Secure SCADA Summit

Dan Mintz, CTO

Civil Health Services Group

dmintz@csc.com

Twitter: technogeezer

,

December 2009

For 50 years, CSC Has Helped Clients Ride Every Major Business- Driven Technology Wave

CSC is a **world leader** in leveraging IT to develop business solutions and services

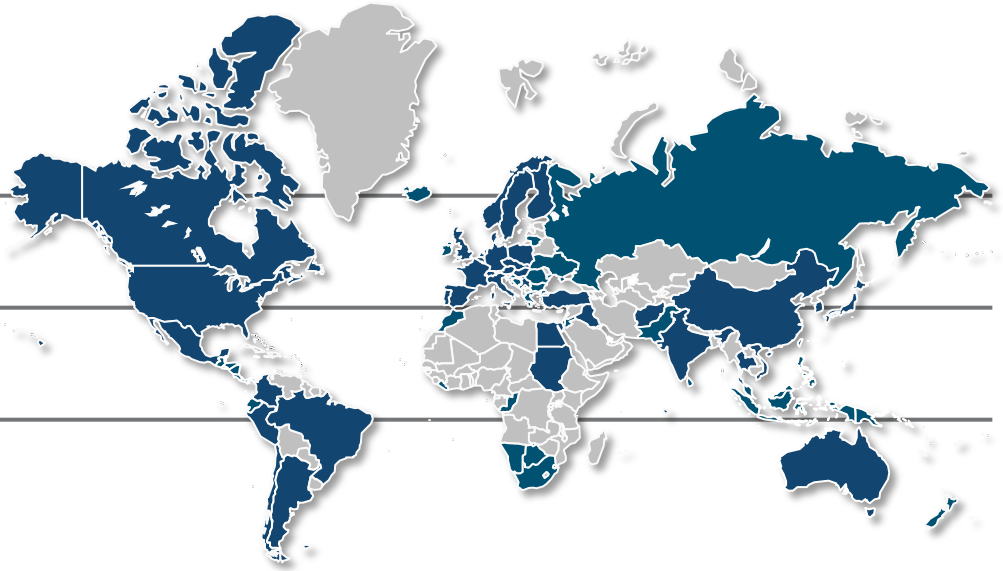
Market-leading corporations and major government agencies partner with us **when delivery is critical to their mission**

Our **91,200 professionals** serve clients in more than 90 countries

We have an enviable track record of **client service excellence**

Our **global delivery network** provides consistent delivery of solutions and services — common processes and highly skilled, cost-effective, multilingual resources

We are CSC: an NYSE, Fortune 200 and Fortune “Most Admired Company” — **50 Years Strong**



