INCOSE

(CIPR-wg)

Critical Infrastructure Protection & Recovery Working Group

International Call & Presentation – April 9

With the COVID19 pandemic currently ravaging the global population and our national economies, humanity has entered into a new, unprecedented era in history. Confronted with these massive challenges, some have pondered -- do we still need to worry about those "other" vulnerabilities - threat scenarios like cyber and other possible attacks on our critical infrastructure?
*The only rational answer is – **MORE SO NOW THAN EVER!!** It is an unfortunate but established reality that the enemies of our society do not sleep, and will perceive any potential weakness and vulnerability as an opportunity to further damage and undermine our systems and way of life.*

CONTINUED VIGILANCE IS NOT AN OPTION! SYSTEMS SECURITY IS ESSENTIAL!

The CIPR working group of INCOSE invites you to participate in this webinar.
09 April 2020, 3PM EDT / 12:00 PM Pacific (Call-in Information Below)

Speaker: Joe Weiss (quote)… ***"Security is a SYSTEM problem"***
Joseph Weiss is an expert on control system cyber security. He authored Protecting Industrial Control Systems from Electronic Threats and gave a keynote to the National Academy of Science, Engineering, and Medicine. He is an ISA Fellow and Managing Director of ISA Control System Cyber Security (ISA99). He was featured in Richard Clarke and RP Eddy's book- Warning – Finding Cassandras to Stop Catastrophes. He started the ICS Cyber Security Conference in 2002. He has two patents on instrumentation and control systems and is a registered professional engineer. Joe is a member of INCOSE, IEEE, ISA and other professional societies.

Abstract: Control systems are used to monitor, control, and safely shutdown physical process in commercial, industrial, manufacturing, medical, and defense applications. As such, control systems affect reliability, availability, safety, and resilience. Control systems are systems of systems consisting of field devices and networks. Consequently, securing control systems requires systems engineering. However, with the cyber security focus being on the Internet Protocol networks, there has been a lack of good system engineering practices on the control system devices. To date, there is a lack of cyber security, authentication, and cyber logging at the device and device network layer. There also has been a lack of training for the control system engineers to recognize potential cyber-related events. It should be noted that cyber incident does not need to be malicious to cause catastrophic damage. Moreover, a sophisticated attacker can make a cyber attack appear to be equipment malfunction. This has real ramifications as there have already been more than 1,200 actual control system cyber incidents resulting in more than 1,500 deaths and more than $70Billion in direct damage which includes both malicious and unintentional incidents. ***There is a crucial need for the engineering organizations including INCOSE, SAE, IEEE, ISA, InfraGard, and others to work together to address the grand challenge of cyber securing our infrastructures.***

Call-in Information: **Meeting ID:** 929 663 384 **Zoom App:** https://zoom.us/j/929663384

One tap mobile (US San Jose): +14086380968,,929663384#; +16699006833,,929663384#
Dial by your location: +1 408 638 0968 US (San Jose); +1 669 900 6833 US (San Jose); +1 346 248 7799 US (Houston); +1 253 215 8782 US; +1 301 715 8592 US; +1 312 626 6799 US (Chicago); +1 646 876 9923 US (New York); or, find your local number: https://zoom.us/u/aIzojIRyU