CH2M HILL’s Automation Group
Industrial Control System Cyber Security

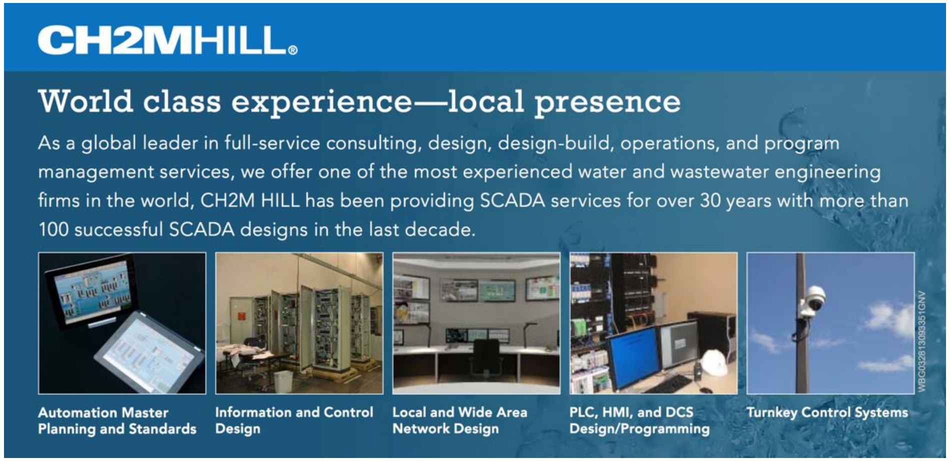
CH2MHILL

Michael Karl

2013

Agenda

- Why should I listen to this guy?
- Short History of Automation
- Cyber Security
  - Why do we need security
  - How to be an hacker
  - Case Study of Utilities Cyber Security



CH2MHILL

World class experience—local presence

As a global leader in full-service consulting, design, design-build, operations, and program management services, we offer one of the most experienced water and wastewater engineering firms in the world, CH2M HILL has been providing SCADA services for over 30 years with more than 100 successful SCADA designs in the last decade.

Automation Master Planning and Standards

Information and Control Design

Local and Wide Area Network Design

PLC, HMI, and DCS Design/Programming

Turnkey Control Systems

WBG032813093351GNV

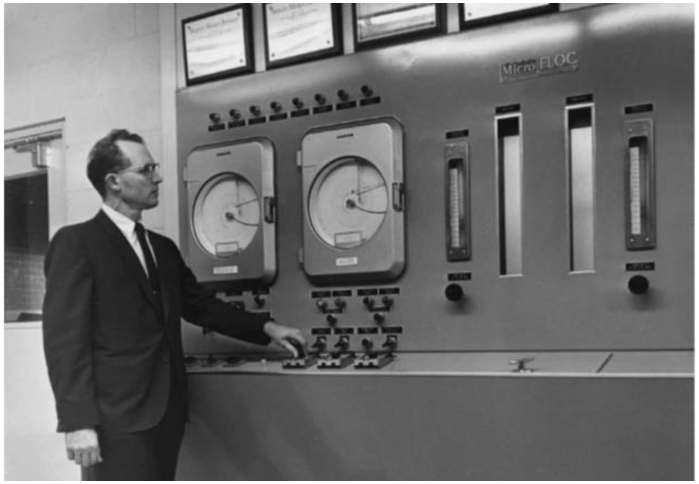
SCADA is Critical to the Mission

- **Reliable**
- **Meets standards**
- **Increase productivity**
- **Safe and Sustainable**

- **The mission:**
- To support the public health, safety and economic interests of the community by providing quality Water and Wastewater services in a responsible, efficient and sustainable manner.

