SAND2012-9027C

Cyber Security Triage for Small Water Utilities

A case study in identifying essential system equipment and cyber security first steps for a small utility

Lon Dawson, Anna Hernandez, Doug Dailey (URS), Will Atkins, Patrick Edgett, Keith Schwalm (DNK), Ray Finley, Robert Pollock

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Outline

- DHS Critical Spares
  - Project Purpose and Process
  - Status and Objective for today
  - Methodology Overview
- Assessment Activities and Findings
- Recommendations

Sandia National Laboratories

Critical Spares Project - Purpose

- **Sponsored by the Department of Homeland Security's (DHS) Control Systems Security Program (CSSP).**

- **Purpose - To develop and validate an all-hazards (with cyber-slant) methodology for measuring the level of risk to the identified components and determining the appropriate response.**

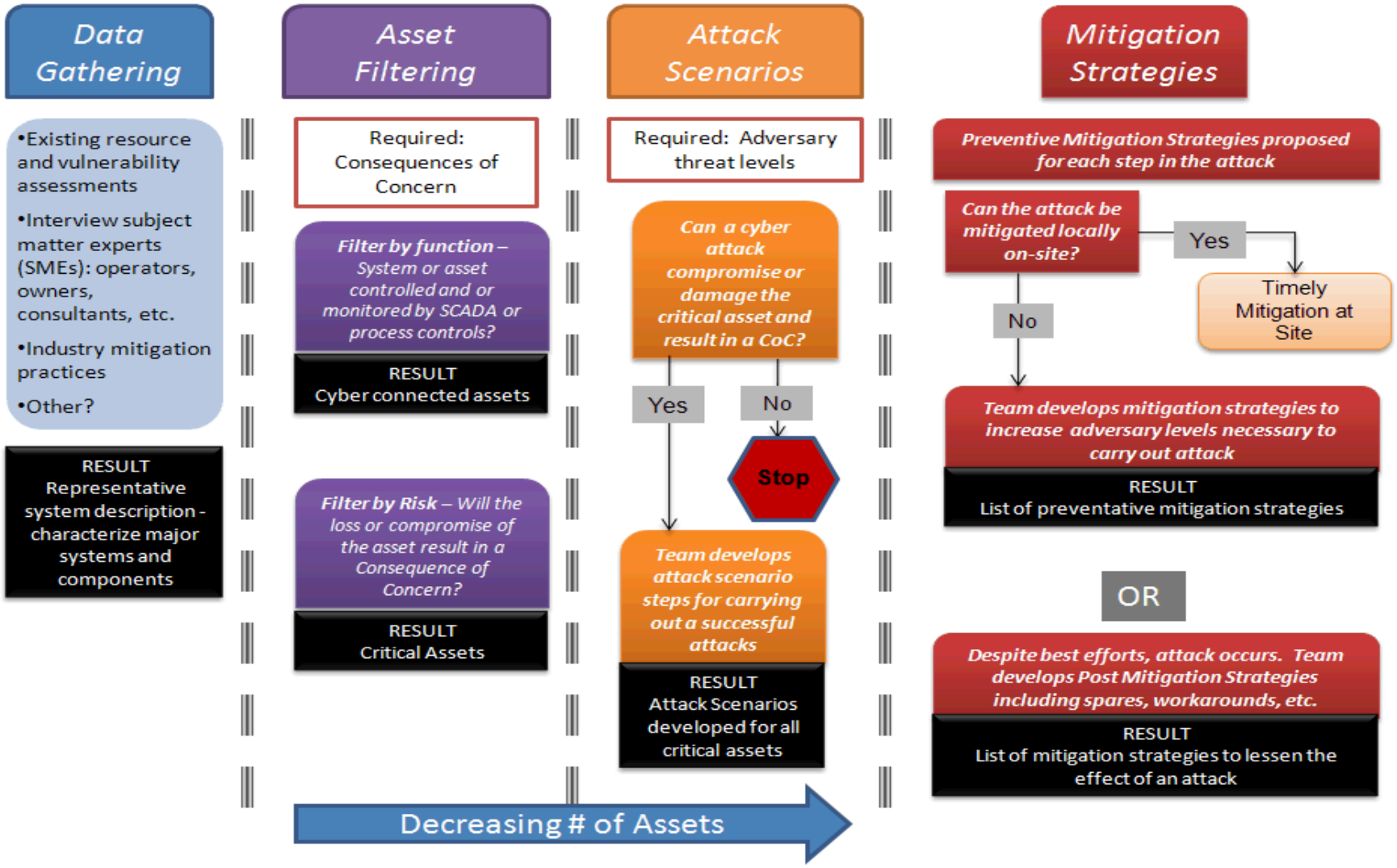
Approach and Pilot Studies

Approach:

1. Develop a methodology for use by **ALL sectors** (May 2010)
2. Conduct pilot studies to exercise the methodology (Now)
   - Engage multiple utilities per sector
   - Use lessons learned to enhance the methodology
3. Transition *proven* methodology to industry

