ROB received 3/14/05

IEEE POWER ENGINEERING SOCIETY
NUCLEAR POWER ENGINEERING COMMITTEE

CHAIR
John J. Disosway
Dominion
North Anna Power Station
P.O. Box 402
Mineral, VA 23117-USA
VOX: 540 894-2589/FAX: 540 894-2178
John_Disosway@dom.com

VICE CHAIR
J.S. Malcolm
AECL
2251 Speakman Drive
Mississauga, Ontario
LSK1B2 Canada
VOX: 905 823-9040/FAX: 905 403-7391
MalcolmS@AECL.CA

SECRETARY
J.D. MacDonald
IST-Conax Nuclear, Inc.
402 Sorwil Drive
Buffalo, NY 14225 USA
VOX: 716 681-1973/FAX: 716 681-1139
J.D. MacDonald@IEEE.org

PAST CHAIR
John P. Carter
Shaw Group / Stone and Webster, Inc.
100 Technology Center Drive
Stoughton, MA 02702-4705 USA
VOX: 617 589-1518 / FAX: 617 589-2969
Jack.Carter@Shawgrp.com

Sub-Committee Chairs
SC-2 Qualification
S. Aggarwal
U.S. Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD 20852 USA
VOX: 301 415-6005 / FAX: 301 415-5074
SKA@NRC.gov

SC-3 Operations, Surveillance and Testing
S. K. Dureja
Calvert Cliffs Nuclear Power Plant
1650 Calvert Cliffs Parkway
Lusby, MD 20657 USA
VOX: 410 495-4006 / FAX: 410 495-3614
surin.k.dureja@constellation.com

SC-4 Auxiliary Power
G.L. (Jerry) Nicely
Tennessee Valley Authority
1101 Market Street, LP 4H-C
Chattanoga, Tn 37402-2801 USA
VOX: 423 751-8236 / FAX: 423 751 8247
G.L.Nicely@IEEE.org

SC-5 Human Factors, Control Facilities and Reliability
S.A. Fleger
Science Application International Corp.
1710 SAIC Drive, M/S T-1-12-3
McClean, VA 20170 USA
VOX: 202 493-3378 / FAX 202 493-3390
flegers@SAIC.com

SC-6 Safety Related Systems
P.L. Yanosy, Sr.
Westinghouse Electric, Co.
1740 Golden Mile Highway
Monroeville, PA 15148-0598 USA
VOX: 724 733-6402
paul.l.yanosy@us.westinghouse.com

Standards Coordinator
J.E. Thomas
MPR Associates, Inc.
320 King Street
Alexandria, VA 23314-1320 USA
VOX;864 962-0128 / FAX 724 733-6168
jthomas@mpr.com

Awards Chair
D.F. Brosnan
PG&E Diablo Canyon PP
P.O. Box 56
Avila Beach, CA 93424 U/SA
VOX: 805 545-6646/
dfb4@pge.com

March 11, 2005

12/16/04

69FR75359

(13)

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

Subject: Comments on Draft Regulatory Guide DG-1130, (Proposed Revision 2 to Regulatory Guide 1.152), Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

Dear Sir or Madam:

The following comments on the draft regulatory guide DG-1130 are submitted by the IEEE Nuclear Power Engineering Committee (NPEC).

History and Background

Regulatory Guide 1.152 was previously issued by the NRC as an endorsement of IEEE Std. 7-4.3.2-1993. With the release of the updated IEEE Std. 7-4.3.2-2003, the NRC has issued DG-1130 to define the NRC endorsement of the updated standard. A large portion of DG-1130 is devoted to defining additional digital safety system security guidance.

The topic of safety system software security was recognized within the introduction of IEEE Std. 7-4.3.2-2003 as a needed addition. At that time it was intended that this topic would be addressed in a future revision of IEEE Std. 7-4.3.2. However, given the scope of this topic it may be more appropriate for a separate standard.

The overall scope of "system safety and security" encompasses more than digital safety systems. As more computer based control systems are implemented, the issue of system safety and security must address the non-safety computer systems in addition to the safety systems. For example, security vulnerabilities in computer based control systems could lead to initiating events that would challenge the safety systems. This content would be outside the scope of 7-4.3.2-2003 and should be addressed by another standard, which would then be endorsed by another Regulatory Guide.

