Cybersecurity at MIT Sloan brings together thought leaders from industry, academia and government with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

**Security Weaknesses in Cyber Physical Systems (CPS)**

A cyber-attack to a CPS is more than just a threat to virtual space; it can create real, physical hazards. This was the case in 2010 when the Stuxnet virus infiltrated an Iranian nuclear power plant controlled by a Cyber Physical System. Traditional IT safety strategies and approaches are not sufficient to address the security challenges of a CPS. Assessments that analyze the failure of individual components miss critical threats to the *interactions* between these components. Research by Cybersecurity at MIT Sloan explores better approaches to CPS protection. This project utilizes case studies such as Stuxnet to study threats and vulnerabilities and suggest how the problems could be addressed at the most basic levels of device design.

**IMPACT:** Since traditional IT approaches are not enough, this research develops new approaches for dealing with cybersecurity in a CPS; Using these analysis methods, threats can be mitigated at the system design level.

**Stuxnet Attack Diagram**

Cybersecurity at MIT Sloan welcomes funding from sponsors for general support of the consortium research, and from organizations interested in specific research topics. All members and sponsors receive invitations to consortium events and activities, and access to consortium research, websites, and newsletters. For more information, visit https://ic3.mit.edu or contact:

- Dr. Stuart Madnick • Professor and Director • smadnick@mit.edu
- Dr. Michael Siegel • Director • msiegel@mit.edu
- Dr. Keri Pearlson • Executive Director • kerip@mit.edu