

NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Risk Analysis Results & Mitigation Discussion

Ron Halbgewachs

Laurie Phillips

Sandia National Laboratories



**U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability**



Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Recap of Fictional Rogue Software Scenario

- The scenario as initially conceived: At a time fixed in advance, a small rogue software program would issue a “trip” command to every accessible breaker.
- Preliminary internal discussions suggested that an unsophisticated adversary could cause a big problem
 - The rogue code would be simple, compact, and easily hidden
 - It would need to be installed on only a few machines
 - It would be used only once
 - forensics and real-time detection would play no role
 - It would not need to be stealthy or clean up after itself
 - The sudden loss of generation would result in a large-scale cascade and multi-day regional outage
 - A large area would be affected and consequences would be great

What we learned

- **CAVEAT:** Risk assessment requires data we didn't have (e.g., specific regional system architecture), so some questions are unanswered
- **Threat:** Scenario-relevant information is readily available on the web
- **Effect:**
 - Successful performance of the scenario cyber activity is straightforward
 - Fixed execution time is not effective; the power system must be under stress (stage 2 alert is required)
- **Impact:**
 - The impact of a single event is low; the generators aren't damaged
 - Follow-on cascade is hard to predict and very hard to model
 - As the event is repeated and more breakers are affected, expected load loss increases significantly over the base case
- **Consequence**
 - Not homogenous across the nation
 - Financial impact can be enormous for small utilities if they're found responsible
 - Insurance companies and government can be hit hard; they are "loss collectors"
 - Increases significantly if the event is widespread and repeated

Summary of Threat-to-Consequence

Threat requirements	
\$ needed	HIGH danger
Physical infrastructure (knowledge)	HIGH danger
Must be willing to risk	MODERATE danger
Organization size	MODERATE danger
Cyber (knowledge & access)	LOW danger
Stealth	LOW danger
Length of time needed	LOW danger

Cyber Effects	
Attack Feasibility	HIGH danger
Potential Effectiveness	HIGH danger
Feasibility with Software Inspection	MODERATE danger
Feasibility with Network Monitoring	MODERATE danger

Impact	
If widespread and repeated	HIGH danger

Consequence	
Cost (including cost due to regulatory effects and operational uncertainty)	MODERATE danger
Business disruption	MODERATE danger

NB: large variation depending on frequency and spread

Danger to the Defender
HIGH danger
MODERATE danger
LOW danger

Post-analysis assessment: Risk is Low-Moderate

- Effect
 - The key cyber effect is straightforward but can be mitigated
- Impact
 - Depends on system state and architecture
 - Hard to predict beyond the affected system
 - Increases dramatically if the event is widespread and repeated
- Consequence
 - Varies greatly from region to region
 - Low to moderate if the event happens only once
 - Increases dramatically if the event is widespread and repeated
- To have high impact and consequence, the rogue software:
 - Must be stealthy and hard to eradicate
 - Must as a result be much more complex than our preliminary idea
- The rogue software scenario requires a sophisticated adversary with significant knowledge and resources.
 - IC Analysis has provided no indication of threat interest at relevant level
 - If such a threat did have interest, risk would be high

Threat-to-Consequence Framework



Challenges/Needs

- Develop a qualitative approach to risk analysis
- Improve accuracy of relative risk estimates
- Rate the full spectrum of cyber risk

Results/Benefits

- Develop tools to support proactive holistic risk analysis
- Develop a “playbook” of well-understood risks
- Foster dialogue to incorporate industry perspective