This presentation reports the results for the first water sector utility assessment and includes "actionable" recommendations that are consistent with the higher-level water sector roadmap, based on the "spares" philosophy (what are the cyber-connected vulnerabilities that can result in Consequences of Concern), but specific to what is believed to be "common" opportunities for improvement for many small utilities in the entire sector.

Methodology



Sandia National Laboratories

Threat Levels

Threat Level	Threat Profile						
	Commitment			Resources			
	Intensity	Stealth	Time	Technical Personnel	Cyber	Kinetic	Access
IV	H	H	Yrs to Decades	Hundreds	H	H	H
III	M	H	Wks to Months	Tens	H	M	M
II	M	L	Months to Years	Ones	M	L	H
I	L	L	Days to Weeks	Ones	L	L	L

Adversary Level	Attributes
Threat Level I – "Garden Variety"	• Common hacker, script kiddies; joy hunting
Threat Level II – "Insider"	• High level of access and knowledge • Acts alone, difficult to detect • Target equipment and operations • Main interests in disrupting operations, causing public embarrassment
Threat Level III – "Mercenary'	• Higher level of skills • Organized crime • Targeting known vulnerabilities
Threat Level IV – "Nation State"	• Very sophisticated , well financed • Backed by foreign intelligence agencies • Difficult to detect • Focused on cyber for data exportation

The team defined these adversary levels, including commitment and resource definitions to help in building attack scenarios.

Source Material:

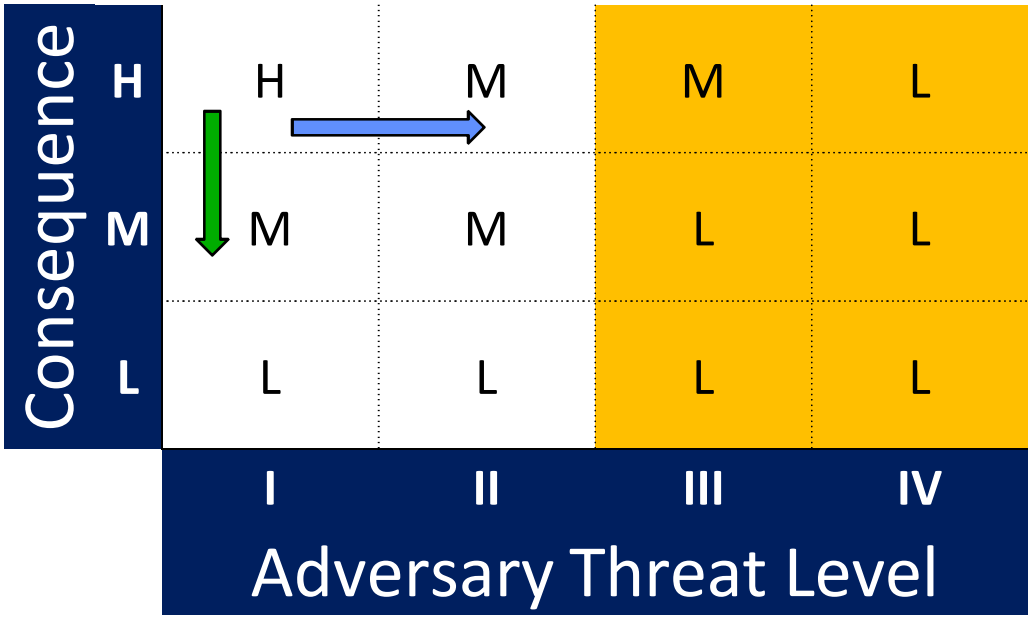
"Categorizing Threat: Building and Using a Generic Threat Matrix" (David P. Duggan, et al, SAND2007-5791, Sep 2007)

