



Industrial Control Systems Cybersecurity Landscape

Patrick C Miller, President and CEO, EnergySec
July 19 2011

Annual Emerson Ovation/WDPF
Users' Group Conference

What Is NESCO?



- Mission: Lead an independent, broad-based, public-private partnership to improve electric sector energy systems cyber security
- Goals:
 - Identify, disseminate common effective cyber security practices
 - Analyze, monitor and relay infrastructure threat information
 - Focus cybersecurity research and development priorities
 - Work with federal agencies to improve electric sector cyber security
 - Encourage key electric sector vendor support and interaction

Advantage: Adversaries



- Security approaches favor new installations, legacy environments are still vulnerable
- Very difficult to replace/patch in-service devices
- Isolation has diminishing security value
- Security products vs. buying secure products
- Engineering (N-1) and Security are different
 - Nature may be sophisticated, but it isn't malicious
- Hackers don't use a compliance checklist
 - Following a compliance checklist won't make you secure

Advantage: Attackers



- Intelligent, adaptive adversaries exist
- Cyberwar:
 - Stuxnet is a game changer, sets the new bar
- Espionage:
 - Project, market & customer data (e.g. NightDragon)
- Organized crime:
 - Same old tricks, new platform

Advantage: Adversaries



- Google search for “APT”
 - 34 hits in Jul 09
 - 169 hits in Jan 10
 - 1.2M+ hits June 11
- Google search for “cyberwar”
 - 416 hits Dec 09
 - 1.4M hits Feb 10
 - 3.4M+ hits June 11
- Welcome to the cyberarms race

Advantage: Adversaries



SONY

citibank



Bank of America



Morgan Stanley

The Washington Post



**Pacific Northwest
NATIONAL
LABORATORY**



HB Gary

SHODAN, ERIPP, ETC



EnergySec

The image displays two overlapping browser windows. The top window is the SHODAN website (www.shodanhq.com). It features a dark navigation bar with "Main" and "Exploits" links, and "Register" and "Login" buttons. The main content area has a search bar and a "Search" button. Below the search bar, there is a banner with the text "Welcome to SHODAN, the first computer search engine" and three bullet points: "» Search the internet for servers, routers and more", "» Find computers running certain software (HTTP, FTP, etc.)", and "» Filter hosts based on geographic location". A "Learn more" button is located below the banner.