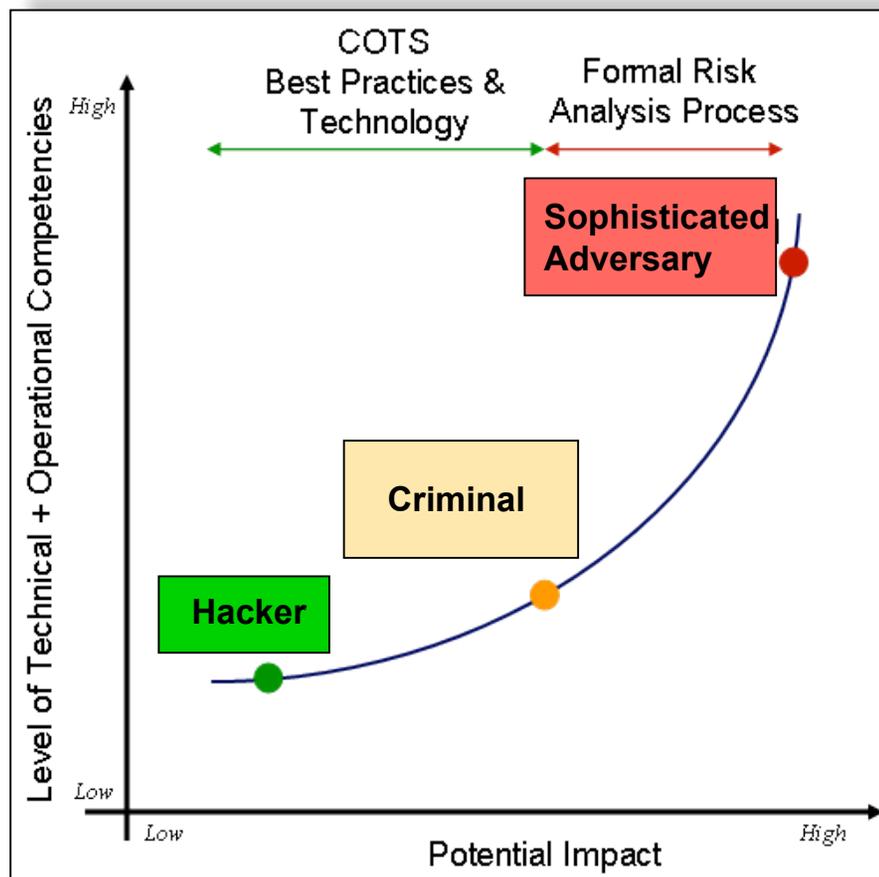
Threat-to-Consequence Framework



- **What mitigation is possible for this attack?**
- What resources can be used to mitigate such an attack?
- How would you recover from the rogue software attack?
- How would you mitigate direct risk to your system under this scenario?
- How would you mitigate indirect risk to your system as a result of interties?
- Can best practices address the rogue software attack?
- Does the use of the FEP constitute a single-point-of-failure?
- **What other questions should be asked in considering the mitigation to this attack?**
- **How can the threat-to-consequence framework be used to prioritize risk reduction activities that address this rogue software attack?**

Risk Mitigation: Approach

- A “Holistic” approach is needed; best practices alone leave gaps
- We recommend using best practices
 - These are cybersecurity tactics that have “stood the test of time”
 - They address many common risks and negate a vast array of low-level threats
 - The cost is known and relatively moderate
- But best practices do NOT address:
 - Sophisticated adversaries
 - Newly discovered weaknesses
 - New operations