State of the Industry

CH2M HILL's Automation Group In Younger Days



Automation in the'50's
(MicroFLOC)

*

DCS Pre-Windows '80s
(Bailey)

Demand for Cost Efficiency Inspired Innovative Solutions

SCADA/DCS

Local HMI

Remote Access (Dialup)

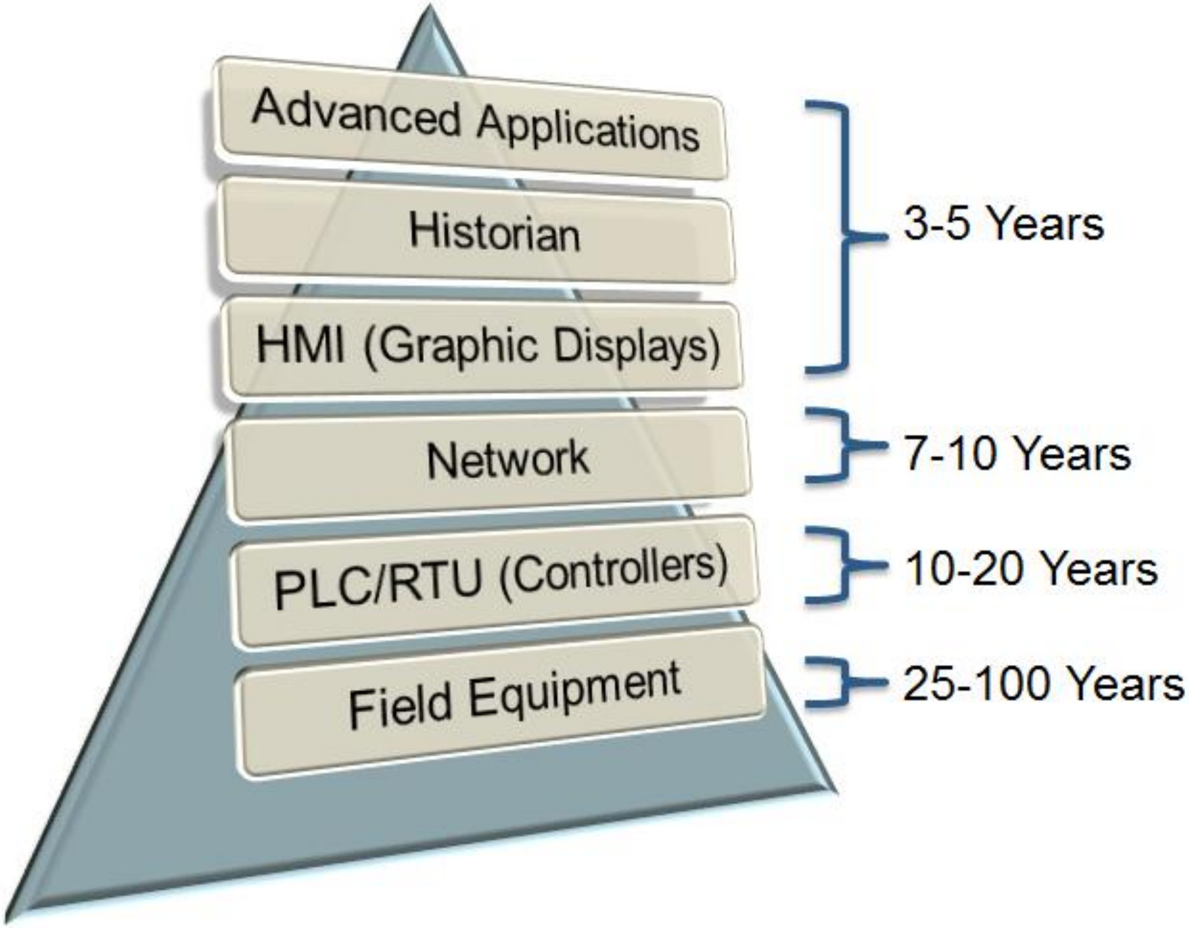
Note: *Image courtesy of Google Images

Regional Controls

SCADA/DCS

Tablets

Average Lifespan of Automation Equipment

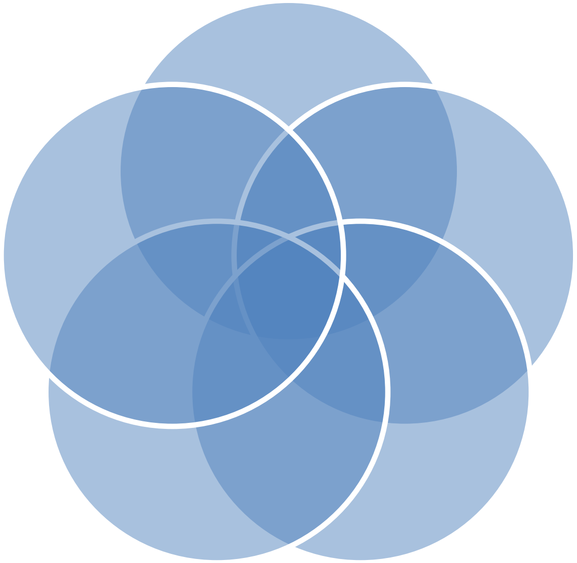


Industrial Control System Cyber Security

Acknowledgements

Infracritical SCADA
Security Newsgroup

CH2M HILL,
Automation Cyber-
Security Practice
Team



All the folks at
McAfee (thanks for
your help and
support)

The Department of
Homeland Security
CSSP

Invensys/Wonderware
Critical Infrastructure &
Security Practice Team

Our World is Changing

Q
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE.. BACK HERE
CYBER SECURITY

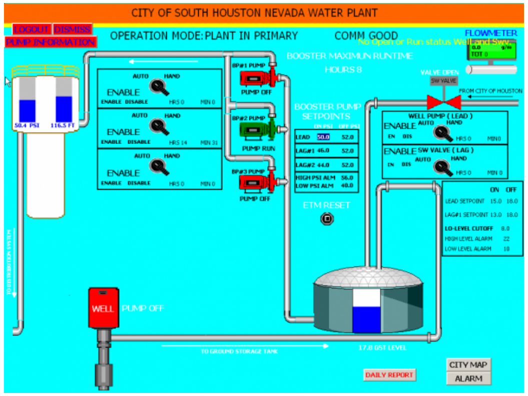
Cartoon credits: The Economist 2009

2013 Executive Order on Cyber Security

- Establishes a voluntary program to support the adoption of cybersecurity standards (called a "Cybersecurity Framework") by owners and operators of critical infrastructure.
- "Critical infrastructure" will be identified using a risk-based approach by the DHS.
- The Executive Order permits agencies to:
  - Add supplemental material as necessary to address risks that are specific to its sector;
  - Use existing statutory authority or identify **additional** authority to regulate the cybersecurity of critical infrastructure;

Media Coverage

- Stuxnet – Infected at least 22 manufacturing sites
- Pump destroyed at water plant Springfield, IL
  - Believed to be due to cyberattack (not confirmed by DHS).
  - Story covered by news media such as the Washington Post, Fox News, CNN, and MSNBC
  - Even though unconfirmed, the utility was in the national spotlight for weeks
- Texas SCADA system hacked and screenshots of HMI released
  - Response to DHS downplay of IL incident
  - Again carried by major news media
  - Used a virtual network connection with the internet with simple password to access network



CITY OF SOUTH HOUSTON NEVADA WATER PLANT

OPERATION MODE: PLANT IN PRIMARY   COMM GOOD

No Open or Run status Well and Swv.