Sandia National Laboratories

Small Utility Consequences of Concern

1. Any fatalities or illnesses
2. Long-term impacts of 7 or more days for recovery
3. Economic loss to owner/operator or to the community of $3M
4. Public confidence/Utility reputation are negatively impacted
5. Cyber attacks that cause significant interruptions and can be easily replicated
6. Unauthorized shut-off notices generated through the Customer Service IT system

Risk Matrix



- Cyber security mitigations (e.g., implementing a firewall) increase the level of adversary necessary to execute an attack.

- Disaster recovery and other operations-focused mitigations may decrease the consequence of an event

•Although a more capable adversary can achieve a higher consequence attack, the risk is lower for a Level III/IV because the attack probability is lower.

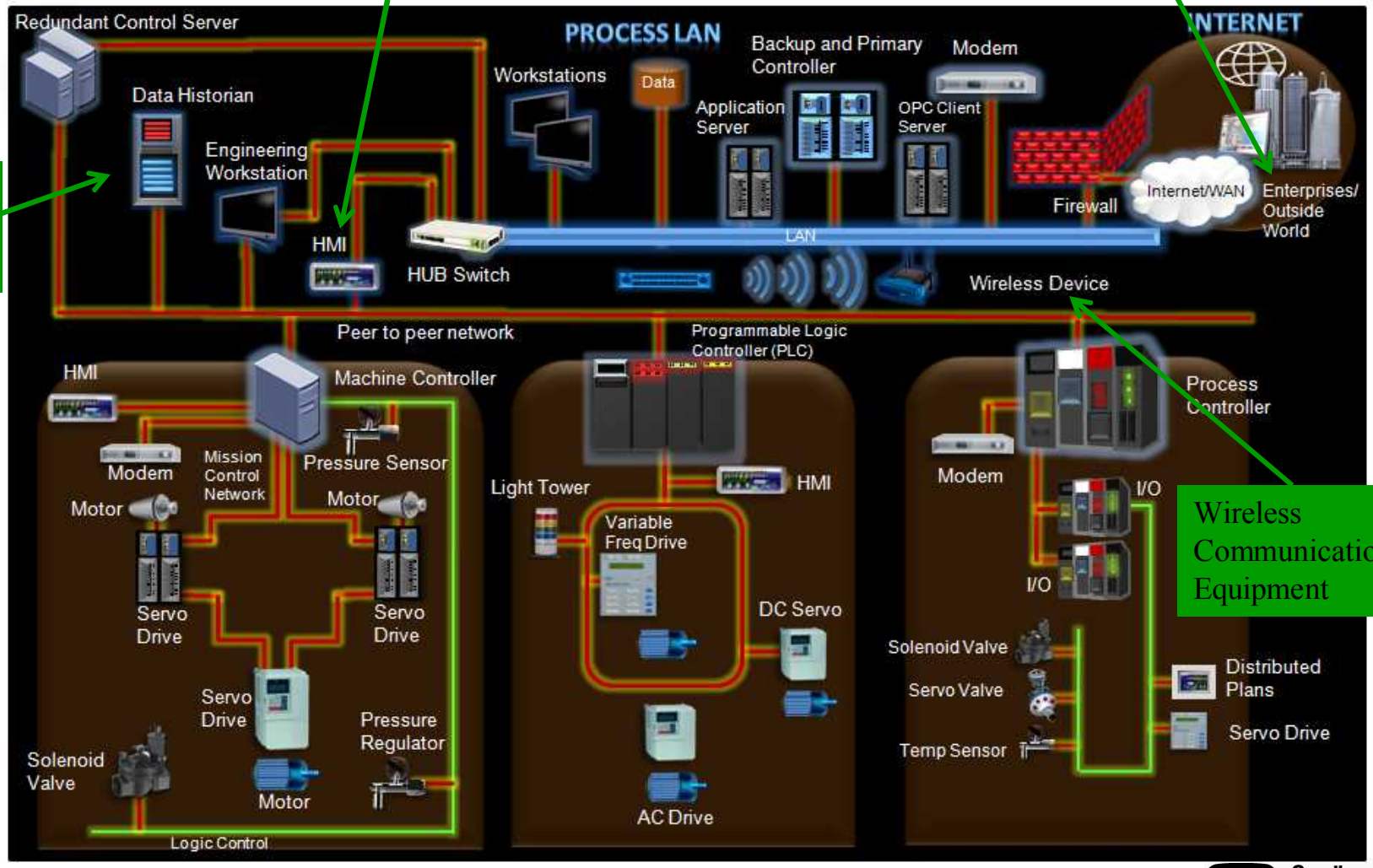
Sandia National Laboratories

Typical Cyber-Connected, Critical Components

SCADA Logic Controller

Enterprise Servers (Financial, Web, E-mail)

Data (SCADA Backups)



