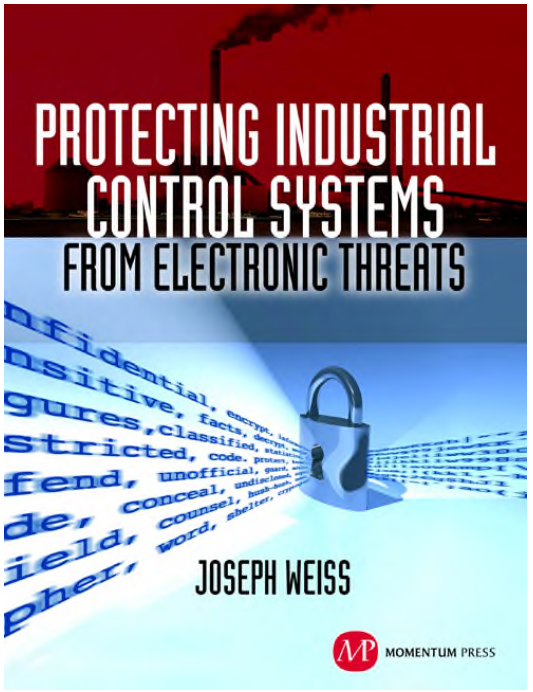
Cyber Security of Industrial Control Systems (ICSs)

February 23, 2016

Joe Weiss
PE, CISM, CRISC, ISA Fellow
Managing Partner
Applied Control Solutions, LLC
(408) 253-7934
joe.weiss@realtimeacs.com



ICSs – What Are They And Where Are They Used?

- ICSs are critical to operating industrial assets including power, refineries, pipelines, chemicals, manufacturing, water, military systems, medical systems, etc
- ICSs include Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Intelligent Electronic Devices (IEDs)
- ICSs monitor and control physical processes in real time

Focus is reliability and safety

Definitions That Can Be Confusing

- Cyber
- Security
- Hack
- Cyber Incident
- Risk
- SCADA
- IT
- Insider
- Malicious

What Has Happened Recently

- ICS honeypot projects
  - Documenting nation-state attempted attacks against ICS
- Continuing ICS cyber vulnerabilities and incidents
  - BlackEnergy, Havex (in US critical infrastructures)
  - Cyber attacks against Ukrainian power, rail, mining
  - German train crash
  - Navy ship failure
  - VW emissions test cheating device
- Hackers paying attention to ICS
  - Hacker conferences with ICS hacking
  - Building out home ICS lab
  - Video game training hackers on critical infrastructures – WatchDog
- Movie on US readiness to target multiple Iranian infrastructures
- Insurance and Wall Street have mounting awareness of ICS risks

