

**RSA**®Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: HT-W02

# Protecting Critical Infrastructure is Critical

**Robert M. Hinden**

Check Point Fellow



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.



**CHANGE**

Challenge today's security thinking

#RSAC

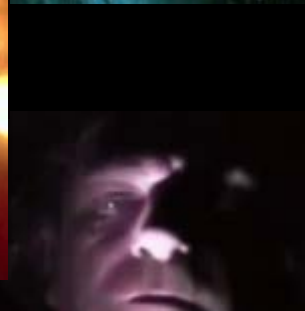
# American Blackout


NATIONAL GEOGRAPHIC CHANNEL  

AMERICAN BLACKOUT



AMERICAN  
BLACKOUT



AMERICAN BLACKOUT TRAILER  66

Learn what it means to be powerless. NatGeo presents a world premiere movie event, Sunday October 27th at 9/8C.

[National Geographic - American Blackout \(trailer\)](http://www.youtube.com/watch?v=FYoXxVnTePA)

Full Video at: <http://www.youtube.com/watch?v=FYoXxVnTePA>

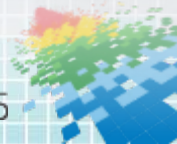


**Check Point**  
SOFTWARE TECHNOLOGIES LTD.



# Critical Infrastructure is at Risk!

- Critical Infrastructure is part of our world
- Many Vulnerabilities
  - Just like other IT systems, but
- The consequences of an attack are much greater
  - Power failures
  - Water pollution or floods
  - Disruption of transportation systems
  - Deaths of people on life support systems



# Talk Overview

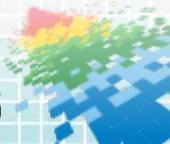
Why this issue is Critical

Real Attacks

SCADA Industrial Control Protocol

Security Issues with Control Systems Platforms

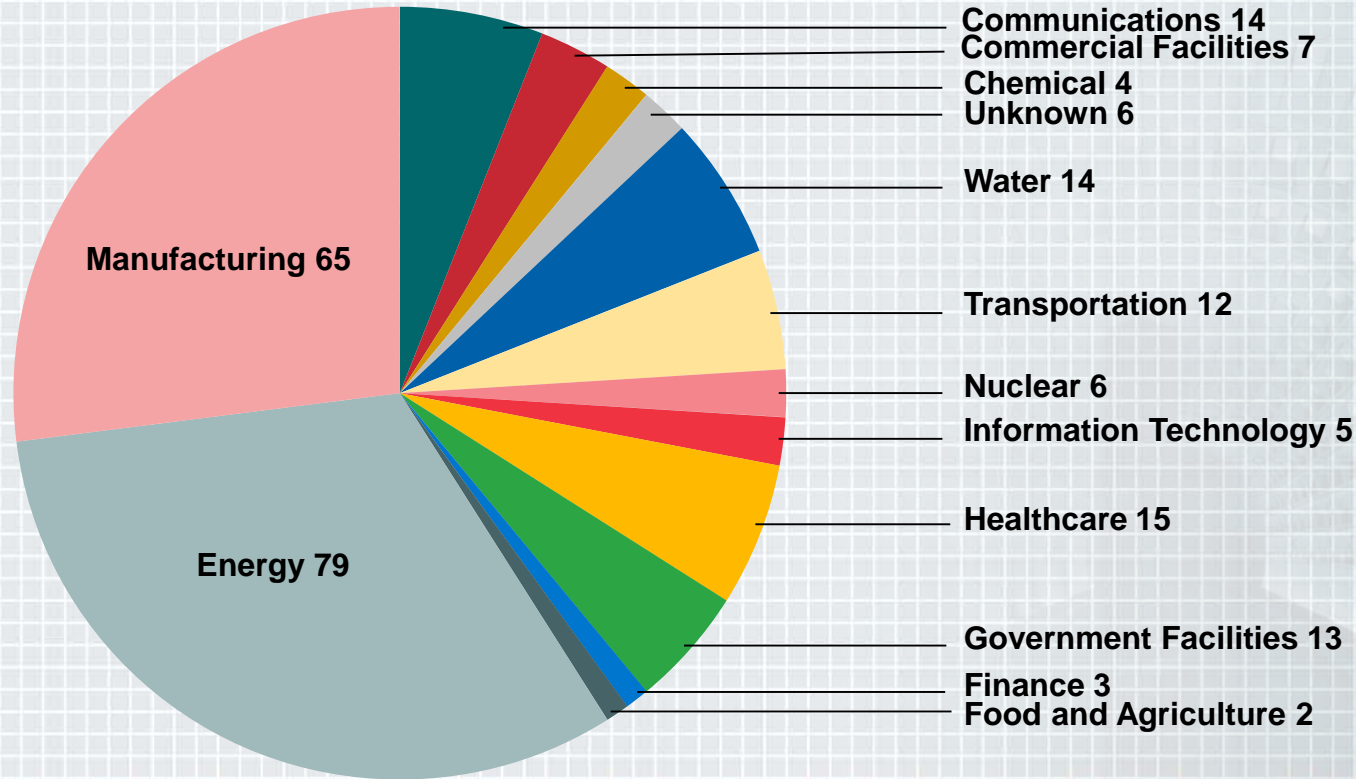
Recommendations and Actions



# Industrial Control Systems are Everywhere



# Critical Infrastructure is Targeted



# Incidents by Type

Brute Force Intrusion

Weak Authentication

Spear Phishing

**Unknown**

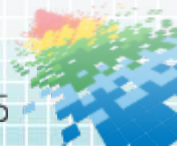
SQL Injection  
Removable Media

Network Scanning/Probing

Miscellaneous

Abuse of Access Authority

[https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT\\_Monitor\\_Sep2014-Feb2015.pdf](https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf)



