NRC letter in a series of e-mails dated June 18, 2014, and June 19, 2014. (ADAMS Accession Nos. ML14181B296, ML14181B276, ML14181B286, and ML14181B270).

Based on the petition and the petitioner's responses to requests for additional information, the NRC staff identified three issues raised by the petitioner:

Issue 1: PLCs currently installed in U.S. nuclear power plants are vulnerable to malware attacks that could negatively affect or challenge plant safety and control systems. The petitioner stated that malware can "maliciously reprogram the re-writeable memories of the present programmable logic computers" in the control systems of nuclear power plants.

Issue 2: By using the petitioner's patented PLC design, nuclear power plant safety and control systems would be safe from malware attacks.

Issue 3: Nuclear power plant staff should be trained to maintain and secure records of all memory programming, and recommends maintenance in secure storage of programmed

memories that may be again employed, as "the control systems of critical facilities are essentially steady-state."

The NRC staff decided not to ~~provide an opportunity for~~ seek public comment on PRM-73-17 because no additional information was needed for the NRC staff's evaluation of the petitioner's claim.

II. Reasons for Denial.

The NRC is denying the petition because the petitioner ~~failed to~~ did not present any significant new information or arguments that would support the requested changes, nor has he demonstrated a need for a new requirement ~~provision~~ for his new-design of PLCs in nuclear power plant control systems. This section provides detailed responses to the issues raised in the petition.

Issue 1: PLCs that are currently installed in nuclear power plant control systems are vulnerable to malware attacks that could negatively affect or challenge plant safety and control systems.

NRC Response:

The NRC disagrees with Issue 1 because the petitioner ~~disregards~~ does not take into account the comprehensive NRC cyber security program requirements for nuclear power plants in § 73.54. Section 73.54, "Protection of digital computer and communication systems and networks," which is known as the NRC's "cyber security rule," requires licensees to protect digital systems in nuclear power plants from cyber attacks. The cyber security rule presumes that any digital system (including PLC designs) is vulnerable to various cyber attacks. The regulations in § 73.54 establish a series of performance-based requirements to ensure that the

functions of digital computers, communication systems, and networks are protected from cyber attack. In particular,
§ 73.54(a)(1) requires nuclear power plant licensees to protect digital computers, communications systems, and networks associated with the following:

- safety-related and important-to-safety functions;
- security functions;
- emergency preparedness functions, including offsite communications; and
- support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness (SSEP) functions.

As required by §§ 73.54(b)(2) and 73.55(b)(8), a nuclear power plant licensee must establish, implement, and maintain a cyber security program that protects any digital system, network, or communication system associated with SSEP functions. Licensees are required to submit their cyber security plans to NRC for review and approval. Once approved, these plans become part of the licensee's licensing basis, and compliance with the plans is evaluated by the NRC during periodic inspections. Civil penalties may be imposed in the event that licensees are found in violation of their approved cyber security plans. The NRC-approved cyber security plans, which are implemented through the licensee's cyber security programs, significantly reduce the possibility that a PLC installed at a nuclear power plant would be vulnerable to a malware attack that would negatively impact or challenge the plant's safety and control systems. The NRC inspects the implementation of the licensee's cyber security programs, at specified intervals, to confirm that they are being implemented in accordance with the NRC-approved cyber security plans.

To properly understand the petitioner's concerns, the NRC staff asked the petitioner to indicate the inadequacies he had identified in the NRC's current regulatory approach and

framework that would be remedied by the NRC's undertaking of his proposed action. The NRC staff asked, specifically, "What cyber threat or vulnerability is not addressed by the current NRC regulations and guidance?" The petitioner stated "the inadequacies in the NRC's current regulatory approach are that the regulations do not address correction for the vulnerability to corruption of the rewriteable PLC memories." The NRC staff disagrees with the petitioner's assertion because the cyber security rule does, in fact, require licensees to have the capability to detect, prevent, respond to, mitigate, and recover from cyber attacks under §73.54(c)(2). To comply with this requirement, nuclear power plant licensees must implement an overall site defensive strategy to protect critical digital assets (CDAs) from cyber attacks, as well as implementing operational and management security controls.

Issue 2: By using the petitioner's patented PLC design, nuclear power plant safety and control systems would be safe from malware attacks.

NRC Response:

The NRC staff disagrees with Issue 2 because the proposed vulnerability to malware attacks described in the petition is already addressed in the current NRC regulations. In addition, the "new-design" PLCs recommended in the petition have not been proven to offer protection from cyber attacks.

The approach recommended in the petition presumes that a "one size fits all" solution would be adequate for the wide variety of industrial control systems and safety systems used in nuclear power plants. However, ~~It~~ it does not take into account other attacks that could be made (e.g., man-in-the-middle attacks where an attacker inserts malicious commands between the PLC and the controlled devices). The objective of the petitioner's PLC design, which was to correct a proposed vulnerability (i.e., to "block malware attacks on the industrial control systems

Commented [LR1]: delete extra spaces on indent.

of those facilities"), is already accomplished by the defense-in-depth strategy in the current regulatory framework. As required by § 73.54(c)(2), nuclear power plant licensees must design their cyber security programs to apply and maintain an integrated defense-in-depth protective strategy to ensure that licensees have the capability to detect, prevent, respond to, mitigate, and recover from cyber attacks. The approach used by nuclear power plant licensees may vary in that NRC regulations are generally not prescriptive, and allow licensees and applicants to propose different methods for meeting the requirements. To comply with the requirements in § 73.54(c)(2), licensees must implement an overall site defensive strategy to protect CDAs from cyber attacks as well as implementing operational and management security controls.

