Quantifying and Optimizing ICS Cyber-Resilience (CR)

GOAL: Design a systematic framework that quantifies cyber-resilience in OT/ICS networks and further optimizes it using graph-based cyber-protection heuristics

Ranjan Pal, Michael Siegel

MIT MANAGEMENT SLOAN SCHOOL

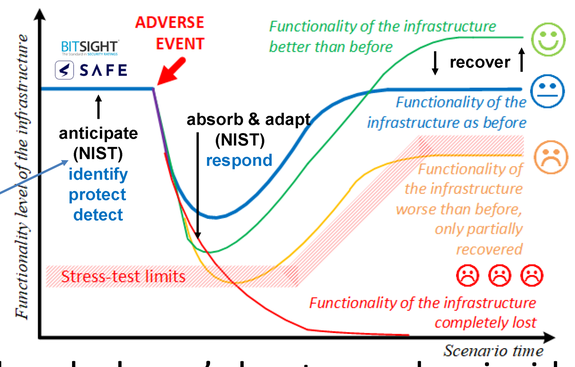
Cybersecurity at MIT Sloan

1. A cyber-driven service disruption is too likely in industrial control systems

1. Modern ICSs are IT and operational technology (OT) driven systems with a big unpatched cyber-risk terrain.
2. Most ICSs comprise legacy components in hardware, software, firmware that are outdated to secure today.
3. Substantial networked OT inventory lacking visibility.
4. Most ICS managements are naively security aware.
5. Hackers are way ahead than ICS security practices.

End Result – ICSs are too vulnerable to (state) hackers!

2. ICS management needs to *assure* a baseline QoS post any cyber-incident

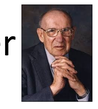


Even if 'hell breaks loose' due to a cyber-incident, ICS managements need ensure *every system performance metric is above 'stress test baselines' all times (NIST).*

3. A precondition of assurance is to be able to *quantify* ICS cyber-resilience

NIST defines cyber-resilience as an ability of a firm to *anticipate*, *absorb*, and *recover* from a cyber-incident.

"If we can't quantify, we can't manage" – Drucker

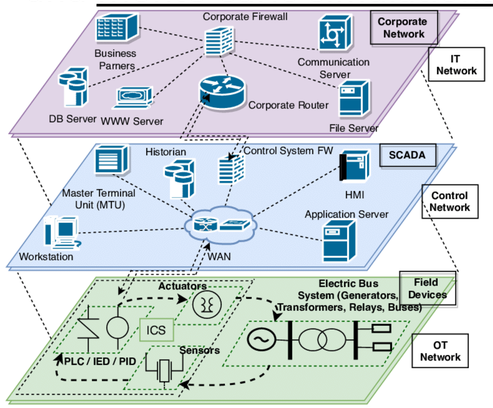


Research Sub-Problem #1

Quantify the ability of an ICS with networked and interdependent OT components to be above stress test limits in events of attack on critical components.

4. We pioneer a framework quantifying CR in OT/ICS networks

We propose a quant framework designed via applying probability theory, network science, and Monte Carlo simulations to quantify cyber-resilience in OT-networked ICSs.



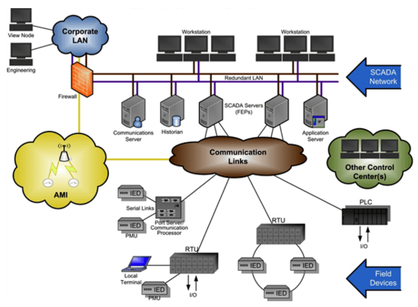
Defense-in-Depth ICS N/W Architecture

Key Framework Novelty Elements

1. We model how direct adverse impact on QoS of network component(s) indirectly affects QoS of dependent components.
2. We deploy network science and probability theory to model all likely ICS network architectures and direct attack scenarios.
3. We estimate using Monte Carlo simulations the time for an ICS to adapt working at a stable baseline+ QoS post incident.

5. We pioneer graph heuristics to optimize CR in ICS networks

A management/board wants to allocate a cyber-protection budget among its *'crown jewel'* components of the ICS network to maximize system cyber-resilience (business continuity).



SCADA ICS Network Topology

ICS CR Optimization Challenges

1. Constrained protection budget approved by management.
2. Satisfying individual component QoS along with optimal CR.
3. Arbitrary ICS network topologies (graphs) to deal with.

Research Sub-Problem #2

Optimize ICS network CR under optimization challenges.

We propose Monte Carlo simulation validated graph heuristics by applying OR and network science theory, to (a) identify ICS 'crown jewels' and (b) optimize cyber-resilience.

1. OR tools (TOPSIS) allow management to rank the crown jewels to be cyber-protected.
2. Network heuristics adopt rank order to optimize CR under constrained security budget.

6. Action items for ICS management on boosting cyber-resilience

1. Identify 'crown jewels' in the ICS network and use CVE/CVSS to score their vulnerabilities.
2. Quantify CR for the ICS network even before any cyber-incident to score overall robustness.
3. Boost CR by allocating protection budget among 'crown jewels' in proportion to their rank.
4. Optimize CR by ranking 'crown jewel' importance based upon *Risk-by-Context* (RbC) idea.

Contacts: ranjanp@mit.edu, msiegel@mit.edu *Credits:* asvin cyberagentur Rohan Sequeira (USC)