# RSAC<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Attacks are Happening

 #RSAC





# BlackEnergy Malware Compromised Industrial Control Systems

- Attack has been ongoing since 2011 via Operator console via Internet Connections
- Targets GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC
- Affects Microsoft Windows and Windows Server 2008 and 2012
- Various attacks point to shared command and control systems

<https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>



# Cyber Attack on German Steel Factory

- German Federal Office for Information Security reported
  - Hackers accessed production network, and tampered with Blast Furnace controls
- Hackers gained access via spear phishing and social engineering to get credentials to access office network
- Blast furnace could not be shut down, resulting in “massive damage to plant”



<http://www.wired.com/2015/01/german-steel-mill-hack-destruction/>

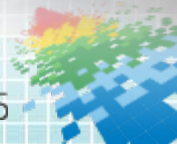


# Malware in South Korean Nuclear Plant

- Malware found in computers connected to nuclear power facility
- Reactor controls of Korea Hydro and Nuclear Power (KHNP) were not connected to any external networks
- Malware likely introduced via USB drive

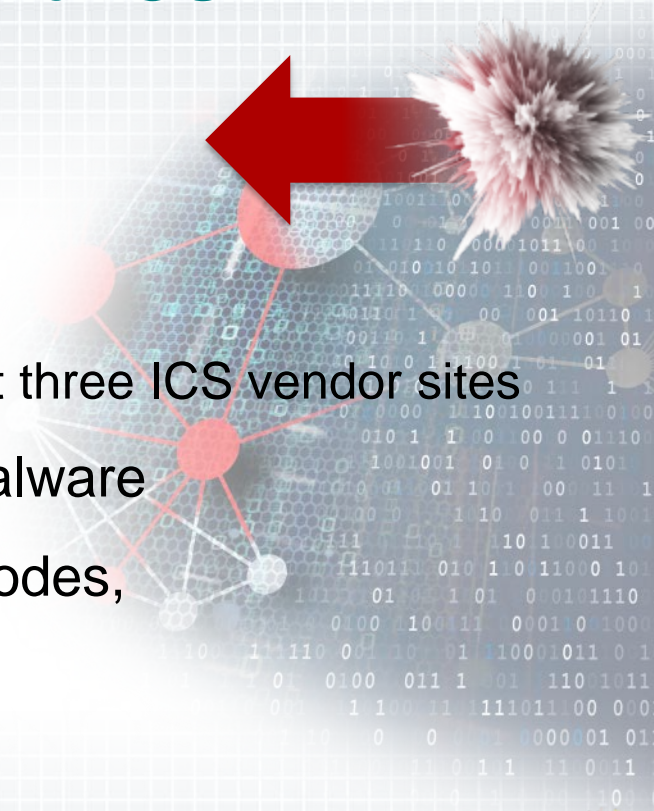


[http://www.huffingtonpost.com/2014/12/22/south-korea-nuclear-plant-operator-computers-hacked\\_n\\_6364500.html](http://www.huffingtonpost.com/2014/12/22/south-korea-nuclear-plant-operator-computers-hacked_n_6364500.html)



# Multiple-Vector Attack on Industrial CS

- Attack used multiple attack vectors
  - Phishing emails
  - Redirects to compromised sites
  - Installed infected update installers on at least three ICS vendor sites
- Installers were infected with Havex Trojan malware
- Malware collected information on topology, nodes, control systems
  - Caused some systems to intermittently crash



# Observation

- Many of the recent attacks were collecting data about Critical Infrastructure deployments
  - Devices, topology, protocols, etc.
- What does this mean?

**Attackers are collecting data  
to enable future attacks**



# Critical Infrastructure Constraints

- Critical Infrastructure use dedicated systems, on specialized networks, with unique protocols
- Deployments can't be changed easily
- Solutions need to last for 10, 20, or 30 years

**Attackers are moving very fast and don't have these constraints**



# RSAC<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Supervisory Control and Data Acquisition Protocol (SCADA)

 #RSAC



# SCADA Overview

- Protocol to monitor and control remote equipment. Used for
  - Pipelines, civil defense systems, heating/cooling systems, etc.
- Main components
  - Remote terminal units (RTU) – Connect to sensors and convert to digital data
  - Programmable Logic Controllers (PLC) – Like RTU, but are programmable
  - Human-Machine Interface (HMI) – Presents data to human operator
  - Network – LAN, WAN, Cellular, satellite, etc.