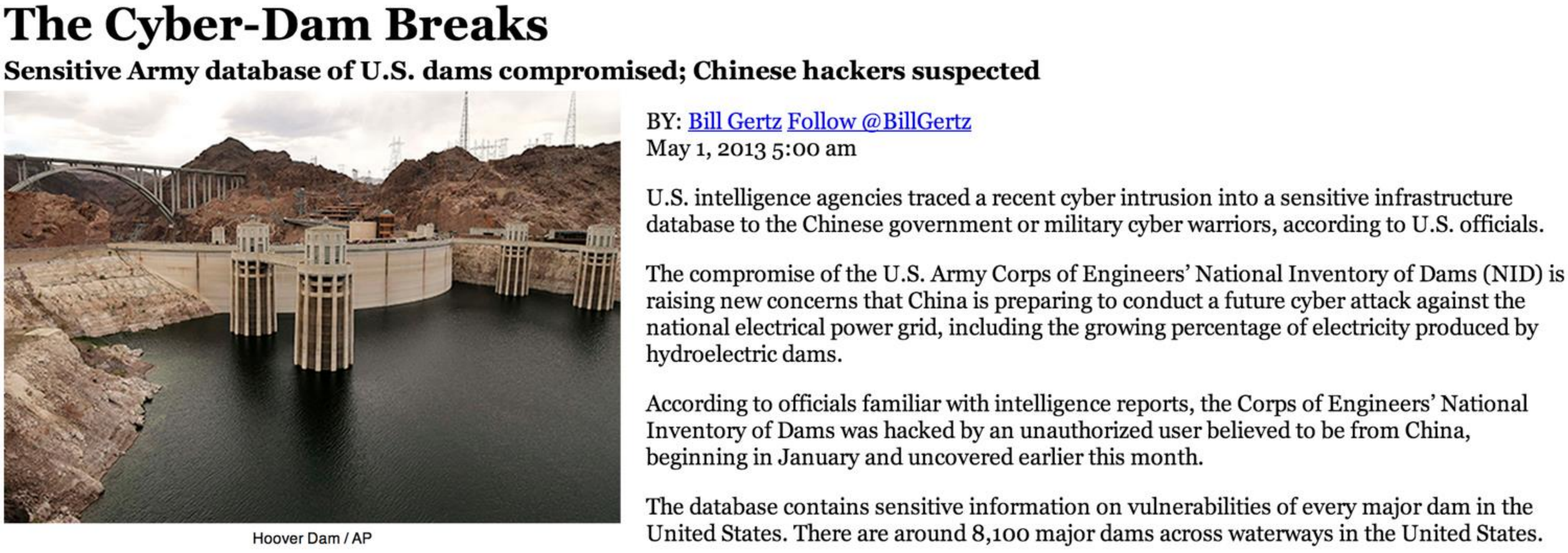
BOOSTER MAXIMUN RUNTIME HOURS 8

BOOSTER PUMP SETPOINTS

	ON PSI	OFF PSI
LEAD	50.0	52.0
LAG#1	46.0	52.0
LAG#2	44.0	52.0
HIGH PSI ALM	56.0	
LOW PSI ALM	40.0	

	ON	OFF
LEAD SETPOINT	15.0	18.0
LAG#1 SETPOINT	13.0	18.0
LO-LEVEL CUTOFF	8.0	
HIGH LEVEL ALARM	22	
LOW LEVEL ALARM	10	

Media Coverage Last 2 Months



The Cyber-Dam Breaks

Sensitive Army database of U.S. dams compromised; Chinese hackers suspected

Hoover Dam / AP

BY: Bill Gertz Follow @BillGertz
May 1, 2013 5:00 am

U.S. intelligence agencies traced a recent cyber intrusion into a sensitive infrastructure database to the Chinese government or military cyber warriors, according to U.S. officials.

