UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

March 31, 2021

The Honorable Christopher T. Hanson
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: UNI-DIRECTIONAL COMMUNICATIONS (NOT IMPLEMENTED IN SOFTWARE) FROM HIGH SAFETY TO LOWER SAFETY SYSTEMS AND INTERNAL PLANT TO EXTERNAL SYSTEMS CONNECTED TO THE INTERNET

Dear Chairman Hanson:

The staff responded to our letter of November 23, 2020, on defense-in-depth of digital safety systems. They disagree with our final recommendation that interconnections between High Safety-Significance systems and those of Lower Safety-Significance be one-way, uni-directional hardware-based devices. They claim that Branch Technical Positions (BTPs) cannot prescribe or impose specific design requirements such as we recommended. We disagree that our recommendation unnecessarily prescribes design requirements. As we reiterate in this letter, the way to safeguard digital instrumentation and control (DI&C) systems from compromising intrusion is as we suggest. Applicants would be free to design or specify the actual hardware devices that provide this needed assurance.

RECOMMENDATION

Commission direction is needed for the staff to assure, during design reviews, that only uni-directional hardware-based data communications mechanisms (not implemented in software) are used when there are communications between High Safety-Significance systems and those of Lower Safety-Significance. Consistent with the Be riskSMART initiative, guidance to the staff in this area would help the staff avoid a case where regulations provide flexibility, but overly rigid interpretation can be detrimental. In other words, this would ensure, at the design review stage, there is not a backdoor or software deficiencies within in-plant networks and systems that can be exploited by internet connected sources resulting in access to in-plant systems and networks. This ensures that independence, redundancy, and defense-in-depth are not compromised.

BACKGROUND

The introduction of computer-based digital instrumentation for reactor protection systems (RPS), engineered safeguards features actuation systems, and other reactor plant and steam plant control and monitoring systems results in significant improvements in overall plant performance.

However, computer-based digital instrumentation drastically increases the vulnerability for control of access to critical RPS, safeguards actuation systems, and in-plant networks through the methods used for communication of digital data and control signals both from safety to non-safety systems and vice versa, to internal plant networks and safety systems, and from these systems and in-plant networks to external plant sources that connect to the internet.

With computer-based DI&C architectures and networks configured for bi-directional data communication using software, control of access is threatened. In-plant systems and networks that control all plant operations are now susceptible to attacks from external plant sources that connect to the internet, resulting in compromise of independence, defense-in-depth, and control of access. These are three of the fundamental DI&C design principles.

The vulnerability of bi-directional software-configured data transmission devices to out-of-plant systems with internet access is not an abstract consideration as evidenced by a few recent events:

1. In early February 2021, a cyber attacker gained access to a Florida city's water system and, once inside the system, adjusted the level of sodium hydroxide (lye) to more than 100 times its normal levels which would have poisoned the city water supply. The system's operator noticed the intrusion and immediately restored the level to normal.

2. In December 2020, the Department of Energy's semi-autonomous National Nuclear Security Administration, which maintains the U.S. nuclear weapons stockpile, discovered that hackers accessed their networks as part of an extensive espionage operation. This also has affected at least half a dozen federal agencies and hundreds of companies.

3. A widely used software-based firewall and VPN system was found to contain a backdoor that compromised its encryption and allowed access to supposedly secret communications.

These cases exemplify the vulnerability of software-based security devices.

DISCUSSION

In our recent letter report of November 23, 2020, describing our review of BTP 7-19, Revision 8, "Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common Cause Failure Due to Latent Defects in Digital Safety Systems," we noted that the earlier November 2019 version of the draft BTP, Section B.2.2, emphasized that interconnections between High Safety-Significance systems and those of Lower Safety-Significance should be accomplished through the use of one-way digital communication devices rather than bi-directional communication devices that reduce independence and defense-in-depth. This requirement would have ensured that external plant access and compromised software in Lower Safety-Significance systems and in-plant networks do not compromise High Safety-Significance systems. This language was deleted in all later versions of the draft BTP.

As a result, we recommended that Section B.2.1 be revised to ensure that interconnections between High Safety-Significance systems and those of Lower Safety-Significance are one-way, uni-directional (not implemented in software) digital communication devices. Based on our recent reviews of NuScale and APR-1400, both applicants adopted this approach in the design of their DI&C systems.

The staff response disagreed stating that BTP 7-19, Revision 8, is guidance for staff reviewers and cannot prescribe or impose specific design requirements such as those described in our recommendation. We strongly disagree that our recommendation imposes a specific component design.

In previous discussions, the staff has stated that they cannot review electronic control of access and uni-directional (not implemented in software) hardware-based digital data communication for internal DI&C systems or communication from in-plant to external systems, during the design review phase of the Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50 or 10 CFR Part 52 licensing process, as part of a defense-in-depth review per BTP 7-19. Instead, it is viewed as an operational issue and covered as a cyber security concern during licensee programmatic review under 10 CFR 73.54, where guidance is provided by Regulatory Guide (RG) 5.71 "Cyber Security Programs for Nuclear Facilities."

The problem is that cyber-security and other security controls are not addressed and applied until the latter phases of the lifecycle that occur at a licensee's site (i.e., site installation, operation, maintenance, and retirement) since they are not part of the 10 CFR Part 50 and 10 CFR Part 52 design review. By then, the DI&C digital data communications architecture is potentially already designed and ready for manufacture or in the installation phase. Incorporation of uni-directional (not implemented in software) hardware-based data communication devices into the architecture at this late juncture in the process would possibly require a license amendment request (since it would be a licensing basis change) to be processed with its inherent delay and cost implications.

