ICS SCADA Operations

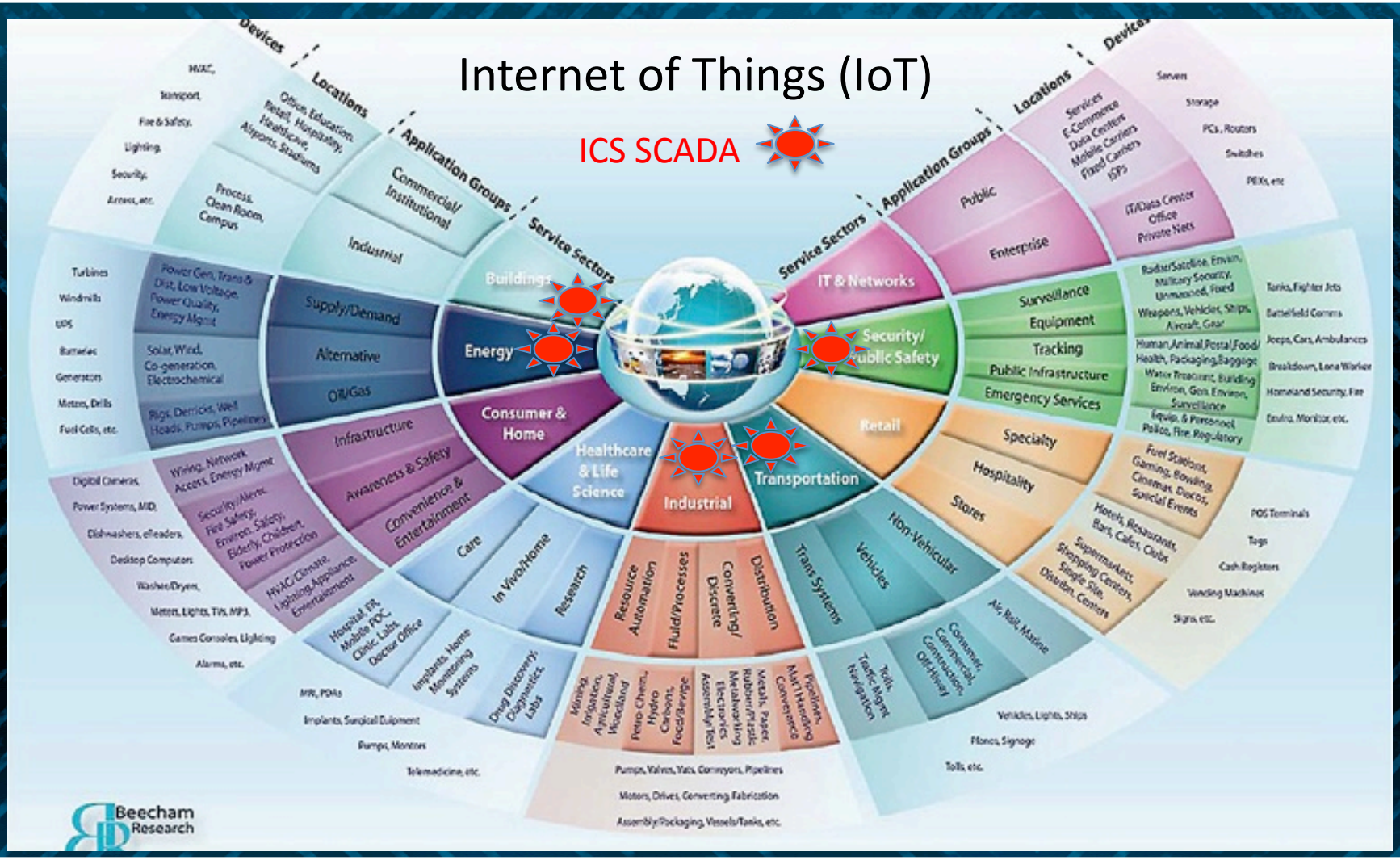
Joe Klein, CISSP …

5/21/14

DISRUPT 6

Internet of Things (IoT)

ICS SCADA




SCADA Systems In Was

Definitions

ICS - Industrial Control Systems

- Command and control networks and systems designed to support industrial processes

