

ROB received

1/11/05

cg

## Comments on Draft Regulatory Guide DG-1130

I am a control system engineer working on control system cyber security and am considered an industry expert. I also am knowledgeable about nuclear plant instrumentation and control systems having managed the EPRI Nuclear Plant Instrumentation and Diagnostics Program for almost 5 years. Based on my experience including conducting fossil plant, substation, and Control Center (SCADA) cyber security assessments and developing control system cyber security policies, I have the following comments on the draft Regulatory Guide:

12/16/04  
69FR75359

(1)

- The title of the Draft Regulatory Guide is Criteria for Use of Computers in Safety Systems of Nuclear Power Plants. This can leave readers to think it only applies to computers in safety systems. However, it also needs to apply to computers in non-safety systems that could impact safety systems or plant operation.
- The Regulatory Guide references IEEE Standard 7-4.3.2-2003 but the IEEE standard does not address cyber security.
- Section 2.1 specifies threats to safety systems. However, non-safety systems could impact safety systems and/or plant operation.
- Section 2.2.1 does not provide any security requirements or guidance for utilizing pre-developed software which are currently utilized in many nuclear plant applications.
- Section 2.2.2 does not provide security guidance or requirements on control system cyber security policies which are different than traditional IT security policies.
- Section 2 does not provide guidance or requirements on how to test the system security features.
- Section 2.7 does not address what to do if the system does not have the ability to monitor and record access use. Many control systems do not have this technology.
- There have been numerous cases of control system cyber security impacts including several in commercial nuclear plants. Many nuclear plants have connected their plant networks to corporate networks making them potentially vulnerable to cyber intrusions. Consequently, the Regulatory Analysis Conclusion that the Regulatory Guide is only optional and voluntary to implement this Regulatory Guide is not technically prudent.

Joe Weiss  
KEMA, Inc.  
(408) 253-7934

E-RIDS = ADM-03

Call = S. Aggarwal (SKA)

SISP Review Complete

Template = ADM-013