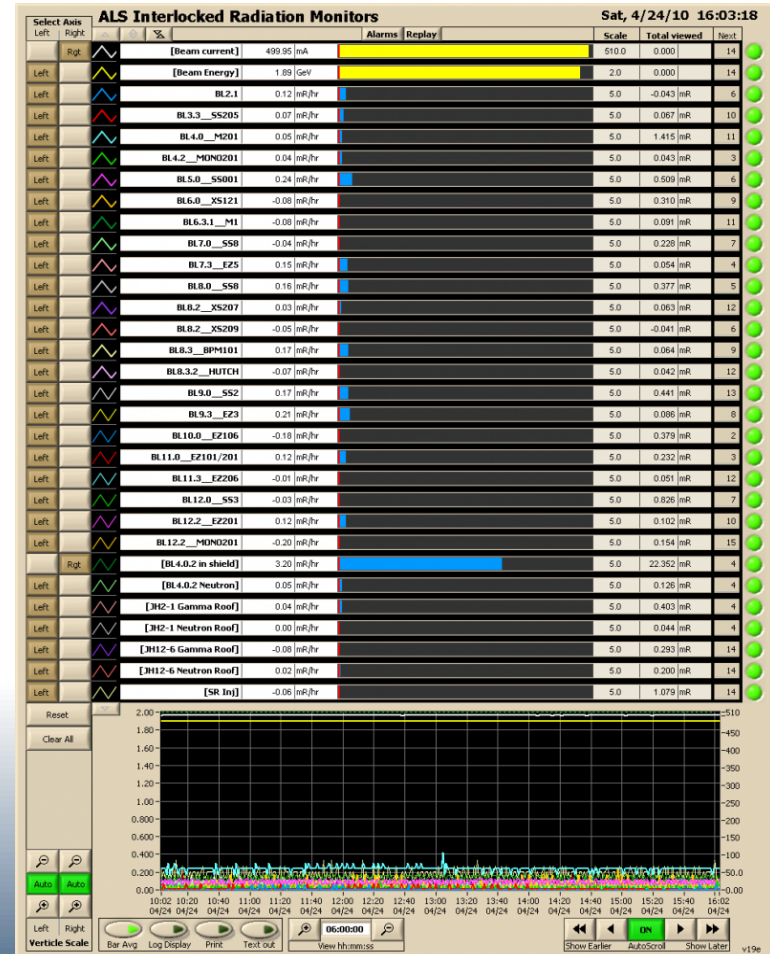
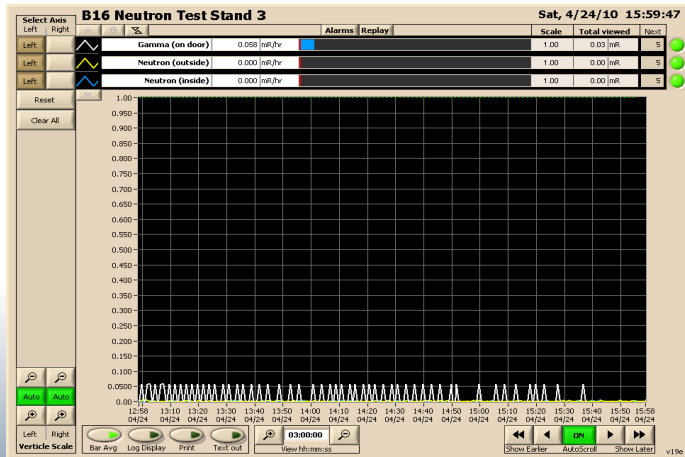
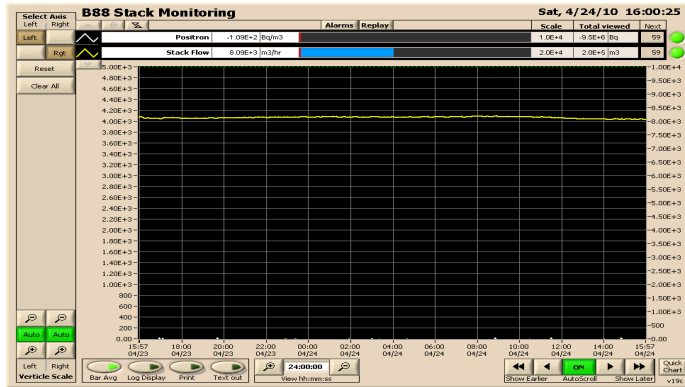
The bottom window is the ERIPP website (eripp.com). It has a blue header with the "ERIPP" logo and the text "Every Routable IP Project". The navigation bar includes "Home", "FAQ", "IP Database", "Stats", and "Contact" links, along with a "Connect" button. The main content area is divided into two columns. The left column has a "stats" section with the following data:

Workers Running:	481
Active hosts found:	15953949
Next IP group:	97.138.118.69
Database size:	2607.8MB

Below the stats is a "Ads by Google" section with a link to "What's Your IP Address?". The right column has a "What's This?" section with the text: "This project will attempt to connect to every IP address on the internet. More specifically, we'll be connecting to port 80 (the port your browser uses to view webpages by default). This will tell us if the address we're connecting to is acting as a webserver." Below this is a "Why do this?" section with the text: "We believe its possible that many websites are not found by modern search engines. This is due to the fact that most search engines use links from sites they've already found (indexed) to find other sites. This leaves the possibility of some sites not being discovered if they are not linked to by a site that's already been found." At the bottom of the right column, it says: "By connecting to every IP address on the Internet, we have the capability of finding sites that have never been indexed before."

The National Electric Sector Cybersecurity Organization (NESCSO) is partially funded by the Department of Energy

SHODAN, ERIPP, ETC



Berkeley Cyclotron HMI images

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy

The “Air-Gap” Myth



EnergySec

69.92.101.2
Added on 10.02.2011

69-92-101-2.cpe.cableone.net

HTTP/1.0 200 OK
Server: **LV_HTTP/1.0**
Date: Thu, 10 Feb 2011 0
Content-type: text/html
Last-modified: Wed, 25 J
Content-length: 704
rrcs-96-11-251-66.central.biz.rr.com

69.139.97.213
Added on 09.02.2011

c-69-139-97-213.hsd1.ms.comcast.net

HTTP/1.0 200 OK
Server: **LV_HTTP/1.0**
Date: Wed, 09 Feb 2011 1
Content-type: text/html
Last-modified: Wed, 25 J
Content-length: 704
64.7.227.38
Adtran NetVanta
Added on 25.05.2010