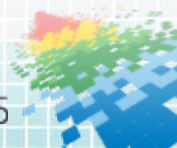




# Why Attacks Can Happen?

- SCADA devices and protocol were not designed for security
  - Security by obscurity?
- Assumed to be isolated from organizations network and Internet
- Assumed shared trust

**None of these assumptions are true!**



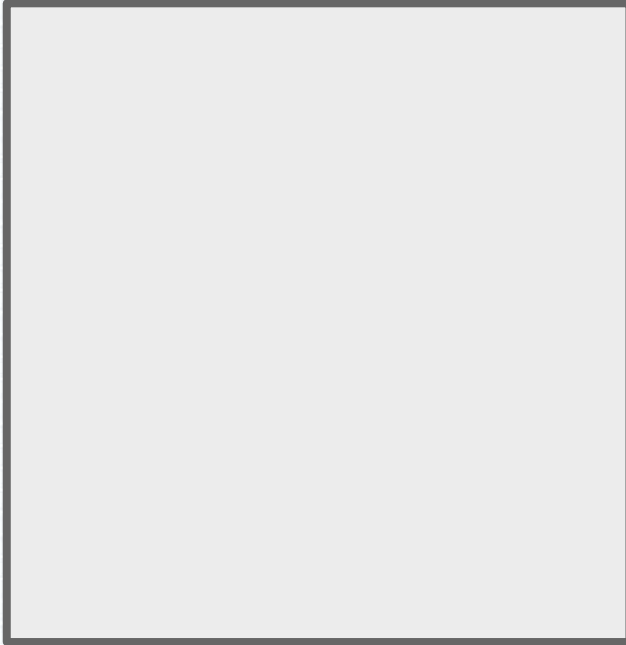
# SCADA Devices are Vulnerable

- Programmable Logic Controllers (PLC) are purpose-built computers used for automation of electromechanical processes such as control of pumps, valves, pistons, motors, etc.
- PLCs are small computers. They have software applications, accounts and logins, communication protocols, etc.
- Analysis of PLCs from leading vendors shows variety of vulnerabilities:
  - Backdoors
  - Lack of authentication and encryption
  - Weak password storage
  - Bugs leading to buffer overruns