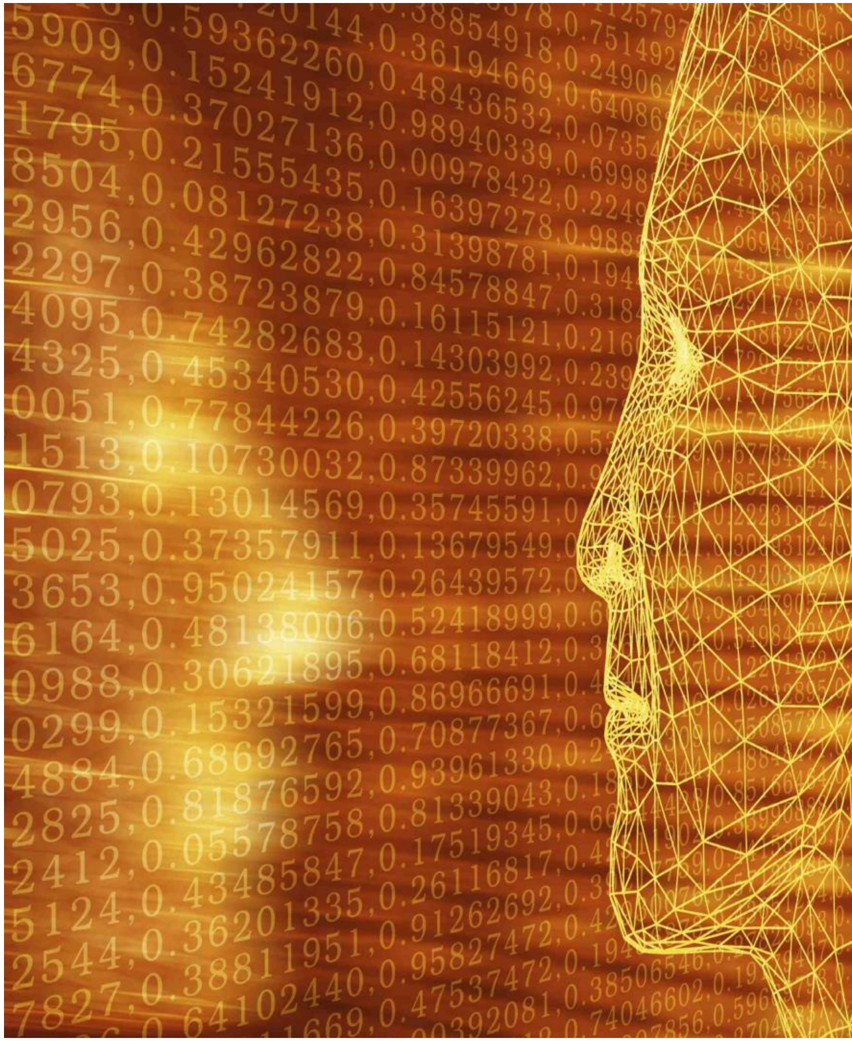
The compromise of the U.S. Army Corps of Engineers' National Inventory of Dams (NID) is raising new concerns that China is preparing to conduct a future cyber attack against the national electrical power grid, including the growing percentage of electricity produced by hydroelectric dams.

According to officials familiar with intelligence reports, the Corps of Engineers' National Inventory of Dams was hacked by an unauthorized user believed to be from China, beginning in January and uncovered earlier this month.

The database contains sensitive information on vulnerabilities of every major dam in the United States. There are around 8,100 major dams across waterways in the United States.

