

From: <Vicki_Hull@dom.com>
To: <NRCREP@nrc.gov>
Date: Fri, Feb 11, 2005 7:24 AM
Subject: Dominion comments on Draft Regulatory Guide DG-1130

RDB reviewed
2/11/05

(See attached file: GL04-038_LtrOnly.pdf)

12/16/04

69FR 75359
(6)

STSF Review Complete
Template = ADM-013

E-RFDS = ADM-03
Call = S. Aggarwal (SK9)
P. Torritty (AF1)

Mail Envelope Properties (420CA403.778 : 5 : 63352)

Subject: Dominion comments on Draft Regulatory Guide DG-1130
Creation Date: Fri, Feb 11, 2005 7:24 AM
From: <Vicki_Hull@dom.com>

Created By: Vicki_Hull@dom.com

Recipients

nrc.gov
twf2_po.TWFN_DO
NRCREP

Post Office
twf2_po.TWFN_DO

Route
nrc.gov

Files	Size	Date & Time
MESSAGE	42	Friday, February 11, 2005 7:24 AM
GL04-038_LtrOnly.pdf	242308	
Mime.822	333091	

Options

Expiration Date: None
Priority: Standard
Reply Requested: No
Return Notification: None

Concealed Subject: No
Security: Standard

February 10, 2005

Rules and Directives Branch
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

GL04-038

COMMENTS ON DRAFT REGULATORY GUIDE DG-1130
CRITERIA FOR USE OF COMPUTERS IN
SAFETY SYSTEMS OF NUCLEAR POWER PLANTS
(FEDERAL REGISTER, VOLUME 69, NUMBER 241, PAGE 75359,
DATED DECEMBER 16, 2004)

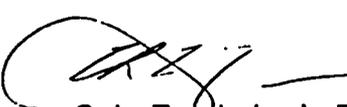
Virginia Electric and Power Company (Dominion) and Dominion Nuclear Connecticut, Inc. (DNC) appreciate the opportunity to provide comments on the Draft Regulatory Guide DG-1130, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," as requested in the above federal register.

Please find our comments attached for your review and consideration. If you would like further information, please contact:

Mr. Bob MacMeccan Bob_MacMeccan@dom.com, or (804) 273-2121 or

Mr. Don Olson Don_Olson@dom.com, or (804) 273-2830

Respectfully,



C. L. Funderburk, Director
Nuclear Licensing and Operations Support

Attachment

Comments on DG-1130
Criteria for Use of Computers in
Safety Systems of Nuclear Power Plants

1. **General Comment** - The format of the Draft Regulatory Guide should be changed to make the regulatory positions easier to understand and implement in a cost-effective manner. The format of the underlying industry standard, IEEE Std 7-4.3.2-2003, utilizes IEEE-Std-603 as a basis for both format and requirements. Since IEEE-603 is directly incorporated in regulations in 10CFR50.55 a (h), using the format of that standard with the level of detail consistent with that standard, would significantly improve the effectiveness of the Draft Regulatory Guide.

The format and level of detail in DG-1130 are consistent with the detailed guidance provided for digital systems in the Standard Review Plan, NUREG 0800, and the current detailed content of Draft Regulatory Guide would be more appropriate in this regulatory context.

2. **Section 2.0** - The waterfall method should not be used to frame the regulatory position. The high level guidance of the regulatory position should be provided in a format consistent with the format, content, and level of detail of the underlying industry standards. Restating the guidance and examples at each life-cycle phase results in guidance that is too detailed and may not be either appropriate or prudent for a specific application. As is stated in the general comment above, including the detail in NUREG 0800 will ensure that the appropriate detailed, application-specific requirements, developed from the high level design requirements, are considered for each life-cycle phase.
3. **Section 2.0** - It is recommended that the general quality assurance requirements and configuration management requirements not be linked to the users security program. Typically a user's security program restricts the access of the user's staff to security information on a "need to know" basis. The linkage to the existing QA and configuration management process is appropriate. It may be appropriate to link elements of the "physical security" aspects of the equipment to a user's security program. This is a consideration for all safety system designs, not just digital. Regulatory concerns dealing with security should be dealt with in the context of IEEE-Std-603.
4. **Section 2.1** - Remote access to safety system data from outside the physical plant is not necessarily a potential vulnerability. Access to data through one-way or fixed function gateways should be allowed, assuming proper verification of the integrity of the gateway is verified.

