PRM-73-18
79FR56525

PUBLIC SUBMISSION

As of: December 09, 2014
Received: December 07, 2014
Status: Pending_Post
Tracking No. 1jy-8fxb-va2m
Comments Due: December 08, 2014
Submission Type: Web

Docket: NRC-2014-0165
Protection of Digital Computer and Communication Systems and Networks

Comment On: NRC-2014-0165-0002
Protection of Digital Computer and Communication Systems and Networks

Document: NRC-2014-0165-DRAFT-0003
Comment on FR Doc # 2014-22523

Submitter Information

Name: Anonymous Anonymous

General Comment

See attached file(s)

Attachments

Petition Comment NRC-2014-0165

Date: 6 December 2014

Reference: docket no. PRM-73-18; NRC-2014-0165

Subject: Public comment on NEI petition discussing 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks

As a process computer system engineer who has been working on nuclear cyber-security since 2007, I concur with the position that significant and widespread technical issues associated with interpretation of 10 CFR 73.54 regulation exist. These issues exist both within the industry and NRC inspection staff. ***The NEI petition does make some points that I agree with, but if implemented as requested will not produce the desired effect, and also does not address many other important technical issues facing those attempting to interpret and implement cyber-security regulation and associated guidance documents.*** This conclusion is based on knowledge gained from being an Electrical Engineer with Information Technology experience turned nuclear System Engineer, being a 10 CFR 73.54 Cyber Security Assessment Team (CSAT) member, and supporting an NRC milestone 1 through 7 cyber security inspection.

Speaking directly to the "as-written" petition, in my experience when consideration is given to broader license context, traditional NRC regulatory purview, and 10 CFR 73.1 / RG 5.69 Design Basis Threat (DBT) content, the industry as a whole is misinterpreting 10 CFR 73.54 regulation. ***The current list of Critical Digital Assets typically scoped into the 10 CFR 73.54 program have very little to do with the NRC's traditional scope and purpose of preventing a radiological release or keeping the public aware of a developing emergency.***

As somewhat discussed in the petition, Target Set and core Security System assets are the only equipment directly responsible for preventing the goals of the 10 CFR 73.1 Design Basis Threat (DBT) (further elaborated in RG 5.69.) Yet mostly because of a concern for plant trips and transients, thousands of other components have been scoped into licensees' 10 CFR 73.54 programs. To me this result is mostly driven by guidance material content (NEI 08-09 and RG 5.71) and industry meeting discussion; and less the result of actual 10 CFR 73.54 regulatory language. The regulatory language says virtually nothing about trip and transient considerations, and the cited DBT only lists Radiological Sabotage concerns.

If the petition intent is to emphasize and more clearly refocus licensees on categorizing devices as Critical Digital Assets (CDAs) only when Radiological Sabotage is a concern, I would suggest modifying the following two language suggestions contained in the NEI document (reference Docket ID NRC-2014-0165):

1. Section 73.54(a)(1)(i) - Rather than propose replacing "Safety-related and important-to-safety functions" with "That are necessary to prevent significant core damage and spent fuel sabotage," directly state that only Target Set and credited Security System equipment need special consideration for preventing the previously established 10 CFR 73.1 DBT intent of Radiological Sabotage.

2. Section 73.54(a)(1)(ii) - Rather than propose replacing "Security functions" with "Whose failure would cause a reactor SCRAM," require a simple concern for trips and transients created by cyber-attacks initiated by outsiders external to the Protected Area (PA.) ***Because most process system components on current CDA lists can directly or indirectly cause trips and transients, the offered NEI petition verbiage (if implemented) will essentially result in the same large list of CDAs previously generated that cannot cause Radiological Sabotage (the main reason for the petition.)*** In my experience most items on current CDA lists are put there out of a reactivity concern (trip or transient by an insider threat.) Cyber security controls cannot prevent, or even make it more difficult, for an insider to cause trips and transients. Within the Protected Area, devices that can produce these results are openly labelled to draw attention and help prevent SCRAMs accidentally initiated by established high assurance trusted and reliable insider resources.

More broadly speaking:

In order to eliminate widespread regulatory interpretation issues and improve inspection consistency, the rule and its associated regulatory guidance material both need simplification (emphasis on regulatory guidance materials.) The rule purpose should be clearly focused on two separate concerns:

1. High assurance protection for preventing radiological sabotage.
2. Preventing plant trips and transients caused by cyber-attacks initiated from outside the Protected Area. A concern for accidental initiation of a cyber-attack by insider action should also be included.

In my professional opinion, ***as currently interpreted by the industry, the rule is actually creating increased plant risk, significant unwarranted expense, and (for both the licensee and NRC) unavoidable regulatory inspection issues.*** Most importantly, operational risk is threatened by those program prescribed actions requiring regular equipment configuration changes. Many of these actions require indirect interconnections between otherwise deterministically isolated equipment and uncontrolled outside environments. The trusted and previously validated configurations of digital devices are also challenged by these and other suggested Information Technology practices.

These activities are required to support a recurring and endless set of configuration changes prescribed by NEI 08-09 and RG 5.71 (i.e. shuttling software patches and virus signature data between isolated devices using portable media.) Literally millions of dollars are being spent trying to reduce risk, while ironically risks are actually increased by this interpretation of legislation.