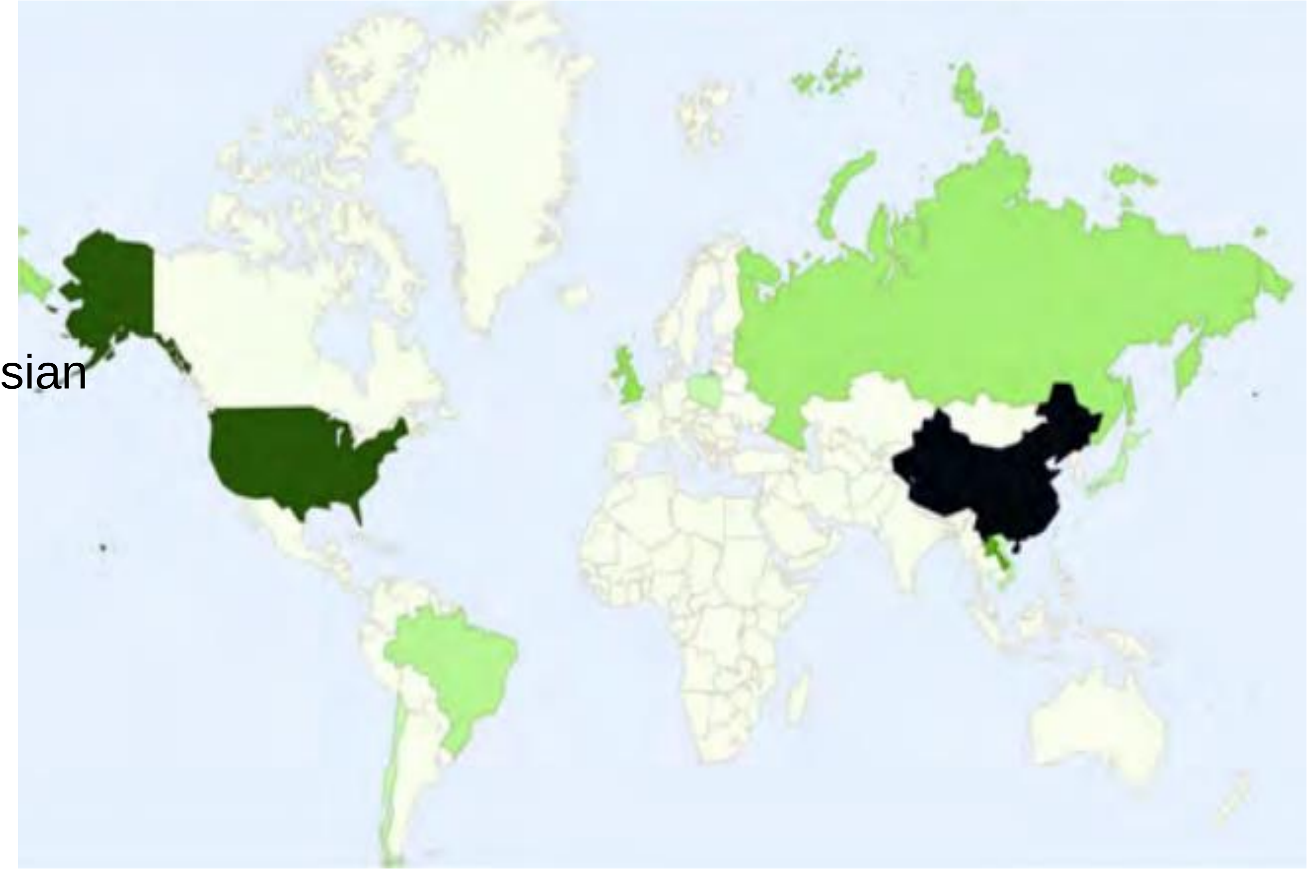
The Threat is Real!

- US Security Advisories
- 2010 (prior to stuxnet)
  - –5 security advisories
  - –3 vendors involved
- 2011
  - – 215 disclosed vulnerabilities
  - – 104 security advisories
  - – 39 vendors involved
- 2012
  - – 248 disclosed vulnerabilities



