



Setting the Standard for Automation™

Self Assessment Development, Process, Standards, and Tools Interest Group

EXPO 2005

Chicago, IL

October 25, 2005

Brian Isle

brian.isle@adventiumlabs.org

www.adventiumlabs.org

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Presenter: Brian Isle



- Chief of Operations & Member of the Technical Staff
 - B.SEE, University of Minnesota, 1976
 - Certified Professional Engineer, Minnesota
 - Six Sigma Certification 2001
- 15 year R&D management
- Control system and product design
- 10 years of experience in critical infrastructure safety and security
 - Ranging from gas and oil transportation to airport security

Agenda

- Introduce PCSF
- Definition of SCADA
- Is the SCADA cyber threat real?
- SCADA specific cyber issues
- Self Assessment Interest Group

Supervisory Control and Data Acquisition

General Definition

- Industrial measurement and control system consisting of:
 - central host or master
 - one or more field data gathering and control units or remotes
 - collection of standard and/or custom software used to monitor and control remotely located field data elements.
- Generally cover larger geographic areas
- Predominantly open-loop control characteristics
- Use variety of communications systems

<http://members.iinet.net.au/~ianw/primer.html>

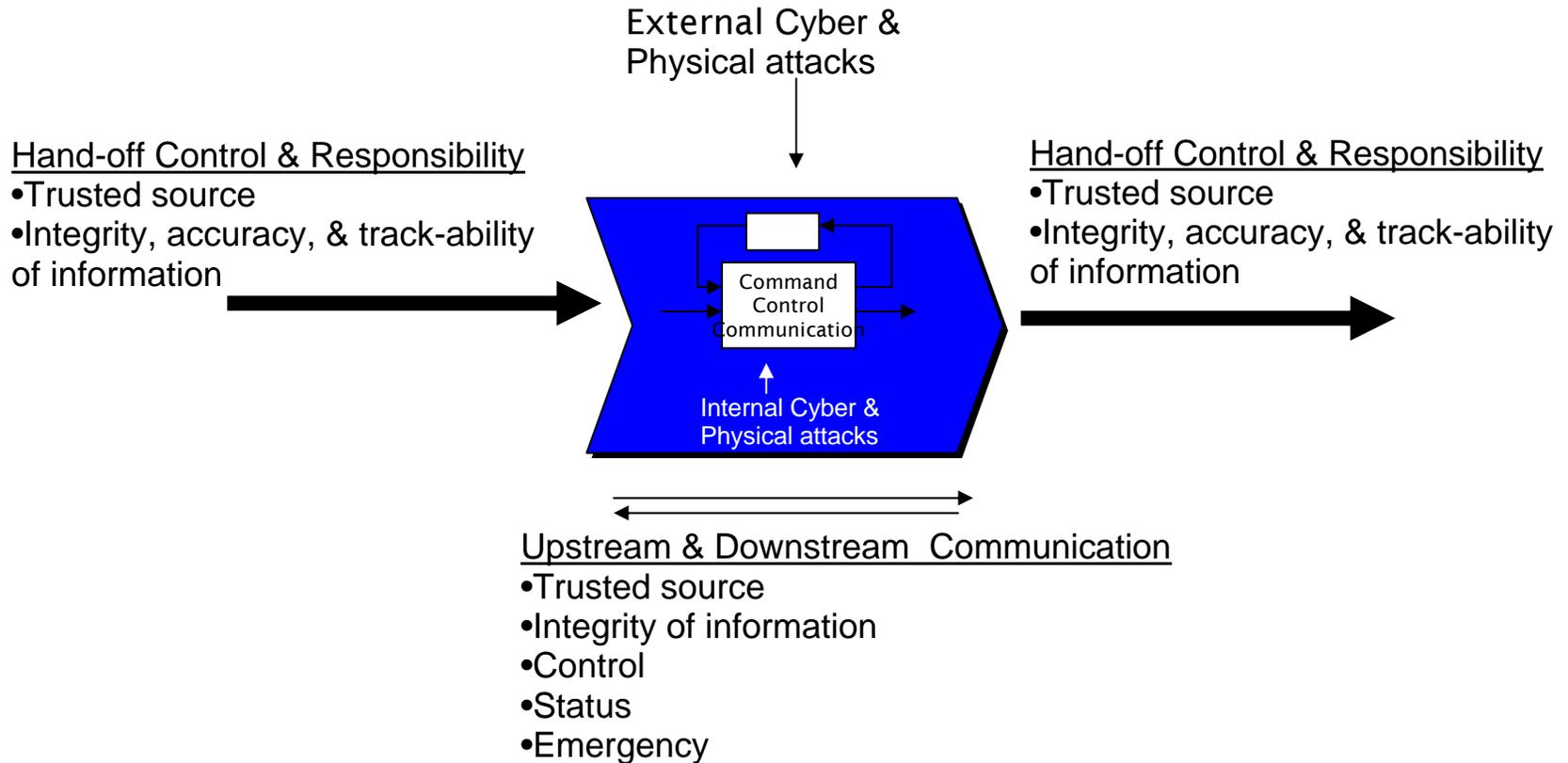
Distributed Control Systems (DCS)