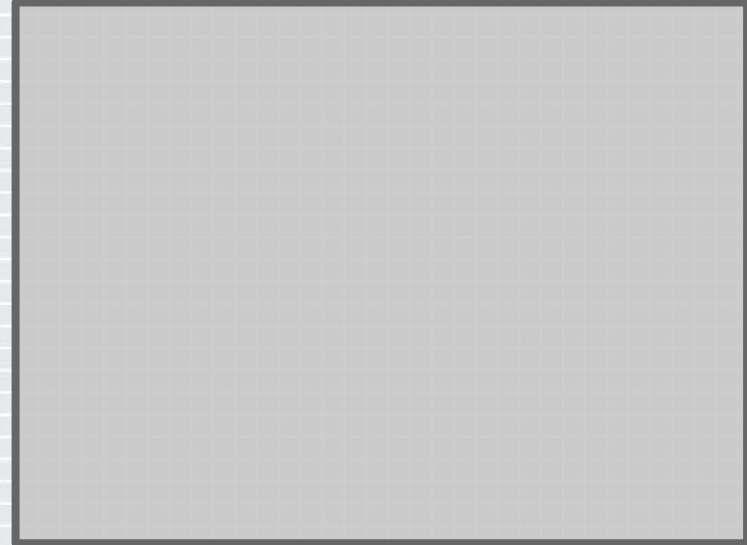


# Typical SCADA Network Structure

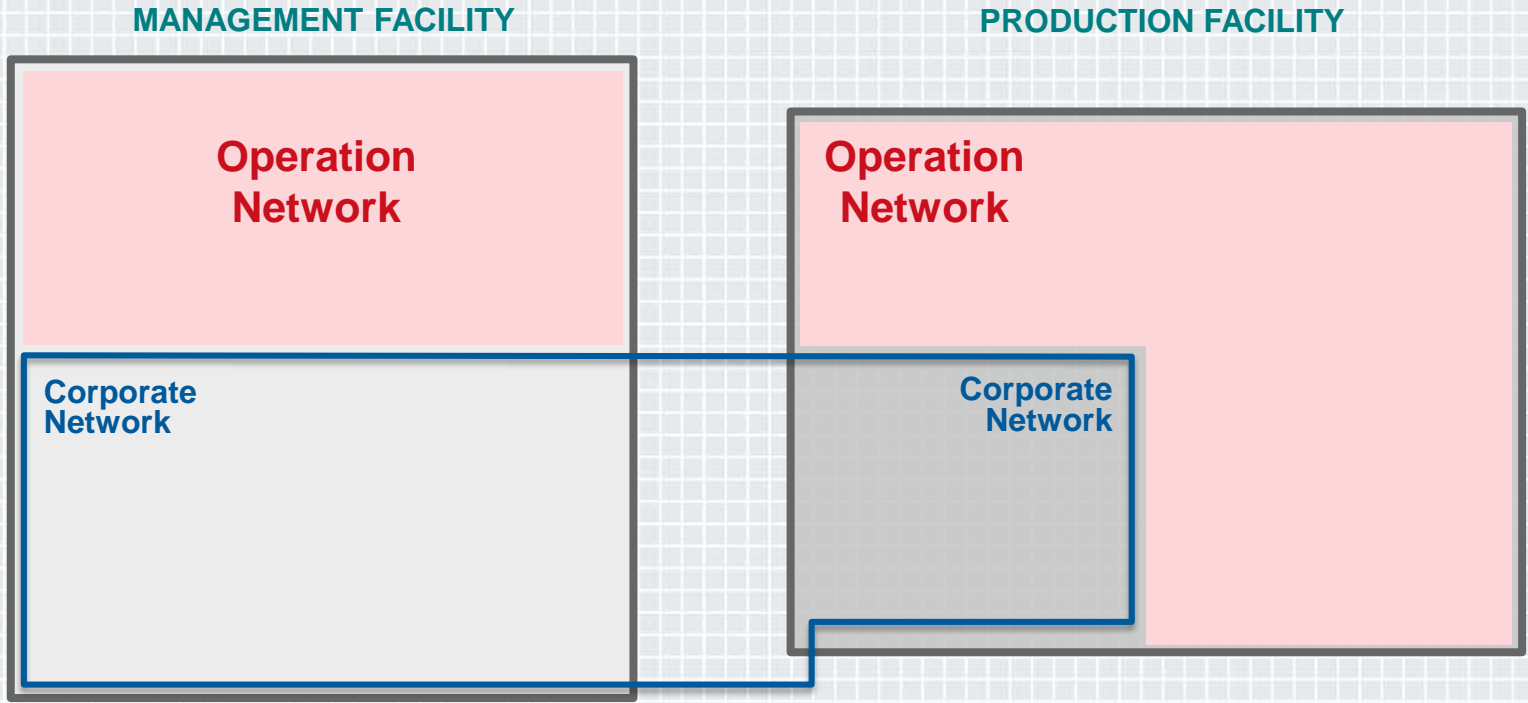
MANAGEMENT FACILITY



PRODUCTION FACILITY



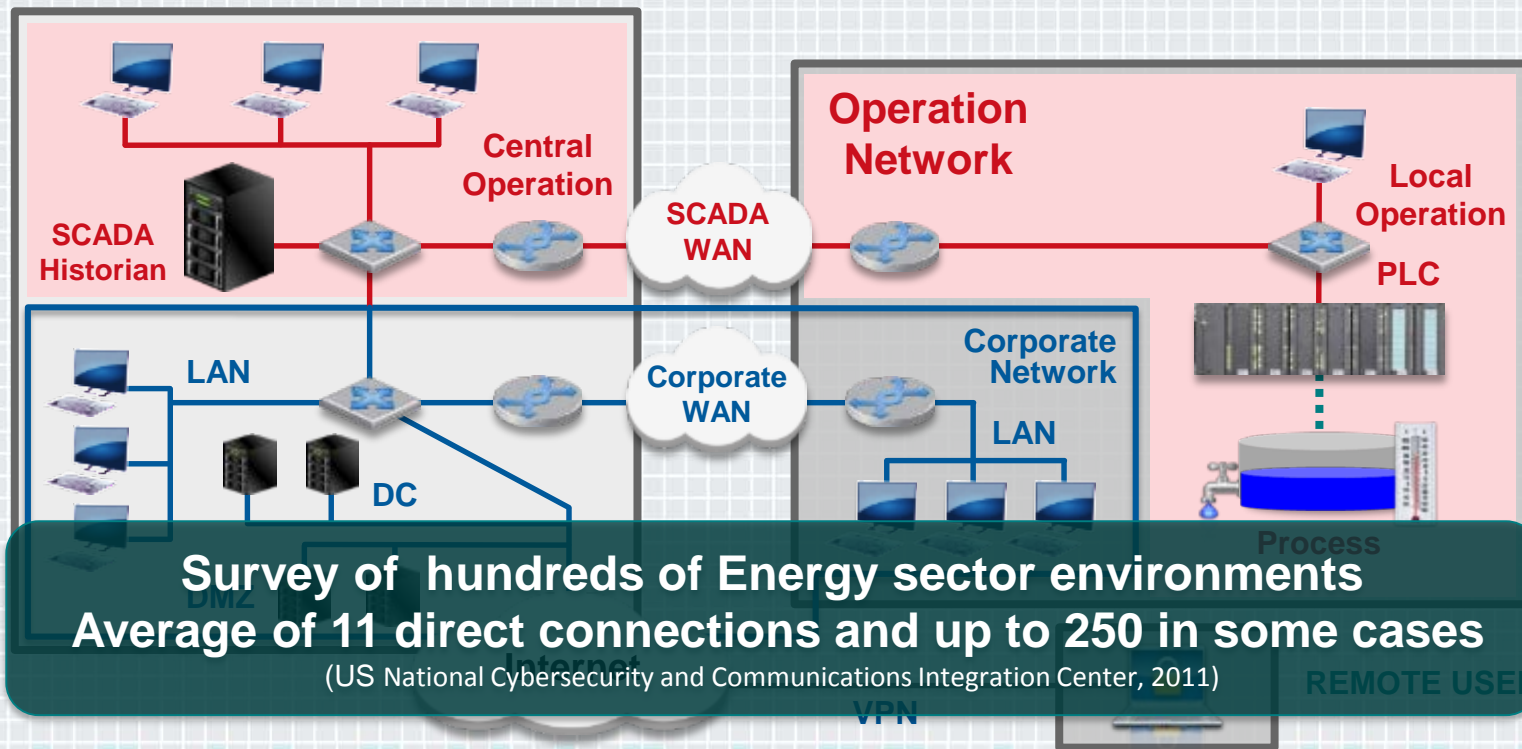
# Typical SCADA Network Structure



# IT and SCADA Networks are Interconnected

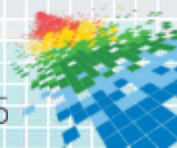
MANAGEMENT FACILITY

PRODUCTION FACILITY



**Survey of hundreds of Energy sector environments**  
**Average of 11 direct connections and up to 250 in some cases**

(US National Cybersecurity and Communications Integration Center, 2011)



