



## ***Transforming the Resilience of Critical Infrastructure Systems and Communities***

**Resilience Week Objective:** A Symposium dedicated to advancing the interdisciplinary dialog on policy and technologies that accelerate critical infrastructure and community resilience to unexpected and malicious threats.

### ***Session 08: Agile Cybersecurity Response Capabilities for Control Systems***

#### **Session Chair**

Andrew Storms, VP Product and Security Services for New Context Services, Inc.

[astorms@newcontext.com](mailto:astorms@newcontext.com)

#### **Session Abstract**

IT security professionals have already recognized that automated detection and response to cyber-attacks is a necessary component in order to combat increasing cyber threats. ICS environments must function on millisecond responsiveness and yet humans are required today for nearly all operational responses. The industry needs to transform its tools and processes to provide a more agile cybersecurity response capability.

Moving the industry from manual and complex cyber security threat intelligence response to automated response is a heavy undertaking. Not only are these systems often complex and heterogeneous, but the historical culture of the ICS world is one of ingrained institutional knowledge that are less apt to share.

This session will focus on challenges and lessons learned to help move the industry to support agile automated response mechanisms. Areas of interest may include use of machine-readable threat frameworks, the risks of automated responses, implementing governance on automation, providing enough context to enable the defenders to identify appropriate remediation actions.