SCADA - Supervisory Control and Data Acquisition Systems

- The largest subgroup of ICS

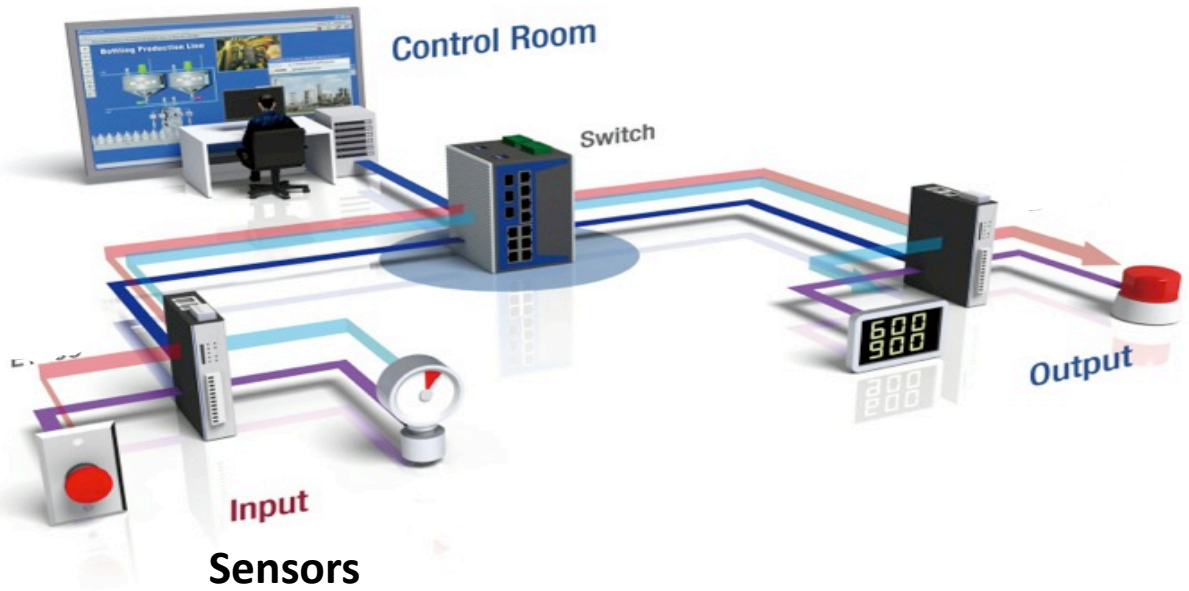
Primary Functions

- Data Acquisition
- Data Communications
- Data Presentation
- Control

Equipment

- Sensors & Controls
- SCADA RTU’s
- SCADA Master
- Communications

ICS SCADA Network

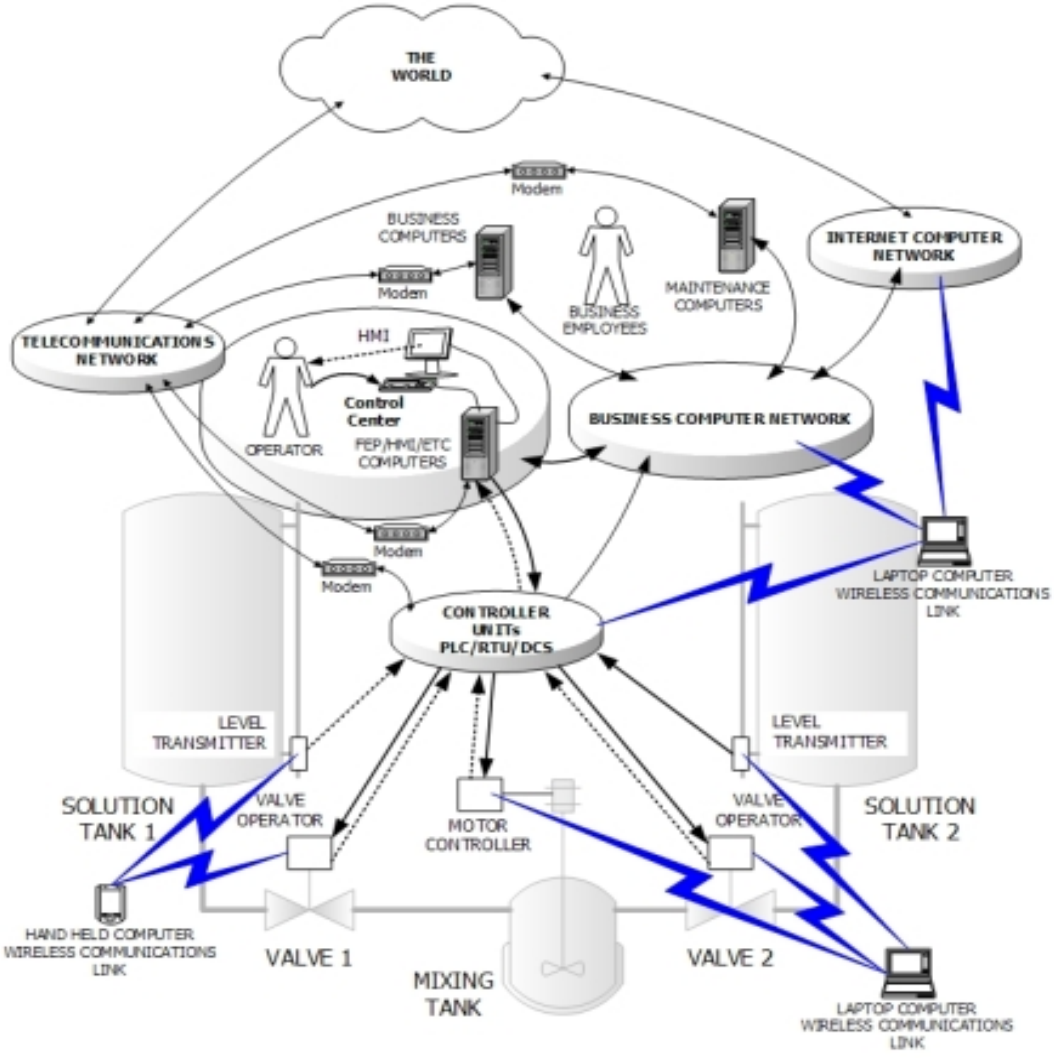


Sensors

ICS gone bad? Staged cyber attack (2007)

https://www.youtube.com/watch?v=fJyWngDco3g

ICS Vulnerabilities



Problems

- Wired
- Wireless
- No trust models
- No data isolation
- No security model
- Physical Access
- No Anti-Malware
- Security Monitoring
- Redundancy