# This is a Real Problem

- F-Secure found SCADA Attack that targets European Industrial Control Systems
- STUXNET worm designed to attack SCADA Program Logic Controllers
- Banking Trojans Disguised As ICS/SCADA Software Infecting Plants
- Hackers gain “full control” of critical SCADA systems
- Hackers aggressively scanning ICS, SCADA default credentials

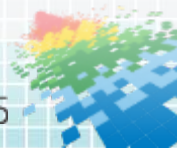
<http://www.darkreading.com/as-stuxnet-anniversary-approaches-new-scada-attack-is-discovered/d/d-id/1278881>

<http://en.wikipedia.org/wiki/Stuxnet>

<http://www.darkreading.com/attacks-breaches/banking-trojans-disguised-as-ics-scada-software-infecting-plants/d/d-id/1318542>

<http://www.itnews.com.au/News/369200,hackers-gain-full-control-of-critical-scada-systems.aspx>

<http://threatpost.com/hackers-aggressively-scanning-ics-scada-default-credentials-vulnerabilities/101150>













































# Examples of SCADA Vulnerabilities


Vulnerability	SCADA Impact
Unpatched Published Vulnerabilities	Most Likely Access Vector
Web Human-machine Interface (HMI) Vulnerabilities	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorization)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
SQL Injection	Data Historian Access
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering


Source: Idaho National Lab, 2011




# Examples of PLC Vulnerabilities

					
Firmware					
Ladder Logic					
Backdoors					
Fuzzing					
Web			N/A	N/A	
Best Configuration					
Exhaustion					
Non-doc Features					

 Vulnerability is present in the system and is easily exploited

 Vulnerability exists but exploit is not available

 System lacks this vulnerability.



# RSAC<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Choice of Platform for Control Systems



# Sometime I Wonder Why People

- **<RANT>**

- Choose the platform with the most exploits?
- Don't upgrade to the latest version of the Operating System?
- Don't apply patches and updates?
- Don't run AV, Anti-Malware, etc.?
- Run systems with no support?

- **</RANT>**

**They must WANT to run Malware!**



# Industrial Control Computers are Not Immune from Enterprise Security Challenges

- General purpose computers bring with them Enterprise vulnerabilities
  - Very common to use enterprise OS as base for industrial controllers
- Recent Problems
  - Siemens Open SSL Vulnerabilities
  - Shellshock / Bash Shell Vulnerabilities affect Industrial Control Systems

<https://ics-cert.us-cert.gov/advisories/ICSA-14-198-03G>

<http://blog.trendmicro.com/trendlabs-security-intelligence/shell-attack-on-your-server-bash-bug-cve-2014-7169-and-cve-2014-6271/>



# Industrial Control Computers

- Using old platforms for Critical Infrastructure increases the risk of an Attack
  - The attackers' don't need to learn new techniques to compromise these systems
- This is a symptom that Critical Infrastructure operators are not taking Security seriously

