

April 9, 2024

To: Secretary Granholm and distinguished members of the Secretary of Energy Advisory Board (SEAB)

Applied Controls Solutions, LLC appreciates this opportunity to provide information to the SEAB for consideration during its April 9, 2024 meeting.

February 24-25, 2024, I was invited by DOE to be an expert reviewer on the status of CYMANII - the Cybersecurity Manufacturing Innovation Institute. These were my observations from the February meeting and recent events that are relevant to all infrastructures under DOE's purview.

Safety and control system experts are generally not involved in cyber security. That is of great concern as considerations for cyber security and safety are often mutually exclusive.

CYMANII's Cyber Passport approach assumes the vendor can be trusted. Given that premise, it was not clear how CYMANII's Cyber Passport program could be applied for cases like the diesel cheat device scandal and port crane manufacturing. Chinese-made transformers, inverters, and port cranes may have hardware backdoors installed by the vendor which makes the software bill of material approach irrelevant. The cheat device scandal was insider cyberattacks against millions of products during the manufacturing process by trusted manufacturers. In February, the government issued a presidential executive order on Chinese-made port cranes from ZPMC which is not a trusted manufacturer. A congressional report warned that the ZPMC cranes have sensors installed that could affect the security and safety of the ports. The port cranes can also affect the electric distribution grid as they are directly connected to distribution substations and are trusted loads. **ZPMC port cranes were used in loading containers onto the MV Dali containership in the port of Baltimore before it crashed into the Key Bridge.**

Control system field devices (process sensors, actuators, drives, analyzers, etc.) are assumed to be uncompromised authenticated, and correct. Process sensor integrity is not being addressed yet has been shown to have significant impacts on productivity, efficiency, and safety whether from unintentional or malicious reasons. Compromised sensor data was used in the Stuxnet attack and could be used in Chinese port cranes, transformers, and inverters to compromise critical infrastructure operation. These issues are not being adequately addressed by DOE in any sector.

CYMANII and DOE's cyber security training is focused on Internet Protocol (IP) networks. There have been more than 100 control system cyber incidents in manufacturing. Control system cyber security impacts in manufacturing have resulted in production shutdowns, equipment damage, environmental impacts, bankruptcies, and even deaths. Inappropriate IP cyber security practices have contributed to some of these incidents. Most of the manufacturing control system cyber incidents were not IP network-related and were not identified as being cyber-related.

Control system cyber incidents are far wider than just in manufacturing. There have been more than 1,000 control system cyber incidents in the electric sector with six control system cyber-related outages affecting more than 80,000 customers. Most of the incidents were not identified as being cyber-related. The DOE OE-417 reports have identified hundreds of control system incidents such as complete loss of view and control in the main control room. However, very few of the OE-417 incidents were identified as being cyber-related. It should also be noted that the E-ISAC list of cyber incidents is far less than in the OE-417 reports. Because of the SEAB's discussions about data centers, it is important to note that there have also been numerous data center shutdowns and damage from control system cyber incidents that were not identified as being cyber-related.

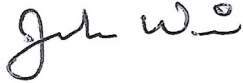
Identifying control system incidents as being cyber-related is the starting point for cyber incident response plans and the information sharing DOE has committed to provide industry. This is not being successfully addressed, which is why training needs to include identifying control system cyber incidents.

The Cyber-Informed Engineering efforts haven't adequately addressed the issues identified above.

What can be done

- Develop CONTROL SYSTEM cyber security training based on actual control system cyber incidents.
- Monitor process sensors at the "physics level."
- Include safety and control system engineers in all OT cyber security programs.

Respectfully,



Joseph Weiss, PE, CISM, CRISC
Managing Partner, Applied Control Solutions, LLC
Joe.weiss@realtimeacs.com
(408) 253-7934