Even when this is pointed out by technically conscience resources, there is overwhelming pressure to conform and move ahead without regard to technical merit, protective effectiveness, concern for equipment reliability, and risk. This industry and NRC lead “group-think” approach is very frustrating for many now working in this unique industry. **If these practices are actually required, they can only be potentially applied to a very small percentage of devices currently categorized as CDAs (<5%), yet**

internal licensee processes and industry guidance materials often lead one to believe these actions are required and applied to almost all CDAs. A lack of prescriptive control guidance for typical industrial process type devices (Dixson indicators, Moore controllers, valve positioners, temperature transmitters, PLCs both QA and non-QA, chart recorders, etc.) is a significant and unnecessary challenge for the industry.

Existing 10 CFR 73.54 regulatory guidance materials are far too Information Technology (IT) centric and ignore the merits of current protective approaches that are based on traditional Instrumentation and Control Engineering and other license requirement. This IT emphasis also ignores that most digital process system components (>95%) are not of a technical form that is compatible with these concepts, and the other <5% are typically obsolete and functionally-stable Information Technology forms of equipment that cannot be used to cause Radiological Sabotage.

The regulatory guidance materials need modification to recognize that:

1. Most equipment in a nuclear process environment are not typical Information Technology-type devices and therefore are summarily incompatible with the litany of currently prescribed controls. ***Also, when these type of controls are compatible with process equipment, they are less effective than current instrumentation and control security approaches.***
2. The regulatory issue and intent should not emphasize information protection, it should emphasize industrial energy protection. Insider threats have unfettered access to the vessels and systems containing the energy requiring protection. The rule should not be crafted for information protection, it should emphasize industrial energy management – there is a significant difference. Insiders are vetted and monitored by the license required Insider Mitigation Program.
3. Most of the prescribed controls require frequent equipment configuration changes. The more critical a device is, more is at risk when changing its configuration. Rather than prescribe IT-type information protections based on non-deterministic network border fortification and layer-defense technique, the guidance materials should require and emphasize the importance and effectiveness of physical protections provided by the Protected Area, deterministic data communication isolation by air-gap/data-diode, and equipment lifecycle management by traditional configuration management practice. Configuration management practices must be required to procedurally consider Portable Media and Mobile Device handling and usage (prevent accidental Cyber Attack initiated by an unknowing insider), and trusted-configuration validation of new devices (new design and maintenance activities) prior to installation and in-service status.
4. ***For systems and components involved in industrial energy management, actual energy behavior serves a central role in being able to detect anomalous operation and initiating mitigation by deep and diverse equipment designs. This should be a codified and credited form of alternate protection that does not submit plant equipment to unnecessary configuration changes. Billions of dollars have been spent deliberately creating these equipment designs, processes, practices, and defenses. These defenses are effective for protecting the public's health and safety concern – even from a cyber-attack. The controls prescribed by guidance material threaten this previous protective accomplishment, and give no clear credit for this past investment.***
5. Only Target Set and license-credited Security devices should be within the Radiological Sabotage scope of concern. ***However, all digital devices used to support industrial energy management***

should require protection by the Protected Area (PA), deterministic data communication isolation, and Controlled Plant Equipment lifecycle management practice. When the PA cannot be leveraged, continuous monitoring and alarm notification must be in place.

6. The regulatory guidance materials should place <u>less</u> emphasis on prescribing <u>unanalyzed solutions</u> (controls), and elaborate on rule intent and how to determine scope/applicability and establish compliant security assessments.

In summary, as a past IT specialist turned nuclear process engineer, I believe the industry's 10 CFR 73.54 regulatory interpretation is challenging the existing and effective public safety protections implemented by previously established regulation. Unlike many other industries, we would never allow a nuclear power plant to be operated remotely, our plants are manned 24 hours a day by highly trained and trusted staff, and are physically secured by a formidable security force and system. All of our important systems are deliberately designed, operated, and maintained with a technical basis. These basis require deep and diverse equipment designs for protecting the public's health and safety interest. Many of these Safety Related systems are analog, and all are diverse in design. These unique industry characteristics should be recognized by cyber regulation. The potential negative impact and lack of practical effectiveness of IT security practices should be considered before being adopted.

Because digital technology can introduce different ways of initiating plant events, special regulatory concepts are needed. The cyber regulations should be careful not to threaten previous protective accomplishment by requiring the use of unanalyzed "solutions" that can lead to reduced operational stability. The rules and associated guidance materials should consider risk. A basic regulatory framework focused on public safety should emphasize analysis of digital Target Set and credited Security System components. However all digital assets involved in the management of power-block industrial energy should be required to have:

1. Physical protection of the license required Protected Area, or when installed outside of the PA be contained in a locked and alarmed enclosure.
2. Deterministic data communication isolation from all non-industrial process environments.
3. Life-cycle management controls using traditional Controlled Plant Equipment configuration management practices. These practices must ensure the use and handling of Portable Media and Mobile Device are addressed within all procedures. Design details of both hardware and software elements must be included in Engineering records.

With this basic regulatory framework in place, license compliance and inspection efforts are more clearly established and enforceable. The emphasis on applying IT-best practices to the nuclear industrial process environment should be removed from guidance documents. In most cases these type controls cannot be technically applied, and should only be applied when an analysis demonstrates that risk margin would be improved. These items should be included in any 10 CFR 73.54 petition designed to improve regulatory intent, clarity, effectiveness, and enforceability.