**Why make the attacker's job easier?**

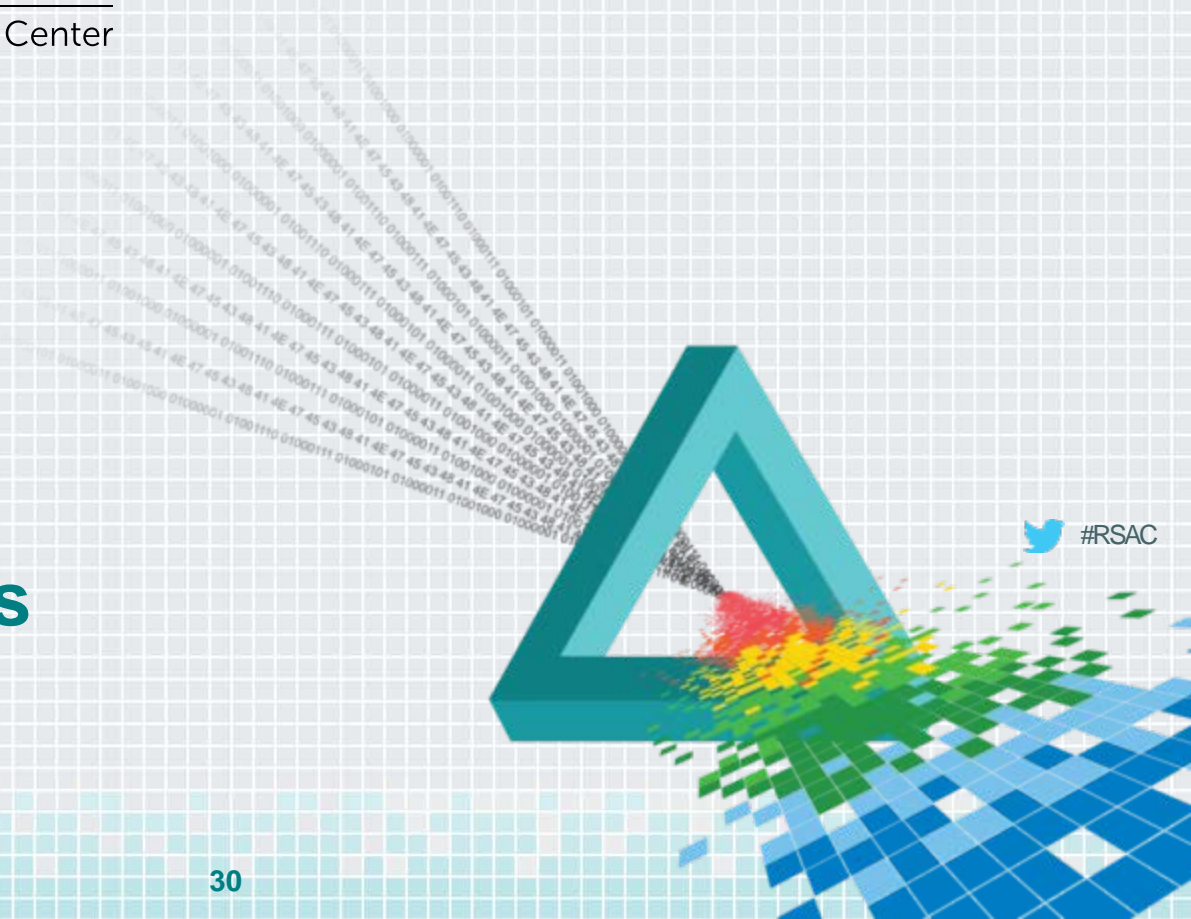


# RSAC<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Recommendations

 #RSAC



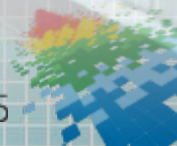
# How to Apply in Your Environment

Deploy strong perimeter security

Select platforms for their security characteristics

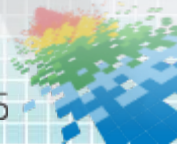
Use SCADA prevention technologies

Make Security a Priority

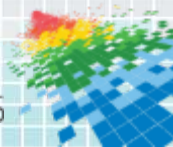
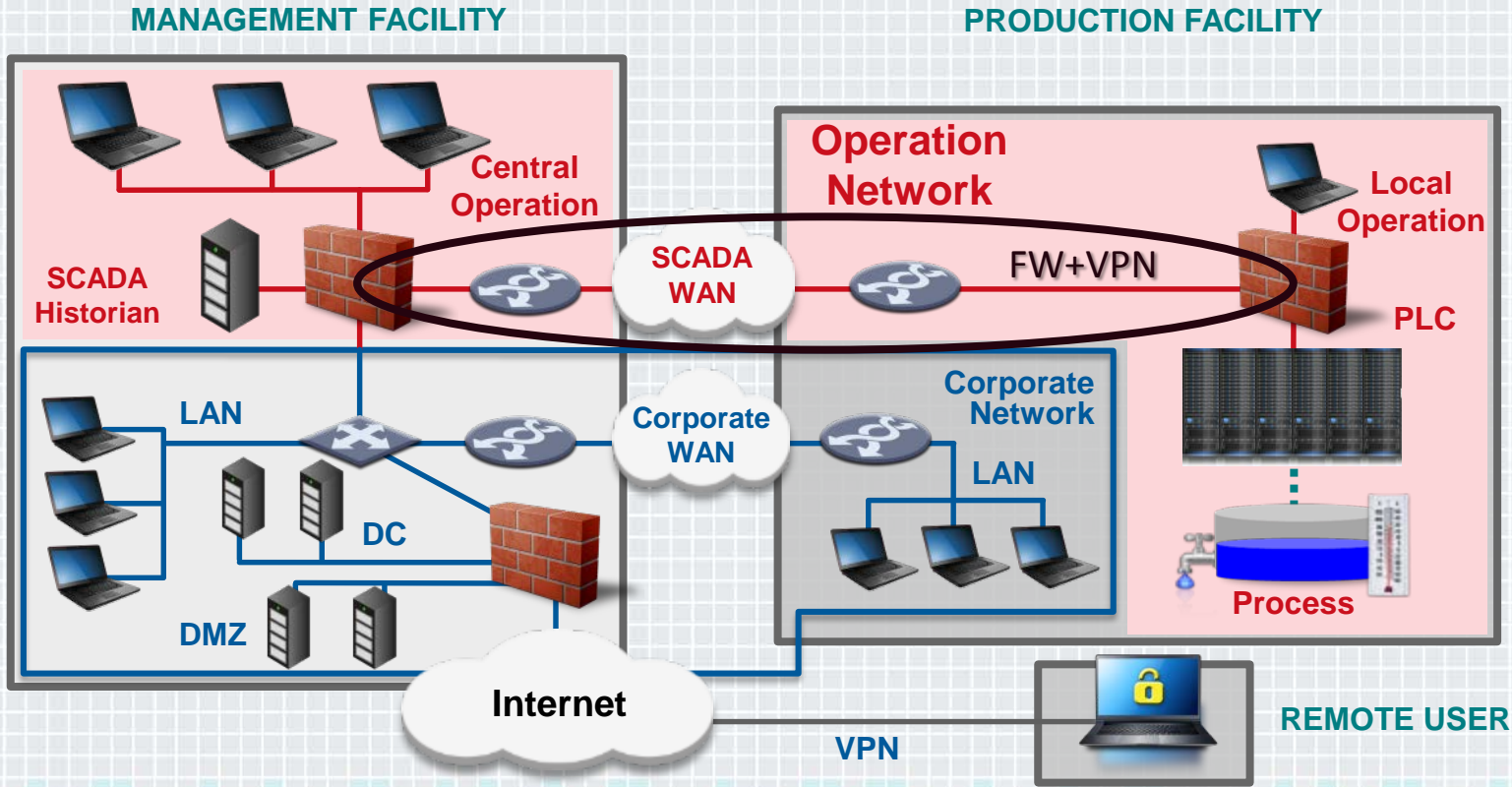