5. **Section 2.2.1** - The last paragraph in this section is worded in a manner that is confusing and difficult to follow. It would be more appropriate to word this more like: "The vulnerability of the safety system should be limited by minimizing the use of pre-developed software."
6. **Section 2.3.1** - The discussion of complex access control should include "such as a combination of knowledge (e.g., password), property (e.g., key, smart-card) OR personal features (e.g., fingerprints)" instead of "such as a combination of knowledge (e.g., password), property (e.g., key, smart-card) and personal features (e.g., fingerprints)". Inclusion of a requirement for use of biometric type access controls will only serve to encourage the use of pre-developed software and even software platforms (e.g., Windows operating systems) that are more vulnerable to attacks than the safety systems they would be safeguarding.
7. **Section 2.3.1** - The first paragraph in this section describes four numbered items for addressing requirements for user control of implemented features and functions. The first three items are required for general design requirements, not just security, to assure deterministic performance. The fourth requirement should not request a "list of personnel who may access and use the system" because this list will not be known at the time the software requirements are written. A higher level requirement is more appropriate than this detailed delineation. The higher level requirement deals with restricting a user's access. Typically, the high level requirements deal with restricting a user's access to functions and data that are appropriate to the user function, such as maintenance. Typically, access to the majority of system function, services, and communications will not be permitted in an "on-line" environment but only in an off-line, development / maintenance environment. For the fourth numbered item, the reference to the risk analysis is appropriate, but the detail in the examples may not be. The concern with the examples is that the focus of the examples is on using technology implemented into the equipment to provide security. However, the risk analysis may utilize existing plant security measures, such as physical security and employment of trustworthy people who have background checks and continuous behavior observation programs. Additionally, access to the network should be considered. Credit should be given for systems that have local networks isolated from the outside.
8. **Section 2.4.2** - There is a repeated use of the term "scanning" that seems to refer to an automated process of virus or spyware scanning tools. The reality is that these problems only exist in the desktop operating system environments and no safety system could receive NRC approval that relied on these platforms for any substantial functionality. Inclusion of this requirement also encourages the use of pre-developed software to perform a necessary function. Few, if any utilities or nuclear vendors have the knowledge or skill sets to develop these types of tools and keep them current.

This section of the Regulatory Position is creating a problem where one is not likely to exist otherwise.

9. **Section 2.4.2** - The implementation of security measures during development would not be practical to implement. Access of the programmer to the software is a matter of trust. This would better be handled as a configuration control matter where the software is automatically scanned before it is returned to the production computer system from the development system.
10. **Section 2.5** - There is discussion of various types of testing (e.g., software testing, software integration testing, software qualification testing, etc.) There are no supplied definitions of what the differences are between the types of testing being listed. The first item listed (software testing) would seem to be the overall scope, but is listed as if it were a peer to the other types of tests listed. It is therefore unclear what the staff would expect from the utility here.
11. **Section 2.5** - Some means of taking credit for security testing done by a software vendor should be allowed. This assumes the vendor has an approved software quality control program.
12. **Section 2.5.2** - This section again lists the use of "scanning" tools. It would seem to be as important to require that the development and production environment testing include verifications that only the expected software processes are running and/or that all memory allocations were as expected by the software design.
13. **Section 2.5.2** - The testing and scanning described here is best done as part of a configuration management program. The software can be scanned when it is checked out and back in from a controlled software library as part of the development process.
14. **Section 2.6** - The requirement for security testing implies there are standards for this kind of testing. They should be included as part of this document.
15. **Section 2.7** - The Draft Regulatory Guide contains guidance to "monitor and record access and use of the system" including "real-time" monitoring for security purposes. Guidance to "add" security-monitoring functions to an on-line safety system rather than to restrict the users access to critical functions may not be the best way to insure overall plant safety. Additional functions in a safety system have the possibility of being fault vulnerabilities and security vulnerabilities and should not be added unless there is an increase in safety that cannot be achieved another way. A high level requirement with the focus on operational monitoring of the physical security and access restrictions is probably more effective in attaining the regulatory goal. This section should include a discussion of the use of real-time access logging and ensuring that the use of the tool does not in fact reduce system reliability through excessive

use of disk or memory resources over long term usage. Industry experience has shown this to be a problem in non-safety nuclear plant computer systems.

16. **Section 2.8.3** - This section implies that a separate security incident response plan be designed, tested and implemented. Instead this section should refer to the appropriate section of the IEEE standard and reinforce that consideration for security threats be included in the already required contingency recovery program.