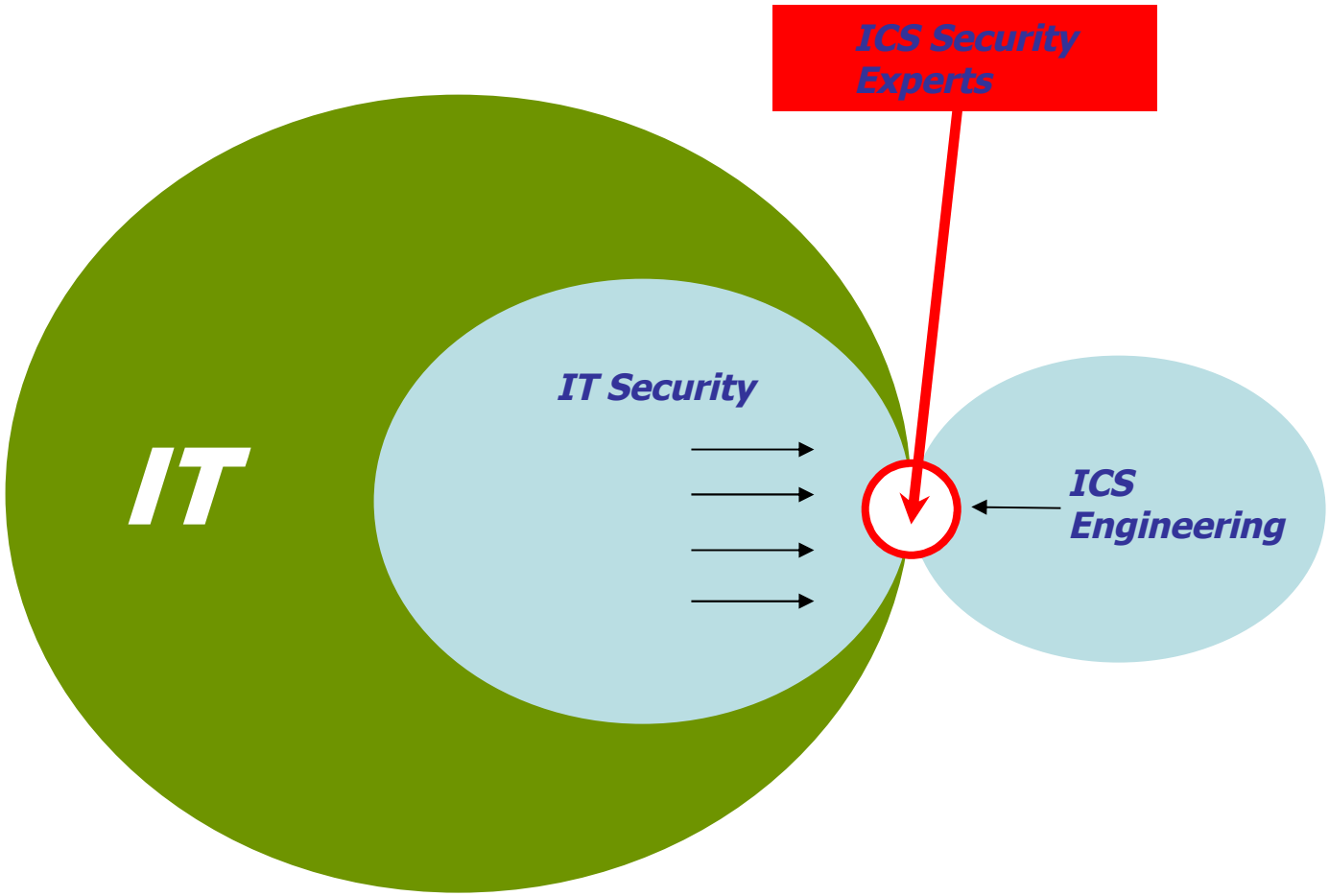
Russian Cyber-Attack on The Ukrainian Grid

(per George Cotter, Formerly Chief Scientist NSA, Member NAE)

