

Security Challenges in Next Generation Cyber-Physical Systems

Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, Zachary Ives
and Insup Lee
University of Pennsylvania

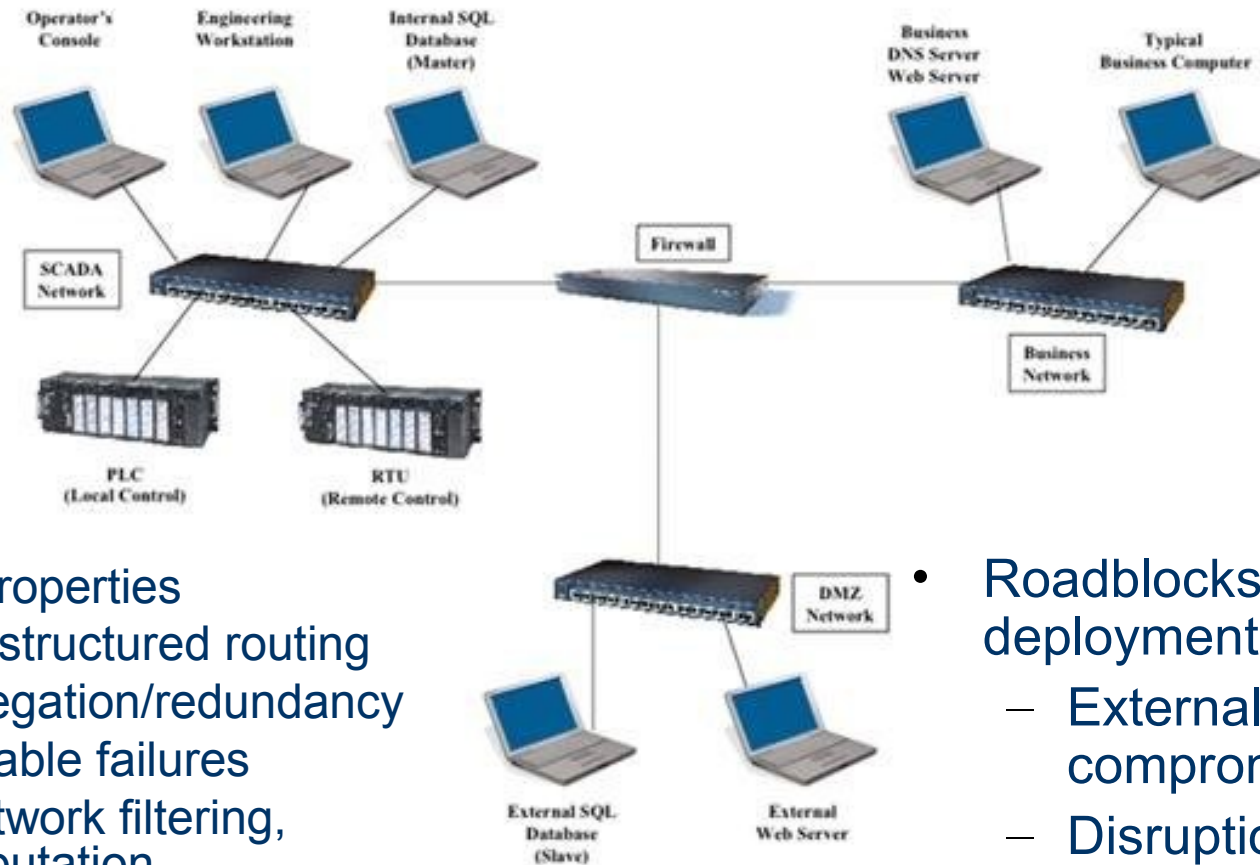


Attack!

Mission: Impossible (1996) anticipated the use of temperature-sensitive notes in a mission-critical application



Where things break down



- Unique Properties
 - Tree-structured routing
 - Aggregation/redundancy
 - Tolerable failures
 - In-network filtering, Computation
 - Phased transmission periods.

- Roadblocks for global deployment:
 - External sensor compromise
 - Disruption
 - State of system confidentiality
 - Sensor replacement.

Cyber-Physical Systems ≠ Internet

1. Measuring Confidentiality
 - Deal with partial compromise, rather than all-or-nothing guarantees.
2. Context Obfuscation
 - Timing, location information needs to be protected.
3. Secure Aggregation
 - End-to-end security solutions cannot work with data aggregation.
4. Topology Obfuscation
 - Secure the non-uniform distribution of information.
5. Scalable Trust Management
 - Develop lightweight solutions that allow reestablishment of trust.
6. Aggregation with Privacy.
 - Sensing is a *passive* activity. Develop techniques that preserve anonymity.