Key Flaws in the System

- Protocol Design
- System Design
- System Implementation
- Procurement & Supply Chain
- System Maintenance & Operation

Vulnerabilities 2013

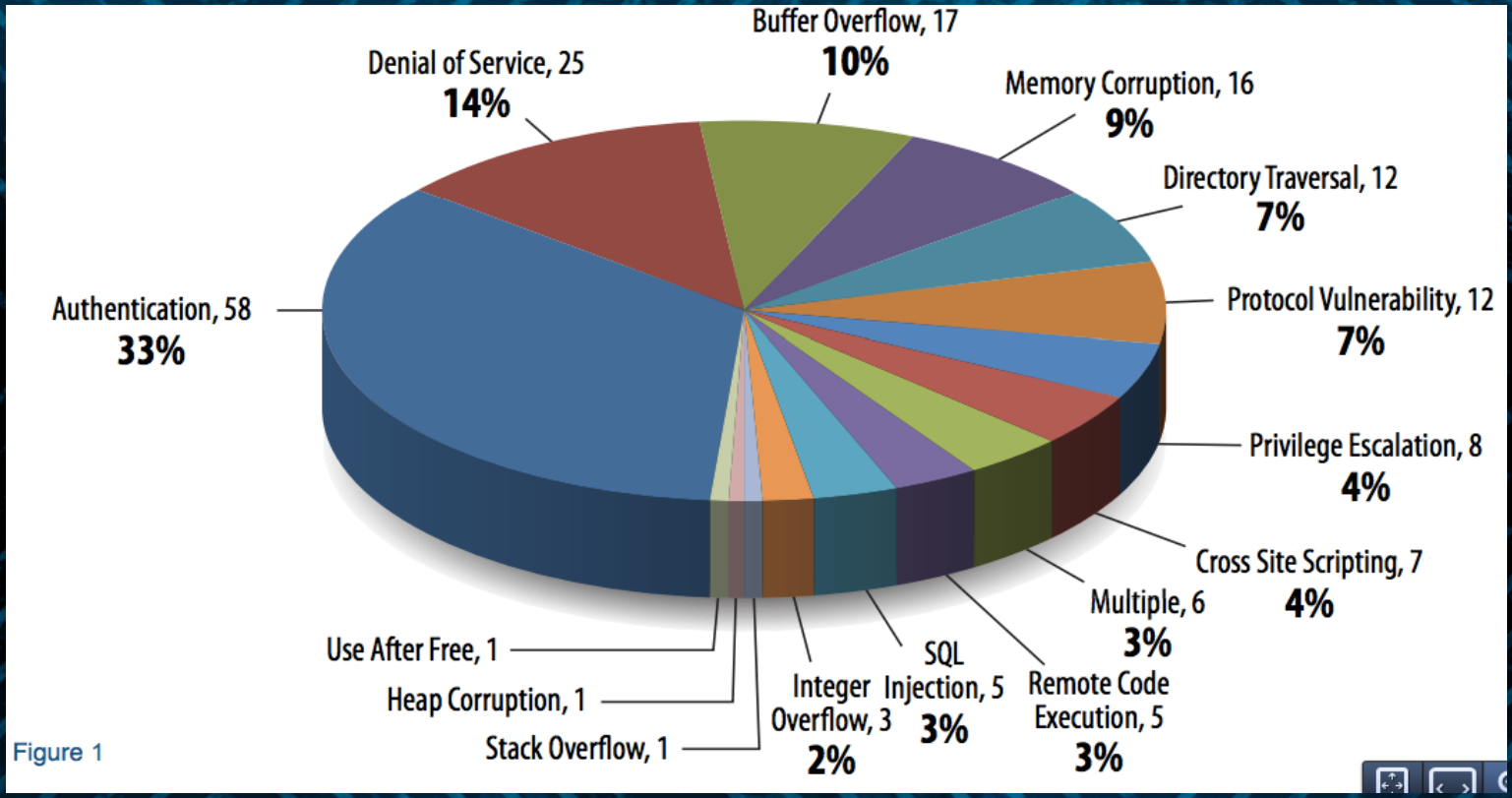


Figure 1

Resources

- DHS ICS-CERT
- NIST SP 800-82
- SCADA Hacker Library
- Digital Bond – S4 Conference & podcast
- International Symposium for ICS & SCADA Cyber Security Research

ICS SCADA Operations

Joe Klein, CISSP …

5/21/14

DISRUPT 6