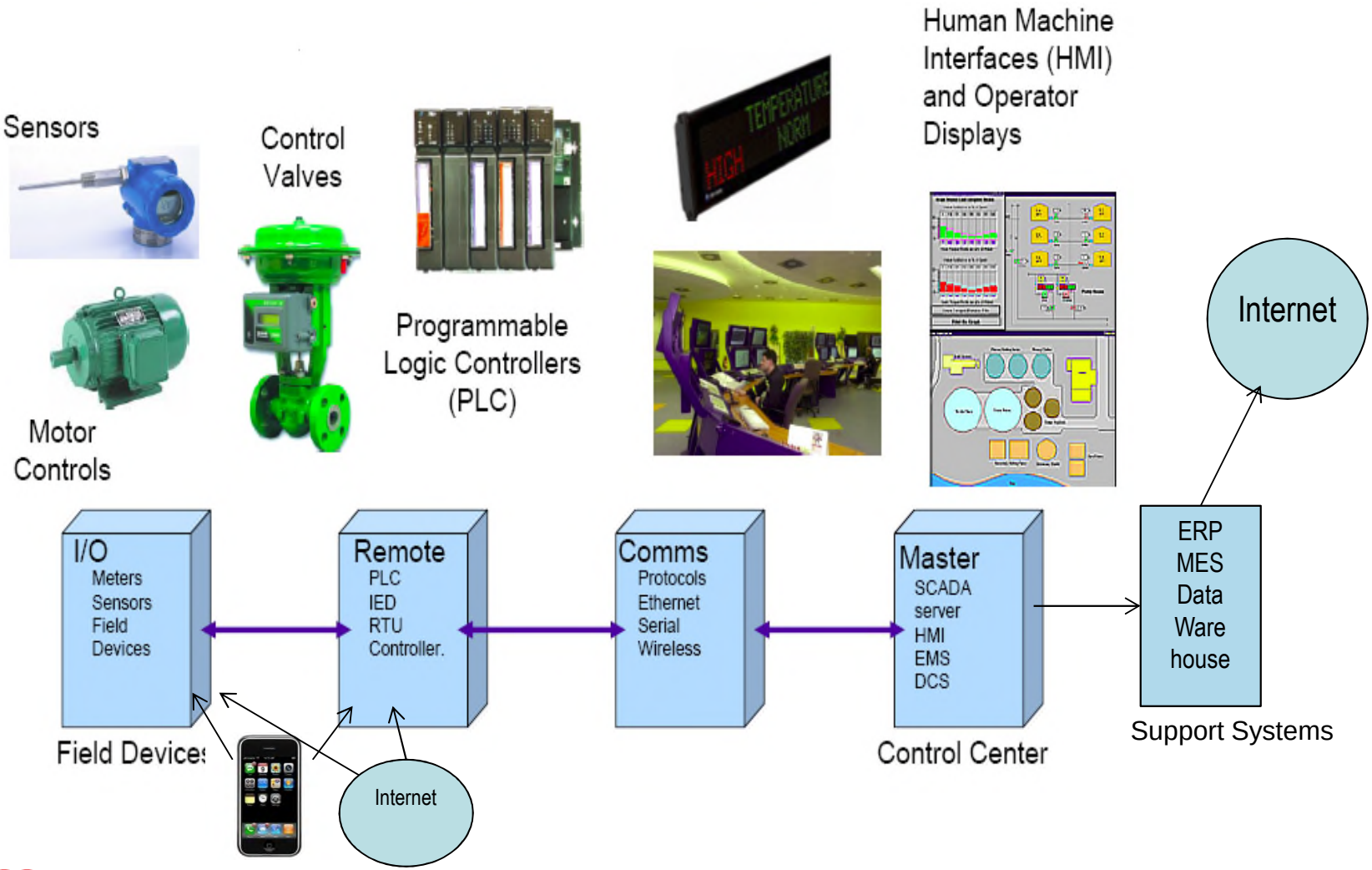
- December 23rd-Sophisticated Attack in 2 Regions, Probably 6 Others
  - Intruded into SCADA Systems, Damaged SCADA System Hosts and Workstations
  - Seized Control at Human Machine Interface (HMI) Level, Blindsided System Dispatchers
  - Opened Circuit Breakers, Cut Power to 225,000 customers, HMI was Undoubtedly Compromised (Precursor to Aurora?)
  - Initiated DDOS Attack on Call Centers to Prevent Users from Reporting Outages
  - Activated KillDisk, Erasing Presence, Denying Forensics
  - Multiple Attack Vectors But Much More to be Learned
- Earlier Intrusions March-July 2015 Evidence of Planning, Penetration
- Sandworm Team, BlackEnergy 2, 3 Techniques Are of Russian Origin
- Directly Related to 2014 BlackEnergy Supply Chain Intrusions in U.S.
- And Yet ES-ISAC Stated:

"There is no credible evidence that the incident could affect North American grid operations and no plans to modify existing regulations or guidance based on this incident."

ICS Security Expertise Lacking



Control Systems Basics



IT vs ICS Cyber Security

Attribute	IT	ICS
Confidentiality (Privacy)	High	Low
Message Integrity	Low-Medium	Very High
System Availability	Low-Medium	Very High
Authentication	Medium-High	High
Non-Repudiation	High	Low-Medium
Safety	Low	Very High
Time Criticality	Delays Tolerated	Critical
System Downtime	Tolerated	Not Acceptable
Security Skills/Awareness	Usually Good	Usually Poor
System Lifecycle	3-5 Years	15-25 Years
Interoperability	Not Critical	Critical
Computing Resources	“Unlimited”	Very Limited
Standards	ISO27000	ISA/IEC 62443

What Are ICS-Unique Cyber Threats?

- Cyber-physical, Not just the network
- Persistent Design Vulnerabilities, Not just Advanced Persistent Threats
- Want undetected control of the process, not denial-of-service

Gap in protection of the process (Level 0)

  - eg, Aurora

Compromise of the measurement (Level 1)

  - eg, HART vulnerability

Compromise design features of the controller (Level 2)

  - eg, Stuxnet

DHS Guidance on ICS Internet Access

- ICS-CERT Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure
  - Original release date: February 25, 2016
- Organizations should isolate ICS networks from any untrusted networks, *especially* the Internet
  - Currently, >2,000,000 ICS systems and devices are directly connected to the Internet
  - What does the DHS guidance mean to the Internet of Things, Smart Grid, and other similar approaches?
  - What will the DHS guidance mean to insurance companies?

What Is an ICS Cyber Incident?