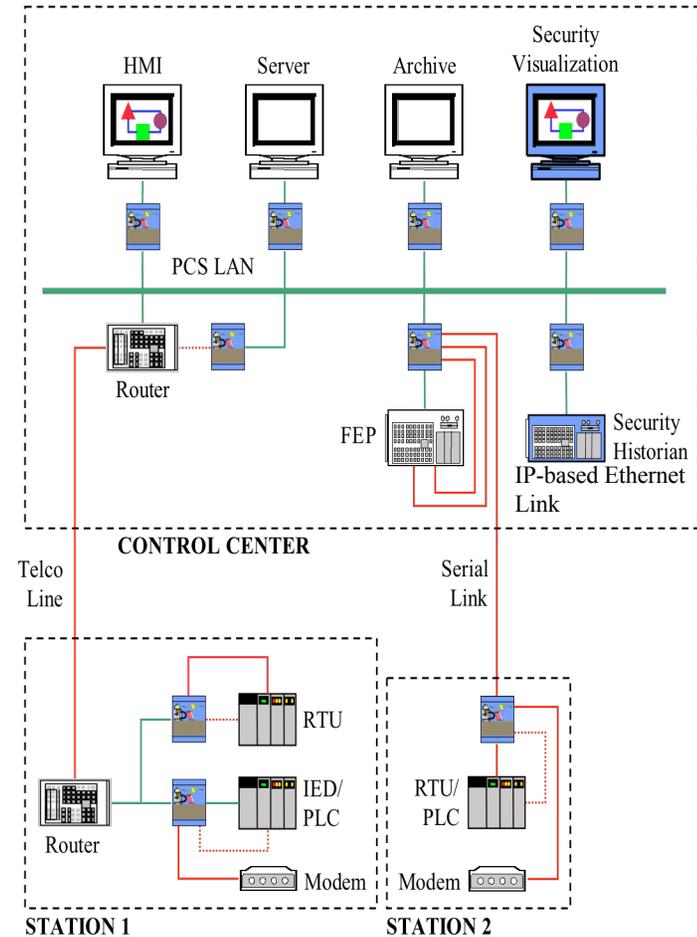


Security Considerations

- Control system monitoring and visualization of the monitored information
- Data logging capture for replay and forensic analysis
- Use of encryption and data authentication
- System intrusion detection and prevention
- Firewalls and network filtering
- Authentication and logging for remote access
- Host intrusion detection and prevention
- Interoperability of control system elements

Reduce the Risk

- Utilize systems that offer built-in cyber security.
- Develop components that operate with any control system.
- Plan for “agile operator” cyber defense training.
- “Raise the bar” – make an attack more and more difficult for an adversary; eliminate the lower level threats by making any attack more costly in time, skill level, access, & money.



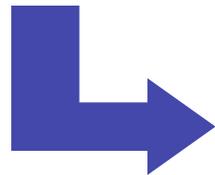
Suggestions to protect against rogue software

- Modify the architecture of the control system. Alternatives to the use of a FEP?
- Establish an independent communication channel for authentication between trusted elements; one at HMI for operators and another at RTU/PLC/Relay.
- Development of Host Intrusion Detection utilizing trusted communications units; requires an initial trusted version of the FEP software and would be used to protect against a maintenance upload of malevolent software.

Risk Analysis from Threat-to-Consequence Framework

- ➔ Threat Analysis:
- ➔ Cyber Effects:
- ➔ System Impact Analysis:
- ➔ Consequence Analysis:

Risk Mitigation:
Analyze, Plan,
Anticipate, Review



Overall Risk Analysis:



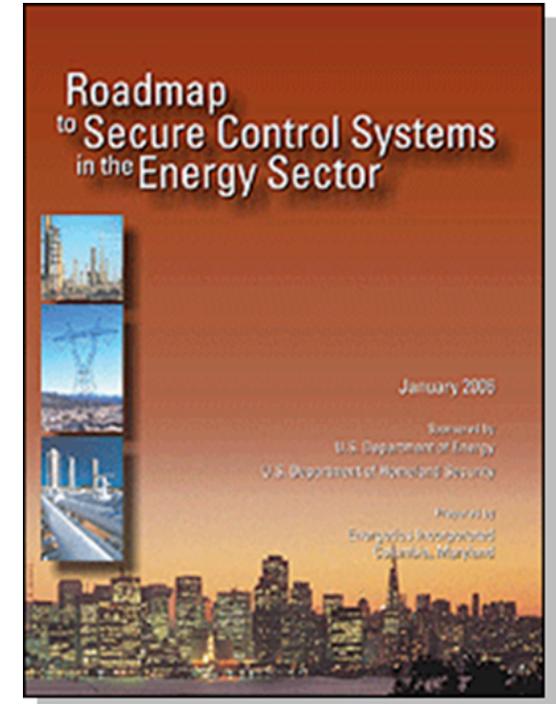
Backup Slides

Template for Action

“By systematically **documenting** and **prioritizing** known and suspected control system **vulnerabilities** (**threats**) and their potential **consequences**, energy sector asset owners and operators will be better prepared to **anticipate and respond** to existing and future threats.