Defense-in-depth strategies are a documented collection of complementary and redundant security controls that establish multiple layers of protection to safeguard CDAs. Under a defense-in-depth strategy, the failure of a single protective strategy would not result in the compromise of an SSEP function. One example of a defense-in-depth strategy involves setting up multiple security boundaries to protect CDAs and networks from cyber attack. In this way, multiple protection levels must fail for a cyber attack to progress and impact a critical system or network. Even if a failure occurred (e.g., such as through a violation of policy), or if a protection mechanism was bypassed (e.g., by a new virus that is not yet identified as a cyber attack), other mechanisms would still be in place to detect and respond to a cyber attack on a CDA, to mitigate the impacts of the cyber attack, and to recover normal operations of the CDA and its system before an adverse impact could happen.

In addition to the fact that a need has not been justified for use of the petitioner's new-design PLCs, the approach recommended in the petition has not been proven by the petitioner to be effective in preventing cyber attacks. Based on email correspondence, the petitioner states that the proposed "new-design programmable logic computers" currently are not used in any facility (nuclear or otherwise). As such, the petitioner was unable to present any evidence

that his PLCs would be effective in preventing cyber attacks. Furthermore, no information was provided by the petitioner as to how the "new-design programmable logic computers" would comply with the requirements in § 73.54 for use in the safety systems and control systems of a nuclear power plant.

Issue 3: Nuclear power plant licensee staff should be trained to maintain and secure records of all memory programming, and recommends maintenance in secure storage of programmed memories that may be again employed, as "the control systems of critical facilities are essentially steady-state."

NRC Response:

The NRC staff disagrees with Issue 3 because the petition does not take into account the awareness and training requirements each nuclear power plant licensee must perform as part of their comprehensive cyber security program as required in § 73.54.

Under § 73.54(d)(1), each licensee is required to ensure, as part of its cyber security program, that appropriate facility personnel, including contractors, are aware of the cyber security requirements and receive the necessary training to perform their assigned duties and responsibilities. As an example, licensees may comply with the awareness and training requirements by performing the following actions:

- Develop, disseminate, and periodically review and update the site cyber security training and awareness plan. This plan defines the purpose, scope, roles, responsibilities, and management commitment to provide high assurance that individuals have received training to properly perform their job functions;
- Perform gap analyses in areas where additional training is needed in cyber security;

- Establish measures to determine whether cyber security policies and procedures are being followed, and if not, determine whether a training or awareness issue is the cause and develop measures to be taken to correct the deficiency;
- Develop, disseminate, and periodically review and update procedures that are used to facilitate and maintain the cyber security training and awareness program; and
- Implement training and awareness security controls.

In addition, § 73.54(d)(3) requires each nuclear power plant licensee, as part of its cyber security program, to evaluate all modifications to assets identified in § 73.54(a)(1) (i.e. systems with SSEP functions) before their implementation. This ensures that the cyber security performance objectives are maintained. As stated above, the NRC inspects ~~the~~ licensee~~'s~~ cyber security programs, at specified intervals, to confirm that ~~they~~ the programs are being implemented in accordance with the NRC-approved cyber security plans.

III. Conclusion.

The NRC has reviewed the petition and appreciates the concerns raised by the petitioner. For the reasons described in Section II, "Reasons for Denial," of this document, the NRC is denying the petition under § 2.802. The petitioner ~~failed to~~ did not present any significant new information or arguments, as part of this petition, that would support the requested changes, nor has the petitioner demonstrated that a need exists for a new provision requiring use of the petitioner's new-design PLCs.

IV. Availability of Documents.

The documents identified in the following table are available to interested persons as indicated. For more information on accessing ADAMS, see the ADDRESSES section of this document.

Date	Document	ADAMS Accession Number/*Federal Register* Citation
January 2010	Regulatory Guide 5.71; "Cyber Security Programs for Nuclear Facilities"	ML090340159
March 14, 2013, as supplemented through December 19, 2013	Petition for Rulemaking from Mr. Alan Morris Regarding Programmable Logic Computers in Nuclear Power Plant Control Systems	ML14016A458
January 27, 2014	Letter to Petitioner Enclosing Federal Register Notice – Receipt of Petition for Rulemaking	ML13308A385
February 7, 2014	Federal Register Notice – Receipt of Petition for Rulemaking	79 FR 7406
June 12, 2014	Letter to Petitioner; "PRM-73-17 Cyber Malware Attacks on Programmable Logic Computers"	ML14120A006
June 18, 2014	E-mail from Petitioner; "PRM-73-17"	ML14181B296
June 18, 2014	E-mail from Petitioner; "RE: PRM-73-17"	ML14181B276

June 18, 2014	E-mail from Petitioner; “RE: PRM-73-17”	ML14181B286
June 19, 2014	E-mail from Petitioner; “RE: PRM-73-17”	ML14181B270

Dated at Rockville, Maryland, this day of , 2016.

For the Nuclear Regulatory Commission.

Annette L. Vietti-Cook,
Secretary of the Commission.