- Electronic communications between systems and/or people that impacts Confidentiality, Integrity, and/or Availability (CIA)
  - Missing safety
- Incidents that are apparently non-malicious can actually be malicious

ICS Cyber Incidents Are Real

- Impacts ranged from significant discharges to significant equipment damage to deaths
- Affects all industries
- Very few ICS-specific cyber security technologies, training, and policies
- >2 million ICS devices directly connected to the Internet (and counting)
- Resilience and recovery need to be addressed









BlackEnergy Hack Is Widespread

(per Kyle Wilhoit, TrendMicro)

- "Based on telemetry data from open-source intelligence (OSINT) and Trend Micro Smart Protection Network, we saw that there were samples of BlackEnergy and KillDisk that may have been used against a large Ukrainian mining company and a large Ukrainian rail company (same samples as against the utilities)"
  - Cyber threats cross industry verticals

Cyber Security Issues With The US Grid

- More than 250 ICS cyber incidents in North America
  - 5 major outages (more than 90,000 customers each)
- Industry is focused on compliance, not security
- NERC cyber standards (CIP) are inadequate
  - Wouldn't have addressed the 5 major outages
  - Excludes most of the electric industry assets
    - Ukrainian substations would have been out-of-scope
    - Most power plants and many substations out-of-scope
    - Routable connections being replaced to avoid compliance requirements
  - Doesn't address communication between control centers and substations
  - Doesn't address ICS issues like Stuxnet and Aurora
  - Doesn't address ICS supply chain issues
  - Doesn't require malware to be removed!
  - DOD issued $70M RFP on cyber security of the electric grid

Aurora Vulnerability

Programmable Digital Relay

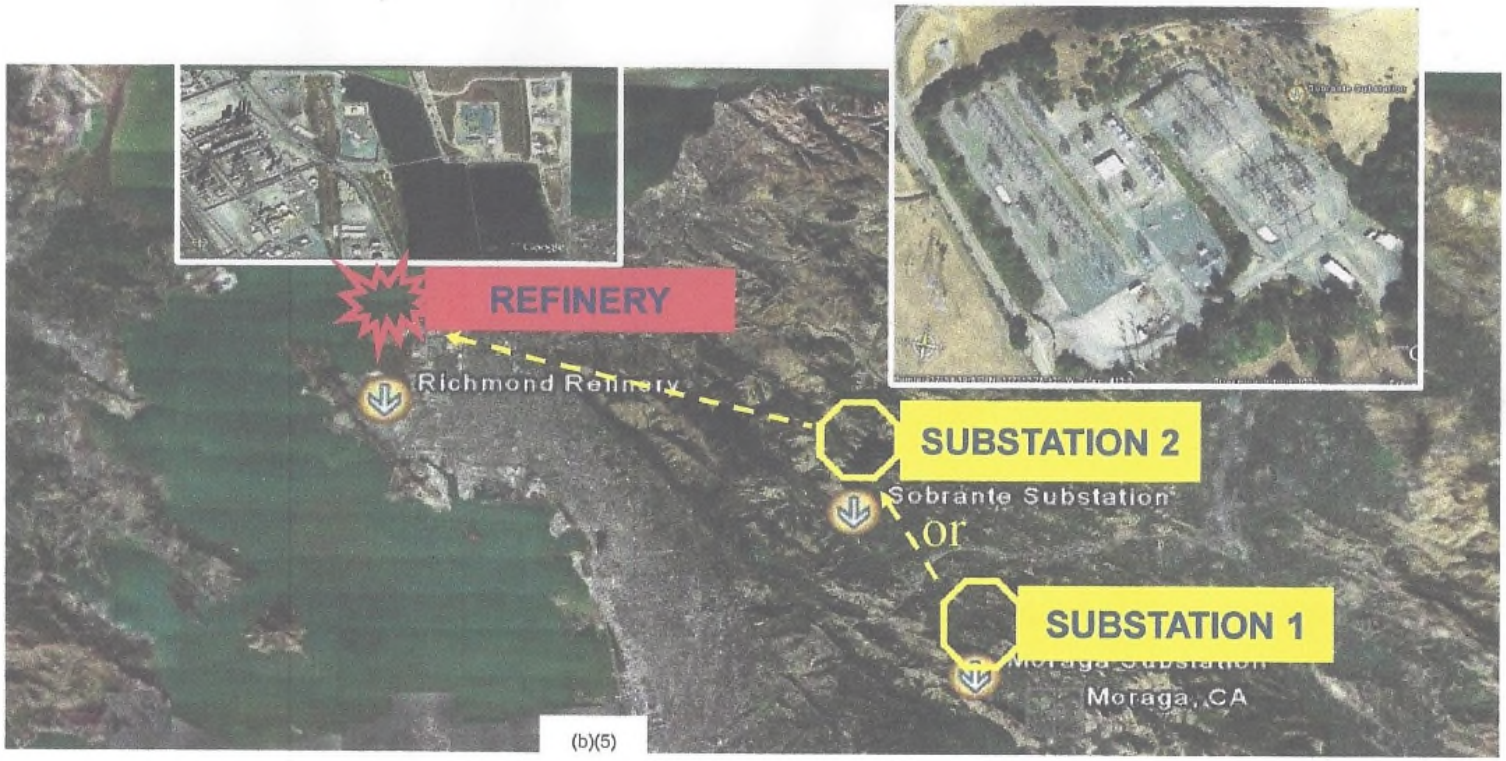
- The Elements Necessary for an Attack
  - Programmable Digital Relay
    - Or other device that controls the breaker
  - High-Speed Breakers
  - Access (front panel, modem, Internet, wireless, or SCADA)
  - Laptop/Desktop Computer
- Knowledge Necessary:
  - Power Engineering (attack planning and device setting skills)
  - Hacking Skills (exploit the relay and conduct the attack)
- Time Required to Conduct the Attack (after gaining access):
  - Less than one minute
  - No additional software is introduced
  - Uses the internal settings of the imbedded relay software