66.212.169.244
Added on 09.02.2011

dl.cashcode.com

HTTP/1.0 200 OK
Server: **LV_HTTP/1.0**
Date: Wed, 09 Feb 2011 1
Content-type: text/html
Last-modified: Tue, 05 A
Content-length: 1041
209.47.163.29
Adtran NetVanta
Added on 15.04.2010

139.6.18.127
Added on 01.02.2011

ntrt127.nt.FH-Koeln.DE

HTTP/1.0 200 OK
Server: **LV_HTTP/1.0**
Date: Tue, 01 Feb 2011 1
Content-type:
Content-length: 580
69.43.15.180
Added on 19.11.2009

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Server: **Ubicom/1.1**
Content-Length: 26
WWW-Authenticate: Basic realm="(Tenn-Plant)"
Connection: close

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Server: **Ubicom/1.1**
Content-Length: 26
WWW-Authenticate: Basic realm="(Wnsbro Water Plant)"
Connection: close

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0



S
C
V
C
I
C
E
S
C
C
F
C
V

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Compliance Application Notice — 0024
Compliance Application: CIP-002—CIP-009 Routable Protocols and Data Diodes

There's An App For That



- “Get mobile access to your control system via an iPhone, iPad, Android and other smartphones and tablet devices. The Ignition Mobile Module gives you instant access to any HMI / SCADA project created with the Ignition Vision Module.”



- ASSISTING NWPPA UTILITIES MEET THE CHALLENGES OF WECC, FERC, CIP & NIST INTEROPERABILITY COMPLIANCE
Approved Smart-Grid OEM for the PNW Smart-Grid Demonstration Project - Battelle & BPA

- PROVIDING NWPPA UTILITIES WITH COST EFFECTIVE SMART GRID METERING, DEMAND-RESPONSE, & SCADA TOOLS
OEM for Direct Connection to BPA 3E34500 Substation



HMI In The Cloud



“Use any standard browser on any device to access HMI. No downloads, no tedious installs, no plug-ins. Login and you have the HMI in your hands wherever you are: factory cafeteria, or parking lot, or on the beach, or even the golf course!”

GoToMyHMI: Your HMI-Gateway™ in the Cloud

Home | Contact Us | Login

Instant HMI

GoToMyHMI - Your 'HMI-Gateway' in the Cloud

Free Live Demo Access

Access InstantHMI 6.0 using any standard browser on any device
No downloads. No tedious installs, No plug-ins.

GoToMyHMI - 'Your HMI-Gateway in the Cloud'

Use any standard browser on any device to access InstantHMI. No downloads, no tedious installs, no plug-ins. Login and you have the HMI in your hands wherever you are: factory cafeteria, or parking lot, or on the beach, or even the golf course!

Video Tutorial

The Three S in 'HMI in the Cloud' Computing

Security Simply Spend

GoToMyHMI provides Secure, Easy and Fast access from any browser to InstantHMI 6.0, ready to serve you on the cloud today. Remotely Monitor, ACK Alarms and Control your HMI for one low flat fee.

More...

InstantHMI® 6.0 - 'Cloud Ready' Today

GoToMyHMI Services and pricing

Selling up 'Cloud Access' to InstantHMI is as easy as 1-2-3

Application Note & FAQ (VNC, Security, ...)

Our Partners

GoToMyHMI - a Certified Secure Site

SOFTWARE HORIZONS INC.