# Deploy Strong Perimeter Security

- Conventional Security Tools
  - Firewall
  - Intrusion Prevention
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
  - Data Loss Prevention (DLP)
- Critical to keep tools and signatures current
  - Internet Connection needed



# ICS Network with Perimeter Security





# Platform Security

- Make security a priority when selecting and/or upgrading computing platforms
- Aggressively replace old platforms and operating systems
  - Only run Operating Systems that are actively supported
  - Don't run Windows 95, 98, XP, Vista, 7
- Always apply latest patches and security fixes
- Always run current AV, Anti-Malware, etc.
- Control usage of USB ports



# SCADA Prevention Approach

LOG ALL SCADA TRAFFIC

Define Normal Baseline

- Full visibility (Known / Unknown / Not Allowed) and query

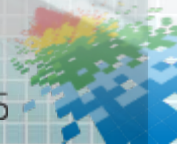
- Does not depend on SCADA devices ability to log

- No reliance on SCADA devices (based on mirror port)

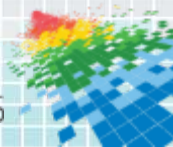
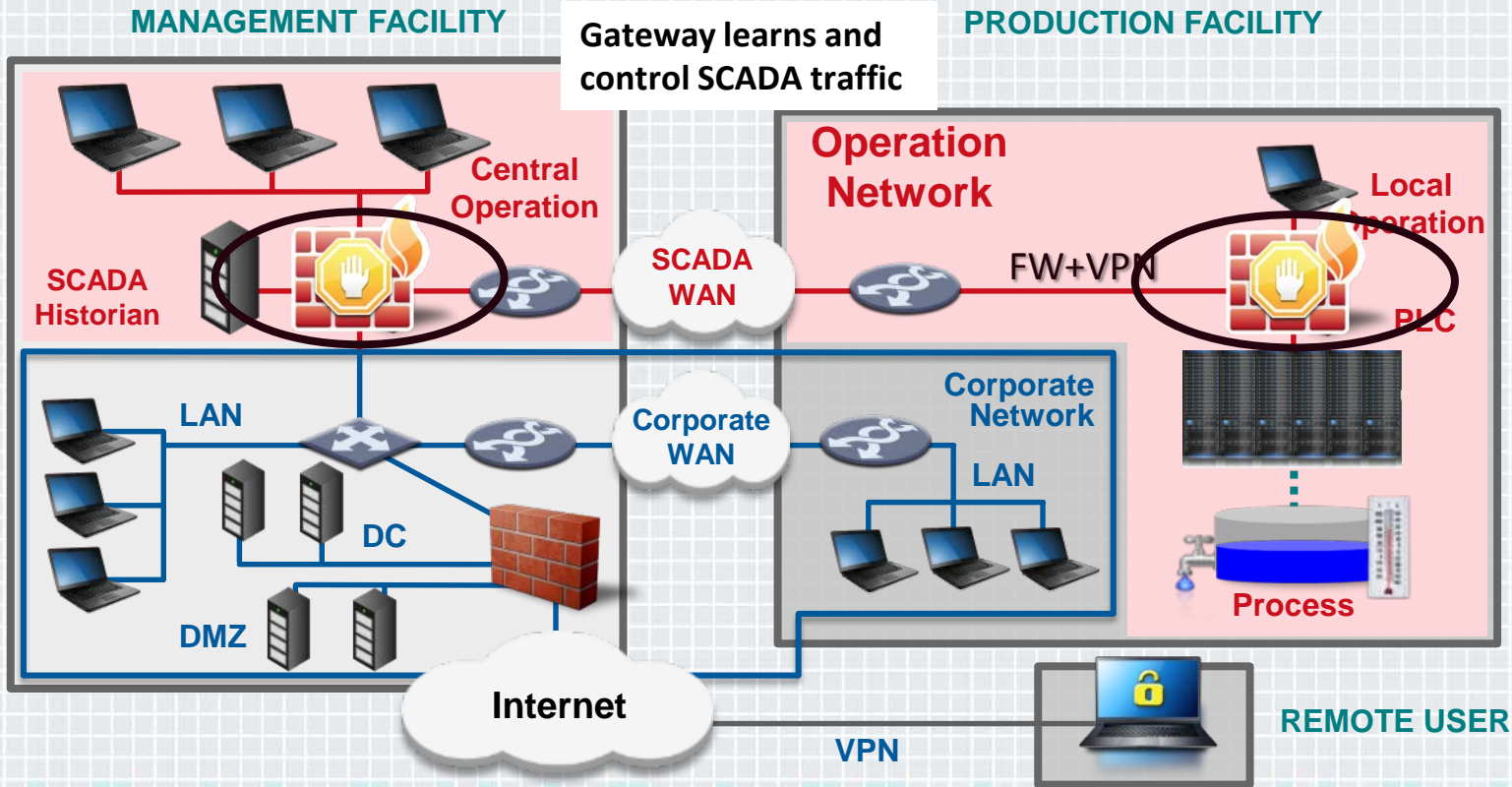
- Have forensics in case of attack