General Security Related Comments Regarding Draft Reg. Guide DG-1130

The material as presented in DG-1130 is based solely upon a life-cycle approach which is overly restrictive. Other approaches, including risk-based, are available and should be permitted to address safety system security.

E-RIDS = ADM-03

SGP Review Complete.

Template = ADM-013

Add = S. Aggarwal (SKA)

The additional security requirements imposed by DG-1130 are very general and do not provide guidance appropriate for a standard. From the general context of these requirements, it is not clear what should be performed, at a minimum, to ensure security, or what types of threats/attacks require protection. For example, section 2.4.2 states "... There should be provisions against the incorporation of hidden functions in the application development software or the system software that could support potential unauthorized access."

While the topic of security applies to both hardware and software, the content of the draft guide focuses mainly on software. Security attributes for hardware need to be addressed as well as providing adequate consideration for Commercial Off The Self (COTS) based alternatives. The consideration of hardware aspects would include physical access control, modems, connectivity to external networks, data-links, open ports, etc.

Additionally, several sections of the DG refer to the use of testing for assurance that security requirements are met (see section 2.5.2 for example). In general, testing cannot be used to check for viruses, worms, Trojan horses, bomb codes, or back door codes. Scanning for known viruses and worms is possible, for a specific operating system environment. Reviews and design control/configuration management methods must be applied to prevent bomb codes and back door codes.

Recommended Wording Changes to DG-1130

Safety software security is currently addressed in BTP-14, the Standard Review Plan and IEEE Std. 1012-1998 as endorsed by Reg. Guide 1.168. Given the overall scope of the Information Security topic, it is recommended that Section C, paragraphs 2.1 through 2.9 be removed. The appropriate structure to address Information Security will be examined by NPEC as part of the scope of a new IEEE Project Authorization Request (PAR). Other industry guidance that will be considered as part of this effort will include ISO/IEC 17799.

Section 2 should be revised to eliminate specific references to the life-cycle model. Section 2 should only provide general reference to the need for safety system security, specifically related to the scope of 7-4.3.2, and list the types of items that need to be considered. The following is suggested wording:

> The development process for Digital safety system software should address potential security vulnerabilities. Topics that should be reviewed and addressed include:
>
> - unauthorized 3rd-party access
> - unauthorized configuration management library access
> - viruses
> - worms
> - Trojan horses
> - bomb codes
> - back door codes
>
> Existing QA practices should include appropriate reviews to determine the effectiveness of the digital safety system security program.

Specific Non-Security Related Comments Regarding Draft Reg. Guide DG-1130

The 5th paragraph in section B (page 3) states "... Annex C to this standard provides useful information on providing confidence that an existing commercial computer is of sufficiently high quality and reliability to be used in a safety system." On page 4 of section B, item (c) states "Annex C is not endorsed by the NRC because it provides inadequate guidance." These two statements seem to conflict with one another.

Addressing the Broader Topic of Information Security Management

The entire topic of digital safety system security should be addressed within the broader context of Information Security Management and not via an add-on to an existing Regulatory Guide. This subject is sufficiently important and complex to merit more considered guidance.

In the final analysis, effective Information Security Management should, at a minimum, address the following topics:

- Pre-Development; including concept and RFP
- Development Activities; including development model, e.g. Life-Cycle
- Post Development; Acceptance, QA, Operations
- Threat Assessments; unauthorized access, disclosure, destruction
- Security Policies
- Personnel Involvement; including developers, contractors, service providers, IT staff
- Incident Reporting
- Component Protection; software, hardware, COTS, operating environment
- Security Procedures; access control, contingency plans

It is anticipated that IEEE/NPEC, through the PAR process, will begin work to develop an overall structure to support a standard that addresses the above topics. During this process, further interactions with interested parties within the nuclear community will be conducted to collect and review material for future standards. The draft standard will be submitted for review and comment prior to release.

Very truly yours,

John J. Disosway
Chairman
Nuclear Power Engineering Committee

cc: J. S. Malcolm, NPEC Vice Chairman
J. D. MacDonald, NPEC Secretary
P. L. Yanosy, Subcommittee 6 Chairman
C. J. Roslund, Working Group 6.4 Chairman