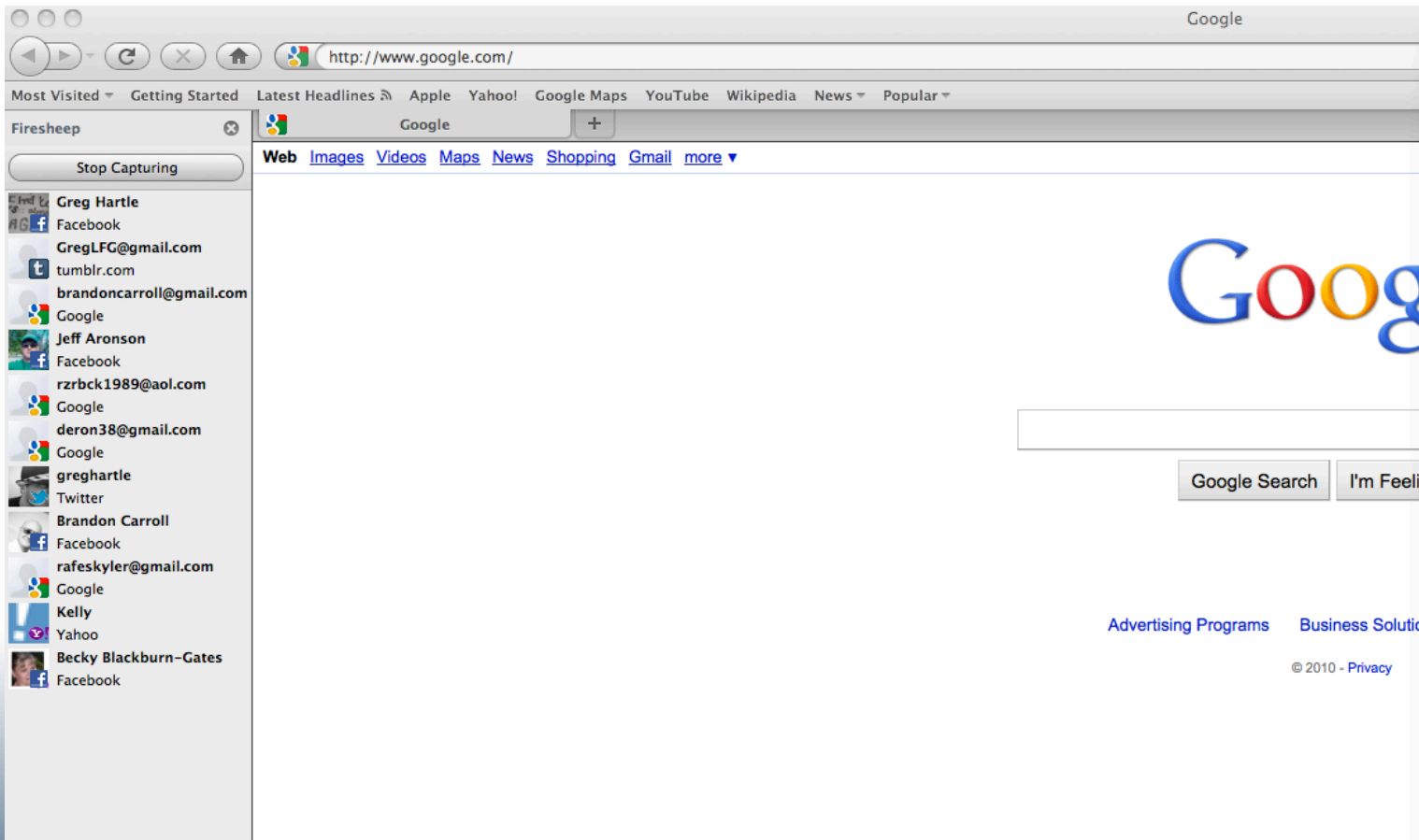
Quick Links: GoToMyHMI Manual | GoToMyHMI Services | InstantHMI Brochure | InstantHMI Downloads

Software Horizons, InstantHMI and InstantPanel are Registered Trademarks. GoToMyHMI, InstantChip, Qi-Widgets, LaunchPad and QuickPad are Trademarks of Software Horizons Inc. All other trademarks belong to the respective companies.

Copyright © 2011 Software Horizons Inc. All Rights Reserved. Last Modified: March 1, 2011

“GoToMyHMI provides Secure, Easy and Fast access from any Browser to InstantHMI 6.0, ready to serve you on the cloud today. Remotely Monitor, ACK Alarms and Control your HMI for one low flat fee.”

Public Domain



Research and Disclosure



46 zero-day SCADA vulnerabilities issued a two-week span



Luigi Auriemma
alugi@autistici.org

ADVISORIES

The complete archive of my advisories about [software security vulnerabilities](#) found by me

News
[Advisories](#)
[Proof-of-concepts](#)
[Research](#)
[Fake_players_bug](#)
[MyToolz](#)
[Password_recovery](#)
[Patches](#)
[MyMusic](#)
[TestingToolz](#)
[About...](#)
[RSS_feeds](#)
[Amiga_ADF](#)
[Forum](#)

[alugi.org](#)
[backup.alugi.org](#)
[mirror.alugi.org](#)

ADVISORIES

Stack overflow in Microsoft HTML Help 6.1 (CHM files)
12 Apr 2011: [adv - PoC - chm_1](#)

Vulnerabilities in Microsoft Reader 2.1.1.3143 / 2.6.1.7169
11 Apr 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - msreader_1/5](#)