Identify Deviations and Attacks

Alert and Prevent Attacks



# ICS Network with SCADA Prevention



# Make Security a Priority

- Make Security part of the procurement process
  - Include Security in Service Level Agreements
- Invest in staff security training
  - This will be a cultural change, but critical
- Periodic Security Audits
- Actively track Industrial CERTs and Vendor Notifications
  - <https://ics-cert.us-cert.gov>
- Don't be afraid to report attacks and compromises



# Closing Thoughts

- This issue is Critical
- Attackers are getting better and are preparing for major attacks

**What are you going to do?**

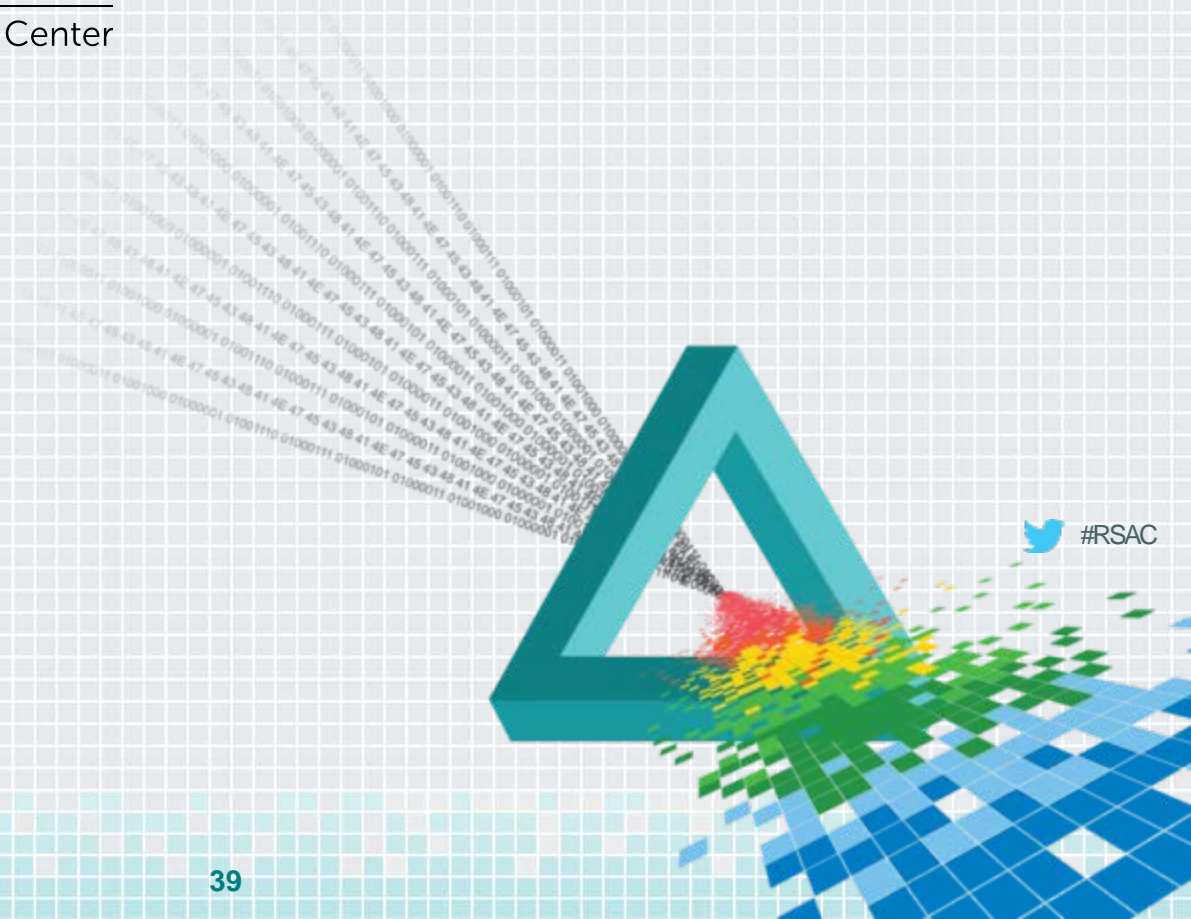


# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Q & A

 #RSAC



# **RSAC**®Conference2015

San Francisco | April 20-24 | Moscone Center

## Thank You

**Bob Hinden**  
**rhinden@checkpoint.com**

