

Data Center Operational Cybersecurity

8/7/26



Joe Weiss

PE, CISM, CRISC, ISA Fellow

Managing Partner

Applied Control Solutions, LLC

joe.weiss@realtimeacs.com

(408) 253-7934

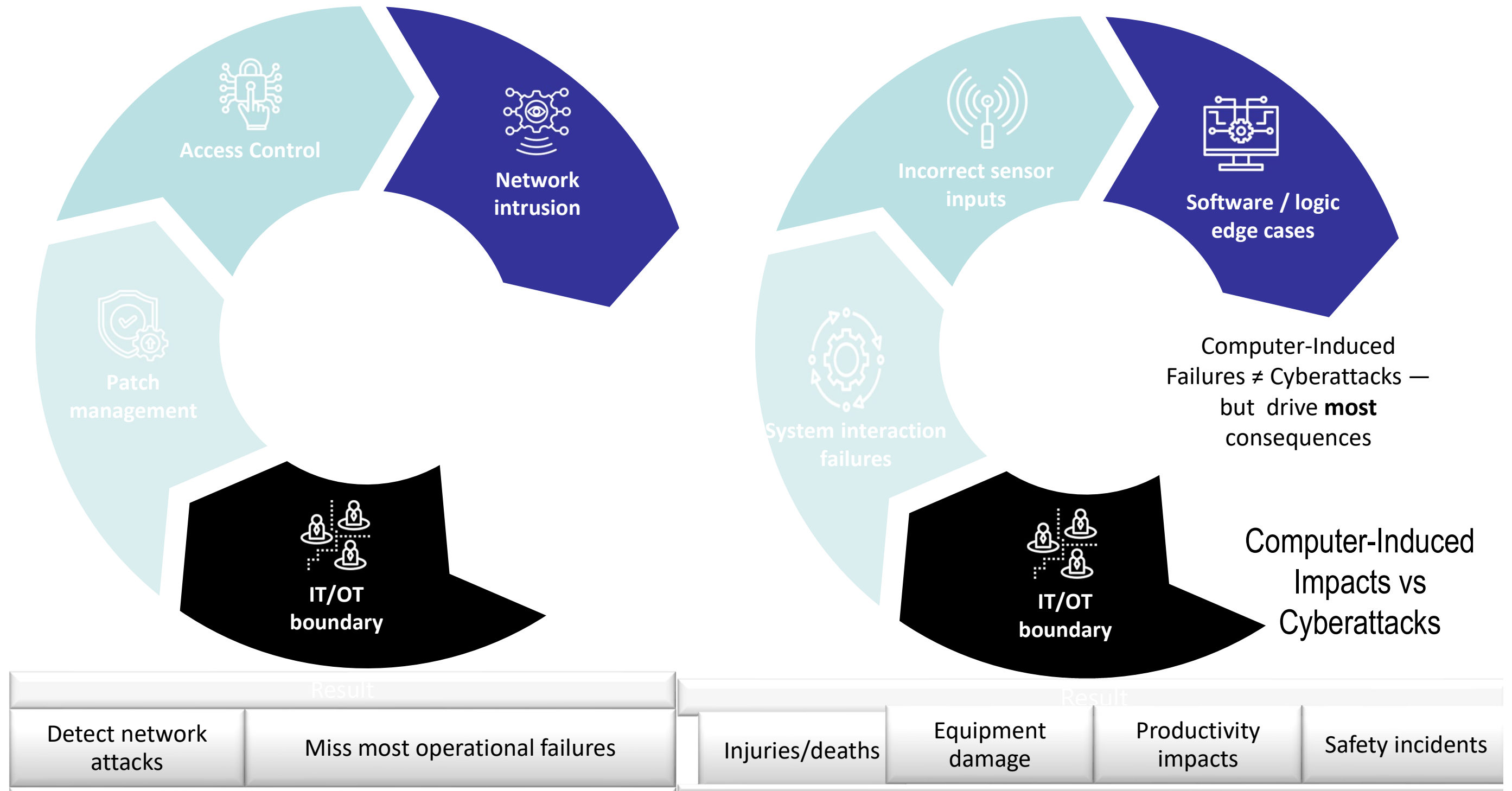
Control system cybersecurity

- Cybersecurity concerns the confidentiality, integrity, and availability of electronically communicated information
- Security engineering is about building systems that remain dependable in the face of malice, error, or mischance
- Control system cybersecurity protects the integrity and availability of electronically communicated information that monitors and controls physical equipment
- *Millions of control system cyber incidents have occurred, many involving incorrect or unavailable process information rather than traditional network compromise.*
- *Control system devices such as process sensors and actuators are generally ignored*

We Are Solving the Wrong Problem

What the Industry Focuses On

What Actually Causes Harm/Operational Impacts



Control system cyber data center impacts

- Malicious cyber attacks
 - Damaged all servers
 - Data center fires
 - **WATER FACILITIES**
 - Others
- Unintentional cyber incidents
 - Control system logic issues
 - Sensor/actuator issues
 - Network switch broadcast storm shuts down facility
 - Others

What needs to be done

- Define control system cybersecurity separately from enterprise IT cybersecurity
- Develop policies, procurement requirements, and workforce training
- Independently monitor process sensors using physics-based validation
- Incorporate sensor cybersecurity into safety and reliability programs
- Ensure that network security and engineering are collaboratively working

Benefit: Improved safety, reliability, predictive maintenance, and security

Joe Weiss
Applied Control Solutions, LLC
joe.weiss@realtimeacs.com
(408) 253-7934
www.controlglobal.com/unfettered