...to more effectively **implement mitigation and response plans...**”

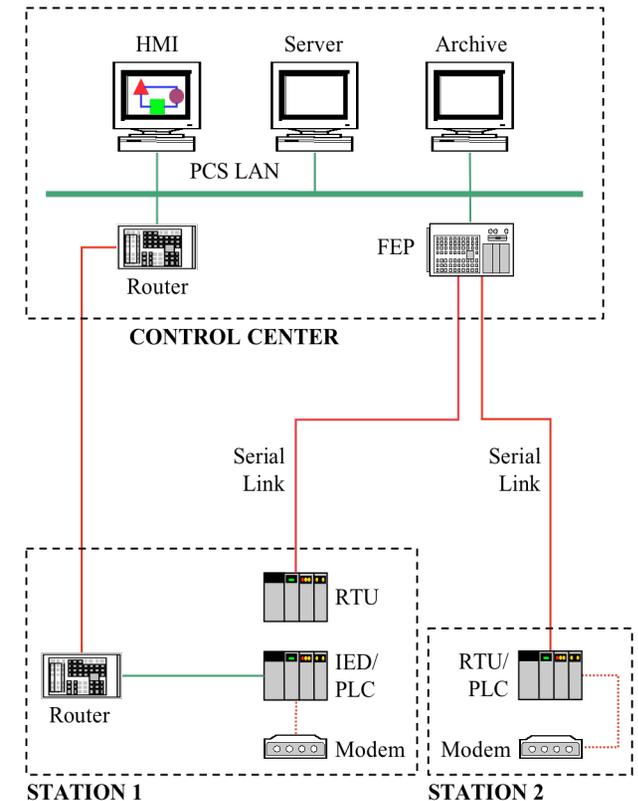
(Identifying Strategic Risk, page A2)



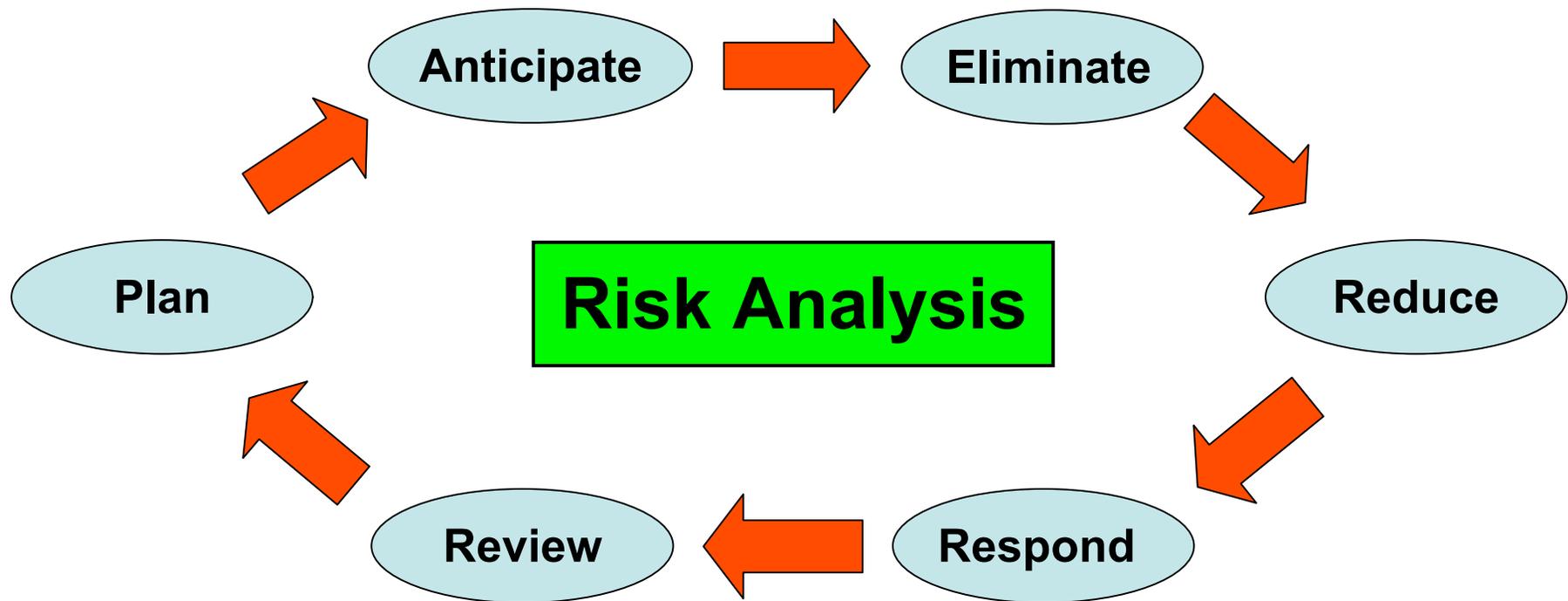
Roadmap to Secure
Control Systems
in the Energy Sector
January 2006