General Definition

- Similar to SCADA systems, used predominately in factories, treatment plants etc.
- Similar functions to SCADA, but the field data gathering or control units are usually located within a more confined area.
- Communications often via a reliable and high speed local area network (LAN).
- DCS system usually employs significant amounts of closed loop control.

<http://members.iinet.net.au/~ianw/primer.html>

Think of Your Facility as a Link in a Chain



Each element of the chain faces security issues.

Is the SCADA Cyber threat real?

“Hackers Cracked Gazprom Security
World's Largest Natural Gas Company
Lost Control of Gas Flows For Some
Time”

MOSCOW, April 26 [1999]

MSNBC STAFF AND WIRE REPORTS

Is the SCADA Cyber threat real?

The threat is real and proven:

A disgruntled ex-employee used a port scan and ping-sweep program to identify active system ports and network IP addresses belonging to an oil company. On finding an active connection and an open port, he initiated communication using various software tools downloaded from the Internet. He subsequently issued instructions to the remote system and deleted sensitive system related to process control flow.

SECURING CRITICAL OIL INFRASTRUCTURE FROM CYBER THREATS, Asian School of Cyber Laws, August 2002, [Rohas Nagpal](#), [Debasis Nayak](#)
http://www.asianlaws.org/cyberlaw/library/cc/oil_report.htm

Is the SCADA Cyber threat real?

In August 2003, the **Nuclear Regulatory Commission confirmed** that in January 2003, the Microsoft SQL **Server worm known as Slammer**—infected a private computer network at the **Davis-Besse nuclear power plant** in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. – Note: the plant was off-line at the time.

<http://www.gao.gov/cgi-bin/getrpt?GAO-04-140T>

Cyber Attacks Are Real



What does it take?

- Knowledge of the control system
- Laptop computer
- Wireless link

More Wireless – More Vulnerabilities

Some wireless data links that were designed for short range can be extended considerably

LAS VEGAS -- ... teens from Cincinnati got an ovation at the DefCon hacker conference here Sunday when organizers announced that the winners of this year's Wi-Fi shootout might have broken a world record for ground distance in **establishing a 55.1-mile Wi-Fi connection.**

http://www.wired.com/news/culture/0,1284,64440,00.html?tw=wn_tophead_2

Bluetooth sniffing over 1 mile has been demonstrated

Cyber Attack Trends: More Bad News

Virus writers are now focusing on smart cell phones & microcode

- “Mosquito virus bites smart phones”, Ben Charny, Special to ZDNet India, August 13, 2004
 - The Mosquito virus forces some cell phones....
 - .. first worm to target smart phones dubbed Cabir, uses the Bluetooth feature of smart phones to detect other phones, and then transfers itself to the new host
 - A virus that infects Windows CE was developed--the first such bug discovered for the handheld operating system.
- "Malware, Fighting Malicious Code", Ed Skoudis, Lenny Zelter, 2004
 - Microcode trojans may be able to attach to the closely held microcode programming that runs internal to a CPU,

Why care? Because the embedded systems in the RTUs are largely unprotected.

