RDB received
2/28/05

Thursday, February 10, 2005

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research

12/16/05
69FR75359

Satish K. Aggarwal
(301) 415-6005

10

COMMENTS TO DRAFT REGULATORY GUIDE DG-1130

CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR PLANTS

The proposed new guide contains many new and indeed needed changes to the previous guide. As written it provides a new awareness of current issues regarding safety system computers.

I realize that this guide addresses computers used in safety systems but you have mentioned on page four (4) in the last half of the first paragraph controls on the physical and electronic access points to computer systems that provide operational information to operators.

This brings up the issue of interconnecting systems that are used to process information such as Supervisory Control And Data Acquisition Systems, or SCADA's. Since the majority of safety systems feed SCADA's where the data is processed prior to being displayed for operations personnel it seems that these systems need to be addressed as well. After all it would be just as easy to manipulate the data during calculations as before or after the calculation is completed. Since it is the information that is being presented to plant operation personnel that is important, at what point is data integrity no longer a concern? Your document makes it appear that after information leaves the safety system computer it is no longer important and needs no further controls. Even sections 2.6.2 Development Activities, 2.7 Operation Phase and 2.8 Maintenance phase, appear only to address the safety system computer and not the entire system.

Most of the computer systems containing safety system information are connected to the plant wide area networks which usually provide paths to the Internet. This could and does provide a path from the Internet to the safety systems, system controls and information displayed to operations personnel. Yet there is no proposal for ensuring a secure environment for the integrity of data and control functions of the computer system, outside of the safety system computer. If an introduction of a virus, worm or Trojan occurred, the parasite would be able to gain access to safety system information and system control software causing system problems and erroneous information displayed to operations personnel. It would appear that the only way to prevent this is with system isolation.

Before the advent of the computer displays in the control room and other areas the safety system computers were isolated and not connected to any other system. Now that is easy to connect to the safety system computer with outside interfaces the data provided by them can be made readily available to everyone. Though this may sound like a good idea it presents new vulnerabilities to the plant safety systems that has not existed in the past. This new area of vulnerabilities should be addressed in some manner to protect data integrity and availability.

Sincerely,

Joseph Land
JoeFLand@bellsouth.net

E-RIDS = ADM-03
Add = S. Aggarwal (SKA)

SISP Review Complete
Template = ADM-013