We recommend that RG 5.71 be used during the design certification phase of an application instead of during the cyber security review when it is too late. The architecture described in RG 5.71 is strong and to the point. Its guidance would have licensees place all digital safety systems in the highest level of their defensive architecture and only permit one-way communication (if any communication is desired) from the digital safety system to other systems in lower levels of the defensive architecture. Only one-way data flow is allowed from the RG 5.71 defined Level 4 to Level 3 and from Level 3 to Level 2, and initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited. In addition, Section B.1.4 of Appendix B to RG 5.71 notes that one-way communications should be enforced using hardware mechanisms.

It is sometimes suggested that the problem can be solved through the employment of cyber security software. This is problematic on two counts. First, this software is reactive; it only protects against attacks that have already been observed. Second, in-plant systems and networks involved in protection, control and monitoring are not amenable to the incorporation of cyber security software into their operating system software. It would disrupt all critical functions and would require constant software upgrades to maintain currency thus further imperiling its timely operation and increasing the possibility of introducing malware during the upgrades that allows cyber compromise.

SUMMARY

Allowing the use of computer-based DI&C architectures and networks configured for bi-directional data communication using software, threatens control of access and compromises independence and defense-in-depth. It compromises plant safety by leaving High Safety-Significance systems open to the kinds of attacks that have seriously impacted other industries and government agencies.

Commission direction is needed for the staff to assure, during design reviews, that only uni-directional hardware-based data communications mechanisms (not implemented in software) are used when there are communications between High Safety-Significance systems and those of Lower Safety-Significance. Consistent with the Be riskSMART initiative, guidance to the staff in this area would help the staff avoid a case where regulations provide flexibility, but overly rigid interpretation can be detrimental.

Sincerely,

Matthew W. Sunseri

Digitally signed by Matthew W. Sunseri
Date: 2021.03.31 13:01:52 -04'00'

Matthew W. Sunseri
Chairman

REFERENCES

1. Advisory Committee on Reactor Safeguards, “Final Draft Standard Review Plan Branch Technical Position 7-19, ‘Guidance for Evaluation of Defense-in Depth and Diversity to Address Common Cause Failure Due to Latent Defects in Digital Safety Systems,’ Revision 8,” November 23, 2020 (ML20328A157)

2. U.S. Nuclear Regulatory Commission, “Review of NUREG-0800, Branch Technical Position 7-19, ‘Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common Cause Failure due to Latent Design Defects in Digital Safety Systems,’ Revision 8,” December 18, 2020 (ML20345A338)

3. Regulatory Guide (RG) 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Revision 3, July 3, 2011 (ML102870022)

4. Regulatory Guide (RG) 5.71, “Cyber Security Programs for Nuclear Facilities,” Revision 1, January 31, 2010 (ML090340159)

5. Bing, Reuters, “Hackers try to contaminate Florida town's water supply through computer breach,” February 8, 2021, Link or Campo-Flores, The Wall Street Journal, “Hacker Changed Chemical Level in Florida City,” February 8, 2021 Link

6. Collier and Strickler, NBC News “Energy Department says it was hacked in suspected Russian campaign,” December 17, 2020 Link

7. Zetter, Wired, “Researchers solve Juniper Backdoor Mystery; Signs point to NSA,” December 22, 2015 Link

8. Advisory Committee on Reactor Safeguards, “Interim Letter: Chapters 7 and 8 of the NRC Staff’s Safety Evaluation Report with Open Items Related to the Certification of the NuScale Small Modular Reactor,” September 26, 2018 (ML18270A374)

9. U.S. Nuclear Regulatory Commission, “Chapters 7, ‘Instrumentation and Controls,’ and Chapter 8, ‘Electric Power,’ of the U.S. Nuclear Regulatory Commission Staff’s Safety Evaluation Report with Open Items Related to the Certification of the Nuscale Power, LLC Small Modular Reactor,” October 30, 2018 (ML18284A071)

10. Advisory Committee on Reactor Safeguards, “EDO Response to ACRS Letter of September 26, 2018 on Chapters 7 And 8 of the NRC Staff’s Safety Evaluation Report with Open Items Related to the Certification of the Nuscale Small Modular Reactor,” March 7, 2019 (ML19066A163)

11. U.S. Nuclear Regulatory Commission, “Response to ACRS Letter of September 26, 2018, on Chapters 7 and 8 of the U.S. Nuclear Regulatory Commission Staff's Safety Evaluation Report with Open Items Related to the Certification to the NuScale Small Modular Reactor,” April 10, 2019 (ML19100A008)

12. Advisory Committee on Reactor Safeguards, “Interim Letter: Chapters 7 and 18 of the NRC Staff’s Safety Evaluation Report with Open Items Related to the Certification of the APR 1400 Design,” September 25, 2017 (ML17265A792)

13. U.S. Nuclear Regulatory Commission, “Interim Letter: Chapters 7 and 18 of the U.S. Nuclear Regulatory Commission Staff’s Safety Evaluation Report with Open Items Related to the Certification of the Advanced Power Reactor 1400 Design,” November 2, 2017 (ML17291A904)

March 31, 2021

SUBJECT: UNI-DIRECTIONAL COMMUNICATIONS (NOT IMPLEMENTED IN SOFTWARE) FROM HIGH SAFETY TO LOWER SAFETY SYSTEMS AND INTERNAL PLANT TO EXTERNAL SYSTEMS CONNECTED TO THE INTERNET

Accession No: ML21085A014 **Publicly Available (Y/N):** _Y___ **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	LBurkhart	SMoore (SWM)	MSunseri
DATE	3/26/21	3/26/21	3/26/21	3/29/21	3/30/21

OFFICIAL RECORD COPY