Homeland Security

~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~

8

Aurora Vulnerability



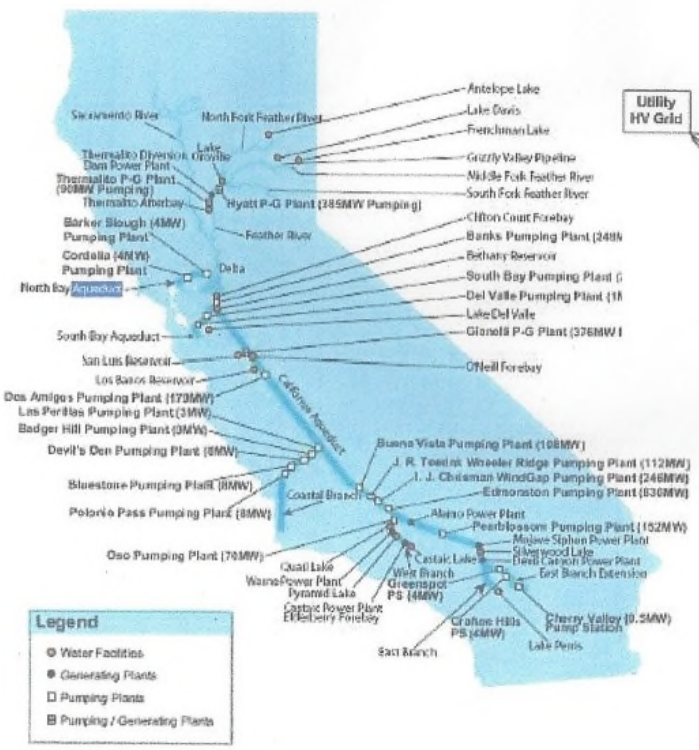
Homeland Security

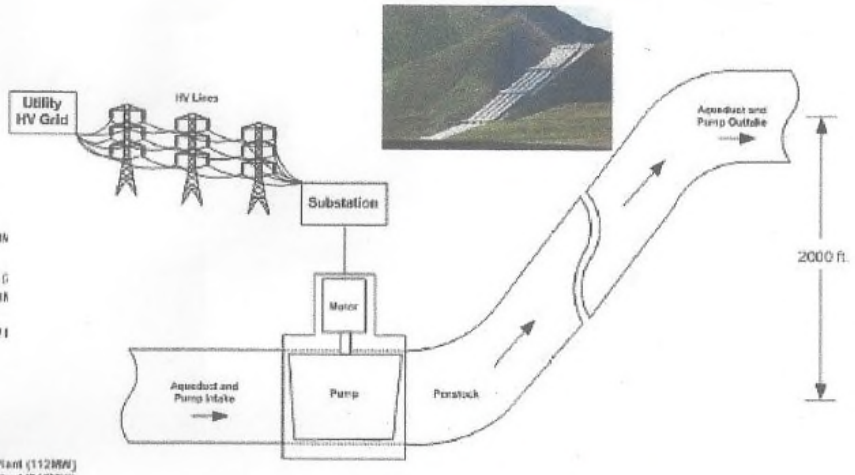
UNCLASSIFIED/FOR OFFICIAL USE ONLY

7

Aurora Vulnerability Example

Water Pumping Plants Use Large Motors in Series





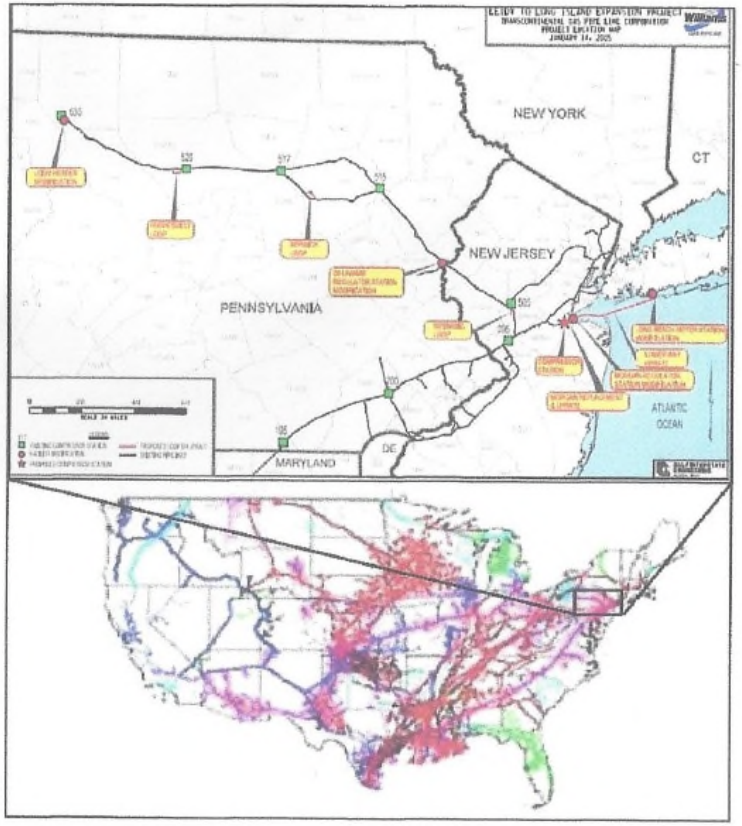
Homeland Security

~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~

9

Aurora Vulnerability Example

Gas Line Compressor Stations Use Large AC Induction Motors Near Cities



Homeland Security

UNCLASSIFIED/FOR OFFICIAL USE ONLY

10

Summary of ICS Cyber Incidents to Date

	Estimated Count
Total	750
Malicious	250
Targeted	100 (of the 250+)
Loss of View/Loss of Control	300
Injury/Deaths	60 (>1,000 deaths)
Equipment Damage	100
Environmental Damage	70
Operational Impact	500
Financial Impact	$30B

Societal Needs and Concerns

- Government has cyber security expertise
  - Industry often doesn't trust the government
  - Need to have "get out-of-jail free" card and anonymize end-users
  - Academia needs solutions that are practical
- Industry has domain expertise
- Industry & Insurance Partners could accelerate "best practices"
  - Lloyd's Study projects losses from US cyber-caused 15 state blackout of $243B to $1 Trillion (July 2015 Report)
- Academia researches "1st-principles"
- Work with "coalition of the willing"
  - Develop appropriate ICS cyber technologies
  - Share information

What Can Be Done Today

- Understand ICS cyber security
- Establish a cross-discipline team reporting to the C-Level
  - Operations/ICS should lead
    - Operations, Maintenance, Engineering, IT, Telecom, Forensics, Risk, PR
- Develop a “living” ICS cyber security program
  - Develop ICS cyber security policies and metrics
  - Understand what is actually installed and connected
  - Perform risk assessment based on mission criticality
- Implement security technologies to meet functional needs
- Incorporate security into ICS procurement specifications

How Can You Help?

- Support cyber security in your own organization
  - Make ICS cyber security as important as IT cyber security
- Participate in industry/government efforts
  - Standards development, government advisory panels
- Share information with others
  - Incidents, solutions, threats, needs

Thank you

Joe Weiss
Applied Control Solutions, LLC
(408) 253-7934
joe.weiss@realtimeacs.com