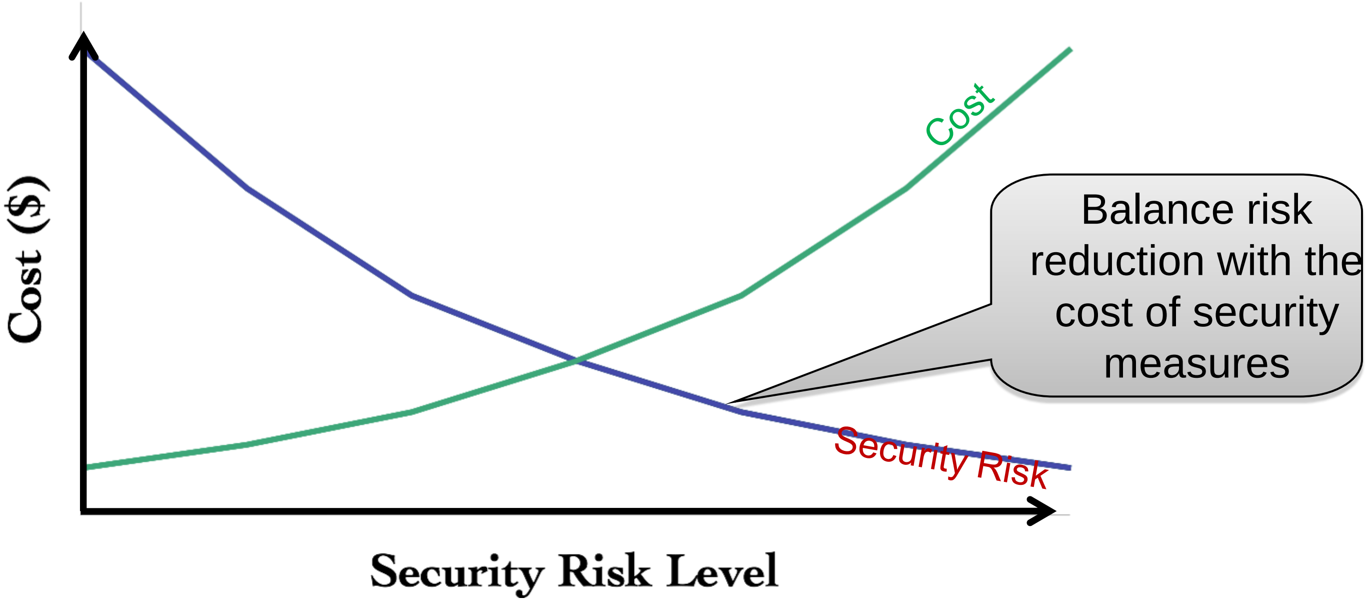
Attackers from the following countries

- 35% from China
- 19% from USA
- 12% from Southeast Asian Nation of Laos



We can Improve Security and Reliability!

- With proper tools your systems can be secure
- Reduce our exposure against the most likely and probable threats
- Security improvements will reduce operational risk



Balance risk reduction with the cost of security measures

How do I meet “Due Diligence”?

- Perform an evaluation
- Implement policies
- Implement tools
- Don’t forget physical securities
- Perform regular evaluations

Training is key

- Create a security culture
- Practice being secure
- Educate social engineering
- Ensure you have additional staff with operational knowledge of your systems
- Operational improvements will be recovered

Myths and Questions from the Industry

Myths

- "I'm secure, I'm not connected to the Internet." – Public Works Director
- "I'm secure, I have three passwords before I can connect" – Operations Manager
- "Using Passwords takes too long and I can't respond to emergencies"
- "Wastewater systems aren't in jeopardy" – Lead Maintenance Mgr.

Questions from Management

- What is the real risk to us?
- What is the golden solution?
- What needs to be protected?
- What do I need to do?

"Cyber security is like an arms race – there is no silver bullet"
Michael Assante – Chief Security Officer NERC

Common Vulnerabilities in the Industry

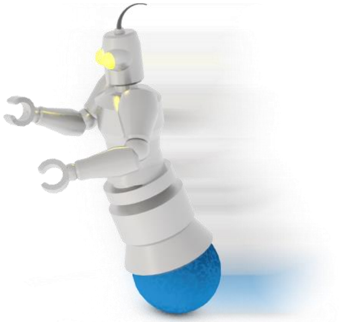
- Utilities serving >1,000,000 to 1,000 customers have the same challenges.

- Common Vulnerabilities:
  - Vendor dial-up access to PLCs directly
  - Routable public IP addresses
  - Many dual-homed computers
  - Unsecure wireless networks
  - Windows XP and Server 2000
  - Unpatched computers
  - Operators who are afraid of passwords

Case Study

Case Study - Typical SCADA Assessment

- SCADA System
  - Supported by Local Integrator
  - Part of the system is new, Others > 25 years old
  - Software/Hardware was typical common equipment from the NW
- Public Works Director Stated the following:
  - I want to perform due-diligence and have our system evaluated by a third party
  - I know our system isn't connected to the internet
  - I am not using Windows 7 yet so I'm a bit nervous
  - I like to understand our single points of failure



