Chairman Resource

From: Joe Weiss <joe.weiss@realtimeacs.com>
Sent: Monday, August 29, 2022 12:41 AM
To: CMRBARAN Resource; Chairman Resource; CMRWright Resource
Subject: [External_Sender] Critical infrastructures cannot be secure when critical equipment isn't

I am the Managing Director of ISA99 - Control system Cyber Security and ISA67 - Nuclear Plant Standards. This Tuesday I have been asked to address the nuclear standards meeting (virtually). Years ago, as part of the PNNL team, I helped support the development of Reg Guide 5.71

August 25, 2022, I received a call from an insurance specialty insurer who had received an Operational Technology (OT) Supplemental Application from a global control system supplier to the aerospace industry, industrial operations, and the US Department of Defense. I am personally aware of at least some of the company's products because of their use in nuclear and fossil power plants, oil and gas facilities, and renewables. The OT Application had twenty-four questions with some having multiple parts. This Application demonstrates the culture and technical gaps between the IT and control system (OT) communities. The form was signed off by the supplier's Senior Director of IT Security. How can IT think it is OK not having OT cyber security experts involved? I, and others "in the know", do not believe this vendor's approach is unique and that other critical equipment suppliers are taking the same or similar approaches. How could any nuclear power plant with this vendor's equipment (this is most, if not all, US nuclear plants) pass an NRC cyber security audit? Even worse, this equipment is out-of-scope for a NERC CIP compliance audit. The responses to the Application raise questions about the validity of CISA's 100-day approaches when this vendor's equipment is an integral part of electric, water, oil/gas, pipelines, and chemical facilities.

https://www.controlglobal.com/blogs/unfettered/critical-infrastructures-cannot-be-secure-when-critical-equipment-isnt

Respectfully,
Joe

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