DoS vulnerabilities in Microsoft Host Integration Server 2010 8.5.4224.0
11 Apr 2011: [adv - snabase_1](#)

Vulnerabilities in Siemens Tecnomatix FactoryLink 8.0.1.1473(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - factorylink_1/6](#)

Vulnerabilities in Iconics GENESIS32 9.21 and GENESIS64 10.51(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - adv8 - adv9 - adv10 - adv11 - adv12 - adv13 - genesis_1/13](#)

Vulnerabilities in 7-Technologies IGSS 9.00.00.11059(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - adv8 - igss_1/8](#)

Vulnerabilities in DATAC RealWin 2.1 (Build 6.1.10.10)(SCADA)
21 Mar 2011: [adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - realwin_2/8](#)

From Obscurity To Novelty



- Smart Meter hacking
- Hacking cookbooks
- Metasploit, Core Impact, etc
- Fuzzers
- Supply chain attacks
- Manuals available in all languages on Internet

Shiny Object



- Shiny object for the mass media
- 60 minutes
- Wall Street Journal, National Journal, CNN
- Too many IT trade publications to name
- Blockbuster films
- Prime time television shows
- Social Media...


TwitBookBlogosphere



twitter Login Join Twitter!

Nice attack scenario shown by Andrei Costin at #t2infosec - you could hack a laser printer so it stops the paper in the fuser, igniting it.

about 12 hours ago via Mobile Web
Retweeted by 21 people

 **mikkohypponen**
Mikko H. Hypponen

 **@reversemode**
Rubén Santamarta

Regarding missile failures, insecure BAS may pose risks <http://yfrog.com/6ggvpp> reporting to the ics-cert...

2 minutes ago via TweetDeck ☆ Favorite ↻ Retweet ↩ Reply

Utah National Guard Armory's
Id= [redacted]
Username:
Password:

twitter Login Join Twitter!

Securing critical infrastructure at a snail's pace <http://bit.ly/gHgn3d> Why bother with kinetic attacks at all?
#cyberwar #infosec #security


about 22 hours ago via web
Retweeted by 2 people

 **ArtKingston**
Arthur Kingston

twitter Login Join Twitter!

I'll be presenting "SCADA Trojans: Attacking the grid" odays+maths+RE+substations...at **#rooted2011** <http://bit.ly/fKfAme>

4 minutes ago via TweetDeck
Retweeted by 1 person

 **reversemode**
Rubén Santamarta

Economic Drivers



- Recession economy brings unique challenges
- Decreased participation working groups and conferences
- Static or shrinking headcount; increased workload
- Downsizing, pay freezes, etc increase insider threat
- Decreased spending on new equipment
- Older products extended beyond intended lifespan
- Security more expensive for customers and vendors

People Problem



- Humans are the **weakest** link in any security system
 - Passwords for candy; Social engineering
- Humans are also the **strongest** link
 - The Aware Person System (APS)
 - ICS culture shift is very slow, but powerful
- Danger: untrained operators of power tools can cause significant damage
 - Increasing complexity = training treadmill



Back In The Good Old Days



- Pneumatic, electromechanical, analog
- Telephone meant POTS or “bat phone” – no VoIP
- No Internet
- Less automation
- Less complexity
- Proprietary
- Long life span

ICS Gen-X



- Automation, more complexity
- Internet Protocol (TCP/UDP/etc)
- Data, more data and even more data
- Processing power, memory, bandwidth
- Interconnected business
- Migration from flat to segmented networks
- COTS software and hardware
- Increasingly shorter lifespans

Millennium Systems



- Highly digital, highly complex
- Highly interconnected, highly layered
- Bitflocking, dynamic emergent behavior
- New protocols
- New interdependencies
- Homogenization
- Innovation treadmill; constant lifespan flux

Current Landscape



- Regulatory compliance is stealing the show
- Mixing legacy and bleeding edge tech is difficult
- Logical distance between kinetic endpoint and HMI is exponentially increasing; “hyperembeddedness”
- No system is 100% isolated or 100% secure
- Researchers and hackers know all of this and more
- Nation-state quality defense is the new norm
- Sufficient motive, means and opportunity exist to take the threat seriously

Questions?



Non-profit. Independent. Trusted.



Patrick C Miller, President and CEO
patrick@energysec.org
503-446-1212
@PatrickCMiller

The National Electric Sector Cybersecurity Organization (NESCO) is partially funded by the Department of Energy