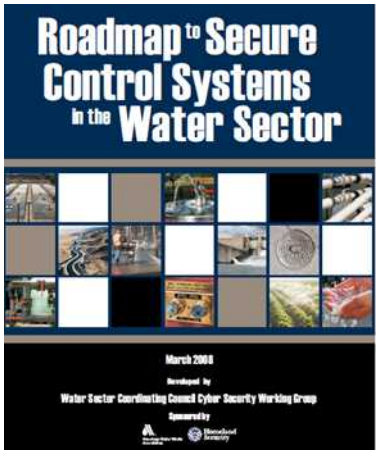
Wireless Communication Equipment

*** Represented on a notional SCADA network ***

Sandia National Laboratories

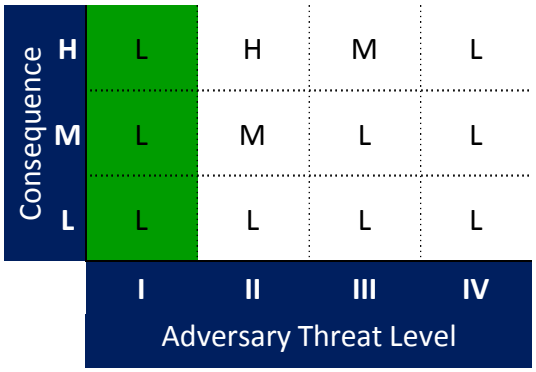
Small Utility Summary Recommendations

- Implement network segregation and improved access controls
  - ✓Corporate network from open internet
  - ✓SCADA network from enterprise
  - ✓Role-based security and concept of least privilege
- Improve physical security of critical cyber assets
- Plan for disaster recovery
  - ✓Develop policies and training for loss of SCADA, including manual operations
  - ✓Improve as-is documentation and backup procedures
  - ✓Maintain supported operating systems
- Implement encryption on wireless communications



✓ *Consistent with established AWWA and DHS guidance*

Collectively, these mitigations have the least effort/cost for implementation, represent common control system security practices and target the Level 1 Adversary. They set the stage for the next focus – a malicious insider adversary.