Additional Background Information

- SCADA covered a master site and remote facilities
- SCADA system had historian, HMI nodes and alarm notification software
- Local Ethernet network
- Local PLCs for control
- Radio network for telemetry communications
- Remote PLCs

Phased SCADA Security Implementation

- Phase 1
  - Review SCADA communication network
  - Evaluate the security of remote access
- Phase 2
  - Implement recommendations found in Phase 1
  - Perform training for utility staff
  - Develop policy and procedures for maintaining software and network
- Phase 3
  - Implement the NIST SP 800-82 guide for SCADA security

Approach to Phase 1

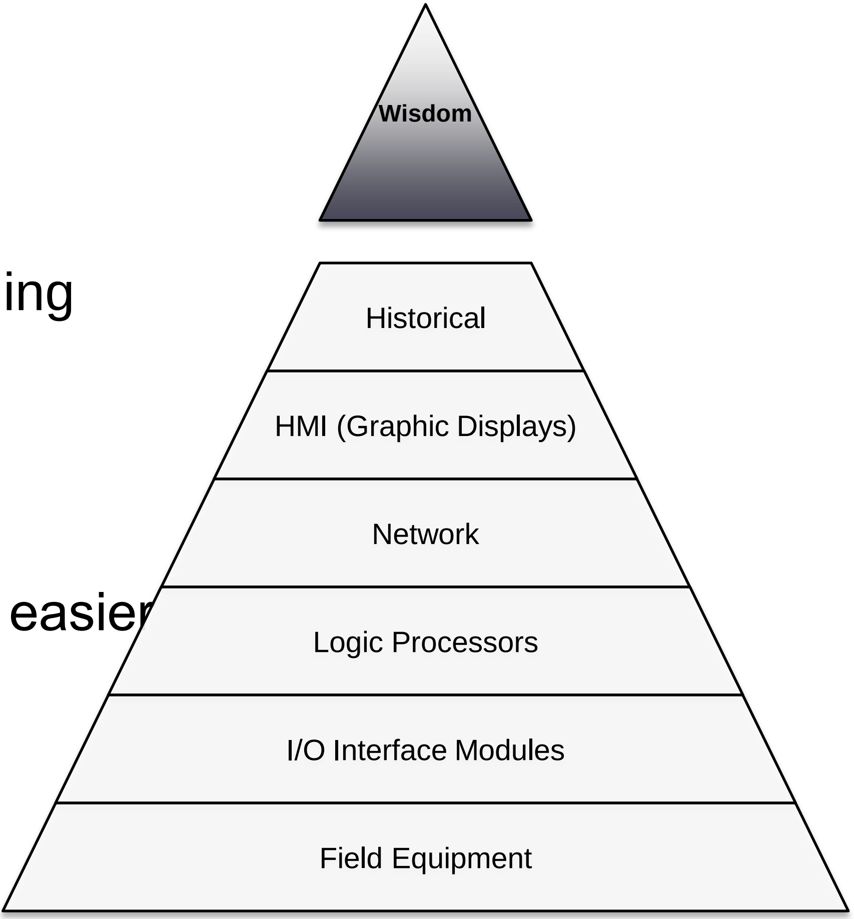
- Request for documentation
- Debriefs
  - Management
  - Systems Integrator
  - Operations staff
  - IT staff
- Perform on-site forensics

Findings of Phase One Assessment

- SCADA directly connected to internet in over 3 ways
- IT group didn’t understand the importance of SCADA
- Know vulnerabilities with
  - PLC Programming Software
  - HMI Software
  - Remote Access Software
- Radio network open to the world
- Surprises - No redundancy and not one backup

Summary - SCADA supports Your mission

- ICS/SCADA is critical
- Threats are dynamic and ever changing
- Security isn’t as simple
- New technology make operator’s life easier
- SCADA security is a necessity



Mike’s “DIKW”

Thank You!
Questions?

Michael.Karl@ch2m.com

425.749.2020

60 Minutes Video