I thought you and the members of the SEAB might find this of interest as there have been more than 500 control system cyber incidents in the North American electric system (includes transmission, distribution, generation, and nuclear plants).

As a speaker, I have been given a complimentary registration code for the Minneapolis Cyber Security Summit next week that can be used virtually. The website is Cyber Security Summit and the Comp Code to use when registering for Onsite or Virtual attendance is _____. This code is for your use only – please do not share. My presentation is at 8:30AM Central time next Wednesday, October 26th. I think you will find my presentation will provide a different perspective on cyber security than the typical cyber security presentation that focus on securing Internet Protocol networks. It is an engineer's approach not a presentation about IT-OT convergence. The Solarwinds hack demonstrated that sophisticated attackers can maneuver around IP network protection. As a result, control systems need an alternate approach that can provide indication of the health of the process that is not susceptible to IP network attacks. Consequently, my presentation will touch on defining what is OT and what is a cyber incident, the cultural and technical gaps between networking and engineering, discussing control system cyber incidents in multiple industries that have caused major damage (not ransomware), and a path forward on what can be done to address control system cyber security, process safety, and reliability that would not be susceptible to IT malware or ransomware attacks. Please let me know if you have any questions.

Respectfully,

Joe

Joe Weiss PE, CISM, CRISC, ISA Life 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