Small Utility High Risk Vulnerabilities and Mitigations

Sandia National Laboratories

Network Segregation

	Observation	Risk	Mitigation	Post-Mitigation Risk	Cost
Network Segregation	Accounting assets are not segregated from other (Internet-connected) assets, simplifying unauthorized access to the customer service system.	H	Logically or physically segment utility's current single network such that access to accounting assets can be more tightly controlled. Apply intrusion detection/prevention.	M	M
	Internet-facing utility assets (web server) are not strongly segregated from internal assets, simplifying unauthorized access to SCADA and accounting assets.	H	Logically or physically segment utility's current single network such that access to SCADA assets can be more tightly controlled. Apply intrusion detection/prevention.	M	M
	SCADA assets are not strongly segregated from other (Internet-connected) assets, simplifying unauthorized access.	H	Logically or physically segment utility's current single network such that access to SCADA assets can be more tightly controlled. Apply intrusion detection/prevention.	M	M

Disaster Recovery

	Observation	Risk	Mitigation	Post-Mitigation Risk	Cost
Disaster Recovery	RTU/PLC logic is not backed up within utility.	H	Backups of RTU/PLC firmware and configurations should be stored in a fire-resistant safe and be directly accessible by utility personnel. utility personnel should also be aware of how to restore RTU/PLC firmware and configuration settings.	M	M
	No SCADA master or recovery plan.	H	Develop policies and procedures to address continuity of operations assuming complete loss of SCADA assets/capabilities. Perform periodic utility-wide exercises assuming complete loss of SCADA assets/capabilities.	M	H
	Little instrumentation exists to allow for local control of facilities.	H	Develop manual operation training and provide facilities to allow for local control and situational awareness (such as level indicators on tanks).	M	H
	District staff have become reliant on the automatic operations of the water system.	H	Institute semi-annual training on manual operations and disaster recovery. Run the system semi-annually in manual for one shift followed by a de-brief that will refine manual operation policies and procedures.	M	L
	Poor physical security and environmental protection of servers, workstations, and local controllers.	H	Consider a dedicated control room that is physically protected and safe from environmental effects.	M	M
	Lack of common security awareness and training (ex. phishing attacks).	H	Require utility personnel to take annual training to familiarize them with IT security best practices. Assign at least one person at utility to become familiar with SCADA network infrastructure.	M	M
	Malicious attacks against closed-loop systems are possible.	H	Use local hardwire control for pump permissive to start/run.	M	L

Secure Practices

	Observation	Risk	Mitigation	Post-Mitigation Risk	Cost
Secure Practices	Common account and password used to access the utility network via VPN.	H	Limit the use of the VPN capability to only those users that need access to perform their assigned duties. Each VPN user should have their own account, and strong passwords should be required.	M	L
	Unencrypted and weakly encrypted wireless communications are in use	H	Require strong encryption (WPA-PSK or WPA2-PSK with AES algorithm) on all wireless links. Further, disable wireless access when it is not in use.	M	L
	HTTPS not used to protect ClearSCADA sessions. Sessions are also not protected using individual accounts or strong passwords.	H	Require SSL encryption (HTTPS) for ClearSCADA sessions. Require users to have individual accounts that are protected with strong passwords that are changed at least annually.	M	L
	Poor control of administrative accounts.	H	Implement role-based security and concept of least privilege.	M	M
	Discontinued/unsupported operating systems are in use.	H	Upgrade to operating systems that are actively supported by vendors. Hardware upgrades should be made as necessary to run modern operating systems.	M	M

Acknowledgements and Contact Information

- Special thanks to AWWA, Kevin Morley for his support and direction

Water Sector Leads

- Lon Dawson
ladawso@sandia.gov
(505) 844-5220
- Ray Finley
refinle@sandia.gov
(505) 844-4462

SNL Program Manager

-Robert Pollock
rdpollo@sandia.gov
(505) 844-4442

DHS Sponsor

- Amit Khosla
amit.khosla@dhs.gov
(703) 235-5886

Sandia National Laboratories