Keynote Speaker 1

Charles Kim is a Professor in Electrical Engineering and Computer Science at Howard University. Professor Kim’s research includes fault and failure anticipation, detection, and location in aero-, naval-, and ground systems of electrical and electronic devices and networks. In line with his research on fault diagnostics, he has worked for safety and security for safety-critical systems in automotive, energy, aerospace, and nuclear industries. In control system’s cybersecurity, he has extensively published on cyber-robust diversified architectures for fail-operate resilient control systems even under compromised situations. Professor Kim received a PhD in Electrical Engineering from Texas A&M University, and he is a Senior Member of IEEE).

Title: Cyber-Resilient ICS through Diversified Redundancy and Intrusion Detection

Abstract: Technological advancement of Industrial Control Systems (ICS) and control systems automation over the past decade has brought greater interconnections of the control devices. The control devices are interconnected via modern control communication bus such as ModbusTCP which now leverages Ethernet to allow interoperability between different solutions and vendors. The enhanced exchange of information has created cyber security vulnerabilities such as entry points for hackers. This presentation discusses diversified redundant architecture as a cyber-resilient system for networked control devices which maintains their normal operation even under compromised situations. This operation-based resilient architecture adds an isolated device, functionally equivalent to the networked primary device but with essential safe-mode operation features only, which is naturally immune to cyber incidents. In addition, a supervisor component monitors the operation of both networked and isolated devices, and transfers control to the safe-mode isolated device if the networked device operates abnormally, assuming that the abnormal operation is resulted from malicious hacking which has not been detected from the network cyber security defense. However, even with its resiliency, the diversified architecture has its own blind side – unawareness of presence of hacking traffic on the control bus when operational changes are not made by the hackers. Therefore, to solve this problem of unawareness of and undetected intrusion, we improve the architecture with an additional feature of intrusion detection utilizing open source software called Snort. The security features of Snort are incorporated as an intrusion detection and awareness solution, and are customized into the supervisor component of the diversified architecture for Modbus TCP/IP traffic monitoring. In laboratory tests, the added feature of intrusion detection has successfully initiated a safe-mode control transfer to the isolated device upon detection of unusual data traffic on the control bus. With this bus monitoring and intrusion detection, the diversified architecture would become a truly resilient and secure networked industrial control system.