There is always email

MINNESOTA TECHNOLOGY
FALL 2004

Infected Junk

If it seems like you're getting more junk in your e-mail box these days, you're not dreaming. These are the numbers from MessageLabs, a New York City-based e-mail security provider. The data is based on the volume of spam and viruses the company intercepted for its customers.

	Percent of e-mail that is spam	Amount of e-mail infected with a virus
2003		
January	24.4	1 in 184.44
February	25.6	1 in 253.96
March	35.7	1 in 265.71
April	43.5	1 in 276.0
May	55.6	1 in 147.69
June	38.5	1 in 125.55
July	51.0	1 in 166.26
August	52.6	1 in 28.94
September	43.7	1 in 10.02
October	50.5	1 in 102.70
November	55.1	1 in 97.20
December	62.7	1 in 158.20
2004		
January	63.0	1 in 129.81
February	59.9	1 in 19.55
March	52.8	1 in 43.73
April	67.6	1 in 10.58
May	76.1	1 in 10.96
June	86.3	1 in 10.70

— E.H.

Policy vs. Cyber Attacks

- “Sound policy is a core element of the cyber security management system. Without it, extensive implementations of routers, firewalls and intrusion detection systems are misguided. Indeed, policy steers the application of technology within this system.” (1)
- 80% of attacks show weakness in internal processes (2) (3)
 - Unauthorized modems
 - Disgruntled employee
 - You hired a terrorist
 - Unauthorized access
 - In-sufficient attention to security (leave the door open)
- Security assessment is viewed as a one-time-event that lacks a metric to allow comparison over time nor assess readiness

No amount of technology will make up for lack of sound policy.

Is the Terrorist Threat Real?

Know Your Adversary

- Technically educated and experienced
- Patient
- Persistent
- Adequately funded
- Trained in the trade-craft
- Able to blend-in

Is the Terrorist Threat Real?

<http://www.gao.gov/cgi-bin/getrpt?GAO-04-140T>

The NIPC report also stated that U.S. law enforcement and intelligence agencies had received indications that **Al Qaeda members had sought information about control systems** from multiple Web sites, specifically on water supply and wastewater management practices in the United States and abroad

<http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html>

“The **same SCADA systems that are used to manage the U.S. power grid also control the grids in Iraq, Saudi Arabia, Indonesia, and Iran.** So it should come as no surprise that SCADA documents turned up in Al Qaeda safe houses in Afghanistan.”

Why do a Self Assessment IG?

- The threat is real, the Nation can't wait
- Need a reasonable means to measure and compare readiness
- Provide independent voice to advise the standards groups

SCADA cyber readiness is largely unknown

SCADA Specific Cyber Issues

- Multi-generational installations
- Geographically distributed systems
- Graying of the workforce
- Safety focused, not security focused
- Lack of accepted cyber vulnerability measures
- These are “control systems” – NOT – “IT”!
- Mostly privately owned, distaste for regulation
- Assessment scalability issues

SCADA CYBER Self Assessment Working Group (SCySAG)



Charter

- Develop the requirements for the SCADA cyber self assessment tools and methodologies that can be used to strengthen the North America's industrial, energy, and utilities infrastructure.
- Look broadly across the sectors, regulated and non-regulated industries, review current and past assessment work, and combine with end-user interaction, to develop the requirements.
- Utilize an open process, industry driven, and utilize broad industry, labs, and Government participation to ensure a cross domain requirement set is delivered.

SCADA CYBER Self Assessment Working Group (SCySAG)



The adoption of the requirements will be voluntary. The results of this effort can be used by:

- Tool and methodology vendors to develop, deploy, and maintain an assessment solution,
- SCADA system vendors to create more secure systems,
- Standards bodies and groups, and
- Owner/operators developing their internal policies and procedures.

- Recruit active volunteers
- Finalize the charter
- Set the scope of deliverables
- Identify the players and interactions
- Develop strategy to make an impact

Move briskly, build on past, & complement other activities

Discussion