Autonomous Facilities

March 5, 2026, 7 am PST

Live Stream Seattle Washington

Join us for a session on Autonomous facilities. Find out how the AI is running them and how the human in the loop is observing. What kind of protection are we using to control the AI? What if the AI gets bad code? Can we safely shut down the facility? Are these robots and automated arms able to harm humans? Find out this and more at our upcoming session. Can we save you a seat at the table? Yes

Joe Weiss

Cybersecurity policies require that cyber incidents be identified as such. Cyber incident response plans are then initiated after incidents are identified as being cyber-related. To meet those goals, training is required to be able to identify control system incidents as being cyber-related and a mechanism to disseminate this information on control system cyber incidents throughout the organization as well as to relevant outside entities. Control system cyber incidents affect physics and therefore there are often physical reactions. That is trains crash, planes crash,

Register at:
https://www.mytechconference.com/event-details/fully-autonomous-facilites

Mike Brisbois, PE | 708.668.5488 | mike.brisbois@ieee.org

lights go out, water supply is compromised, pipelines burst, robots “misbehave”, etc. You can’t hide the impacts, but people often can’t (or won’t) identify the incidents as being cyber-related. US government reports from NTSB, NRC, DOE, EPA, TSA, FDA, etc. have not identified many control system incidents as being cyber-related nor have many internation government organizations either. Neither have industry organizations such as NERC. Government and industry cyber information sharing programs are about vulnerabilities not consequences. A concern about control system cyber incident disclosure was identified after 9/11 - connecting the dots. This is made more difficult with the silos between sectors and federal law enforcement withholding information that a cyber incident has occurred until an indictment is issued which can be a year or more.

Joe Weiss has over 40+ years in industrial instrumentation controls, and automation and 20+ years in cyber security of industrial control systems. He authored Protecting Industrial Control Systems from Electronic Threats ISBN: 978-1-60650-197-1 and Cyber Security Chapter Electric Power Substations Engineering.

Dr. Gambhir as Department of Artificial Intelligence and Data Science in place of Department of Computer Science and Engineering

Dr. Abdella

Register at:
https://www.mytechconference.com/event-details/fully-autonomous-facilites