CYBERSECURITY LECTURE SERIES

FROM RELIABILITY TO RISK: SECURITY DEBT IN MODERN INDUSTRIAL CONTROL SYSTEMS

March 23 at 9:30 - 11 a.m.

DMC Theater, LSU Digital Media Center

Irfan Ahmed

VIRGINIA COMMONWEALTH UNIVERSITY

ABSTRACT

Industrial Control Systems (ICS) were engineered for determinism, availability, and safety, not adversarial resilience. Over decades, reliability-driven design assumptions in programmable logic controllers (PLCs) and control networks have accumulated into a form of security debt that modern cyber-physical threats can exploit.

This talk synthesizes insights from real-world PLC firmware analysis, memory forensics, and control-logic integrity research to expose structural weaknesses: implicit trust in runtime execution, limited integrity verification, insecure update and communication pathways, and minimal forensic visibility. These systemic gaps enable stealthy manipulation of physical processes while preserving outwardly normal behavior, challenging traditional detection and safety mechanisms.

The talk argues that incremental patching cannot resolve insecurity rooted in architecture. Instead, the field must move toward redesigning ICS for security, grounded in verifiable execution semantics, strong integrity guarantees, and forensic-ready industrial infrastructures that can sustain long-term trust and resilience.

SPEAKER BIO

Dr. Irfan Ahmed is a Professor of Computer Science in the College of Engineering at Virginia Commonwealth University (VCU) and a leading researcher in cybersecurity, digital forensics, and the security of industrial control and cyber-physical systems. His work focuses on PLC firmware analysis, control-logic integrity, memory forensics, and adversarial threats to critical infrastructure and advanced manufacturing. He has received multiple national recognitions, including the USCYBERCOM Commander, Guardian, and Defender Awards, for developing innovative defensive technologies for operational technology environments. Dr. Ahmed collaborates with national laboratories, industry partners, and government agencies to advance secure-by-design industrial platforms and workforce development in critical infrastructure protection. His research aims to restore trust, resilience, and forensic readiness across next-generation industrial control systems and advanced manufacturing.