

RulemakingComments Resource

From: Joe Weiss <joeweiss16@yahoo.com>
Sent: Thursday, March 17, 2016 5:33 AM
To: RulemakingComments Resource
Cc: robert.beale@nrc.gov
Subject: [External_Sender] Docket No. PRM-50-112; NRC-2015-0213 "Important to Safety"

Secretary
US Nuclear Regulatory Commission
Washington, DC 20555-0001
Attn: Rulemaking and Adjudications Staff

Subject: Docket No. PRM-50-112; NRC-2015-0213 "Important to Safety"

I am a nuclear engineer with more than 40 years of experience in instrumentation, controls, and cyber security. I am currently the Managing Director of the International Society of Automation (ISA) 67 – Nuclear Plant Standards and ISA99 – Automation and Control System Cyber Security. I have also been designated by the International Electrotechnical Commission (IEC) as a US expert to the IEC Technical Committee (TC) 45A Nuclear Plant Cyber Security.

My concerns with the term "important to safety" arise from the electronic connectivity issues associated with cyber security. Depending on the electronic connectivity, systems that normally would not be considered "Important to Safety" can become so if they have connectivity with systems that are important to safety or are safety-related. In June, 2015, under contract to the International Atomic Energy Agency (IAEA), I analyzed three actual case histories of systems that would not be considered "important to safety" by themselves. However, because of connectivity to systems that are considered important to safety, each of these events resulted in significant plant safety impacts – automatic shutdown of a nuclear plant, loss of off-site power of a nuclear plant, and loss of view and control of a turbine.

The NRC Regulatory Guide for Cyber Security, Regulatory Guide 5.71, would not have considered the non-safety systems that were the precursors to these three events to have been important to safety. Consequently, the term "Important to Safety" needs to be broadened to include any systems that, through electronic connectivity, can affect safety systems.

Respectfully,
Joe Weiss, PE, CISM, CRISC
Managing Partner, Applied Control Solutions, LLC
Managing Director ISA67, Managing Director ISA99

Joe Weiss PE, CISM, CRISC, ISA Fellow, IEEE Senior Member, Managing Director ISA99
Applied Control Solutions, LLC
(408) 253-7934
(408) 253-7974 Fax
(408) 832-5396 Cell
joe.weiss@realtimeacs.com
www.realtimeacs.com
blog site: www.controlglobal.com/unfettered
Book URL: <http://www.momentumpress.net/books/protecting-industrial-control-systems-electronic-threats>

This message (with attachments) may be privileged, confidential, or proprietary. If you are not the intended recipient, please notify the sender and delete it. Do not use it or share it.