Steps Leading to Mitigation

- Having identified
 - potential & plausible threats
 - system vulnerabilities
 - Impacts
 - consequences
- Risk has been defined to be a function of Threat, Vulnerability, & Consequence
- ***What can be done to mitigate the risk?***

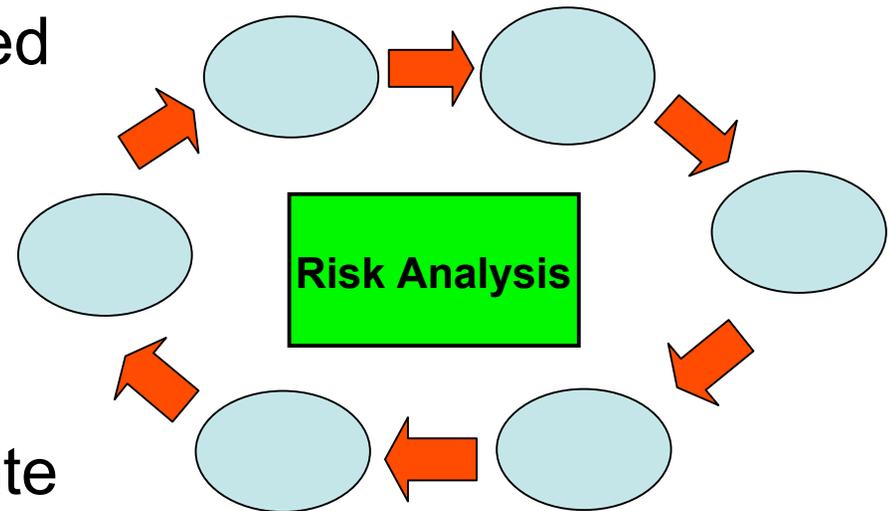


Risk Mitigation Process



Risk Mitigation – Full Spectrum Analysis

- All aspects of the cyber control system should be analyzed
- All threat levels should be considered
- Determine what impacts different vulnerabilities will have on your system
- Determine what can effectively be implemented at a cost commensurate with the protection provided
- Develop a risk mitigation plan and review periodically since all aspects of the problem change over time



Anticipate the Potential Risk

- Perform the risk analysis process through each step.
- Evaluate levels of risk:
 - Local level – asset owners & customer base
 - Regional level – extending beyond local system
 - National level – cascading even beyond a regional level or a regional effect for an extended period of time
- Determine time of recovery – temporal conditions present an additional dimension to the risk

Eliminate the Risk

- Utilize systems that offer built-in cyber security.
 - Determine what risks can be eliminated:
 - Identify those threats your system can protect against; establish barriers; render the threat as non-existent
 - Eliminate the vulnerability
 - Reduce the consequence to an extremely low level; assure there can be no cascading effects
 - What key elements of security must be in place?
- Develop effective countermeasures; segmentation of the system.

Respond to the Risk

- Assure there are processes in place to respond
 - At the local level: specifically addressing your own facilities, assets, customers owners
 - At the regional level: cascading beyond local bounds
 - At the national level: extending beyond local & regional systems; major national consequence
- Establishment of communication with first responders that might be needed in a attack of major consequence.

Mitigation - Response

Catalog of Control Systems Security: Recommendations for Standards Developers (CCSS 2.2.4)

The organization's security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.

Supplemental Guidance:

Expand relationships with local emergency response personnel to include information sharing and coordination of contingency plans as well as coordinated response to cyber security incidents.

Review the mitigation planning

- All elements that compose the risk to the control system change with time: threats, vulnerabilities, consequences, and hence how we must be prepared to respond to those changes.
- Periodic review required to stay diligent in the protection of our control system, systems around us, and the infrastructure of the U.S.

Planning for Risk Mitigation

Just as the organization considers the risks associated with physical and environmental hazards when planning new control system facilities or reviewing existing facilities...risk mitigation strategies are documented in the control system security plan. (CCSS 2.4.18)

Risk-reduction mitigation measures are planned and implemented and the results are monitored to ensure effectiveness of the organization's planning process. (CCSS 2.7.9)