Across the globe — when delivery is critical

The most successful company you may have never heard of…

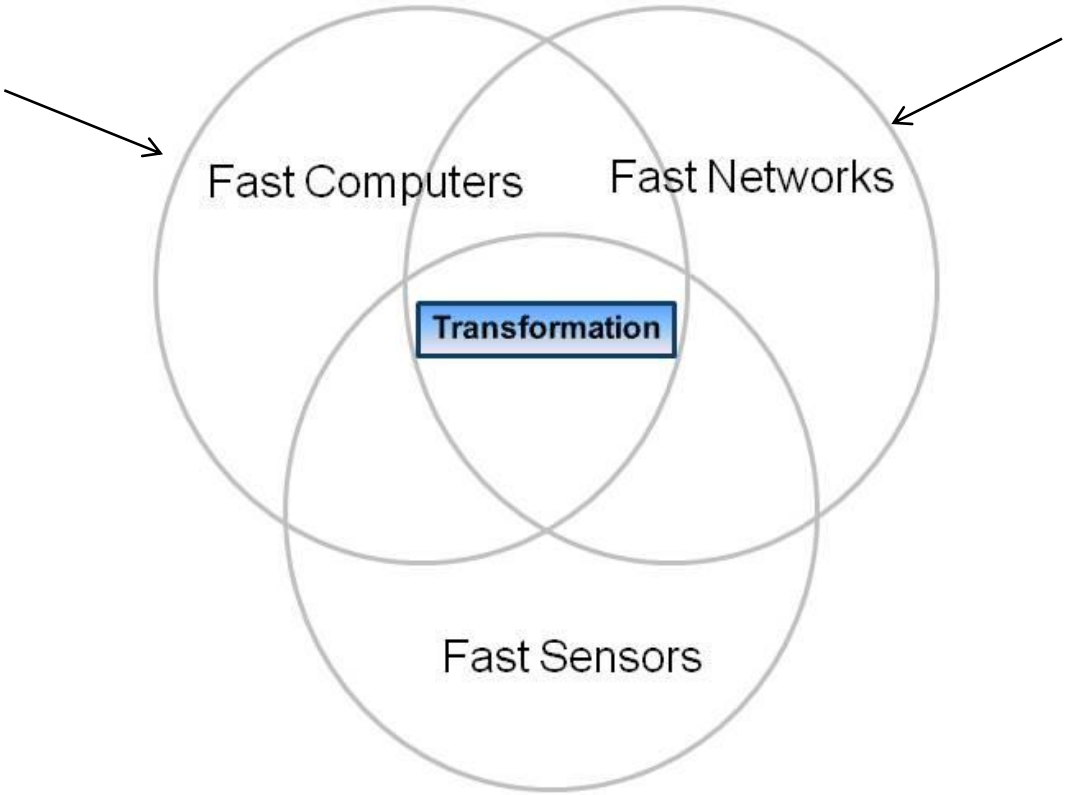
Part I – Some Context

- **How did we get here?**
  - Transactional Cost Economics
  - Technology
    - Fast computers, Fast Networks
- **A Few Interesting Questions (at least they're interesting to me)**
  - Everything's an intermediate step, nothing in the center
  - I never knew clouds at all
  - Fast Sensors
- **So What's the Government Going to do About All This**

Transactional Cost Economics

- **What do you know about Ronald Coase?**
- **He provided an explanation for the economic basis for a corporation ‘s existence**
  - The higher the cost for a ‘transaction’, the more advantageous to integrate that capability internal to the corporation
- **BUT – when transactional costs are reduced dramatically by the impact of the Internet, what then?**
- **For example, Proctor and Gamble …**

The Immersive Internet



Ptolemy Versus Copernicus

From earth centered to Sun centered to nothing centered

How I Would Like to Look At Clouds

- **Everything is a cloud**
- **Your desktop computer is a cloud – just not a very optimized one**
  - It is, in fact, a private cloud
- **A typical server is a community cloud**
  - Multiple users who have some afinity
- **Your browser accesses a public cloud**
- **You are a private cloud**
- **Your company is a community cloud**
- **Your industry may be a community cloud or a public cloud**

Cloud Computing

	Approach	Governance	Security	Economics
Private	Virtualization	1	User Self-Managed	Expensive
Community	Andy Hardy	➢1	User Coordinated	Varies
Public	We hug your servers so you don't have to	None	Provider created (reputational environment)	Inexpensive

- Over time when is it possible to avoid moving to the public cloud?
  - Security clearances enable a community cloud
  - Oligopolies can achieve a community cloud

What Happens As We Add Fast Sensors?

- **With the addition of fast sensors to the fast computers and fast networks that are now in place in much, though not all, of the country**
  - Sensors become participants in the network, not just passive receptors of instructions or senders of data
  - It becomes possible to perform real-time simulations in real-time with real-time data
- **And thus virtual environments and 'real' environments being to comingle**
  - Becomes possible to emulate accurate representations of reality in real-time for interpretation and management
  - The implications are enormous and hard to predict

Government Issues

- **Private-Public Partnership**
  - What does that mean
  - Governance process; private membership?
  - Public leadership? White House, DHS, Commerce?
- **Tie cyber issues to financial?**
  - Risk ratings? Re-insurance?
- **At least three different pieces of legislation are, or will be, out there**
  - Rockefeller – Snowe
  - Lieberman – Collins
  - House version
- **Sharing vs Protection? Protection vs Resiliency?**
  - How much can be kept out of the ‘public’ cloud?

Part II – Industry Thoughts

Security Concerns Permeate CENR Industries

Cybersecurity, physical security, and data protection are the top three security concerns across the CENR market.

Energy

- Intelligent grid
- Renewable energy (wind, solar)
- Energy efficiency (in-home displays)
- Smart metering

Utilities

- Smart metering
- Intelligent grid
- Info and comm technology (ICT)
- Mobile communications

Oil & Gas

- Web 2.0
- Data management
- Telepresence
- Virtual teaming
- Collaboration tools
- Remote connection
- Social networking

- Cybersecurity
- Identity mgt
- Network security
- Application security

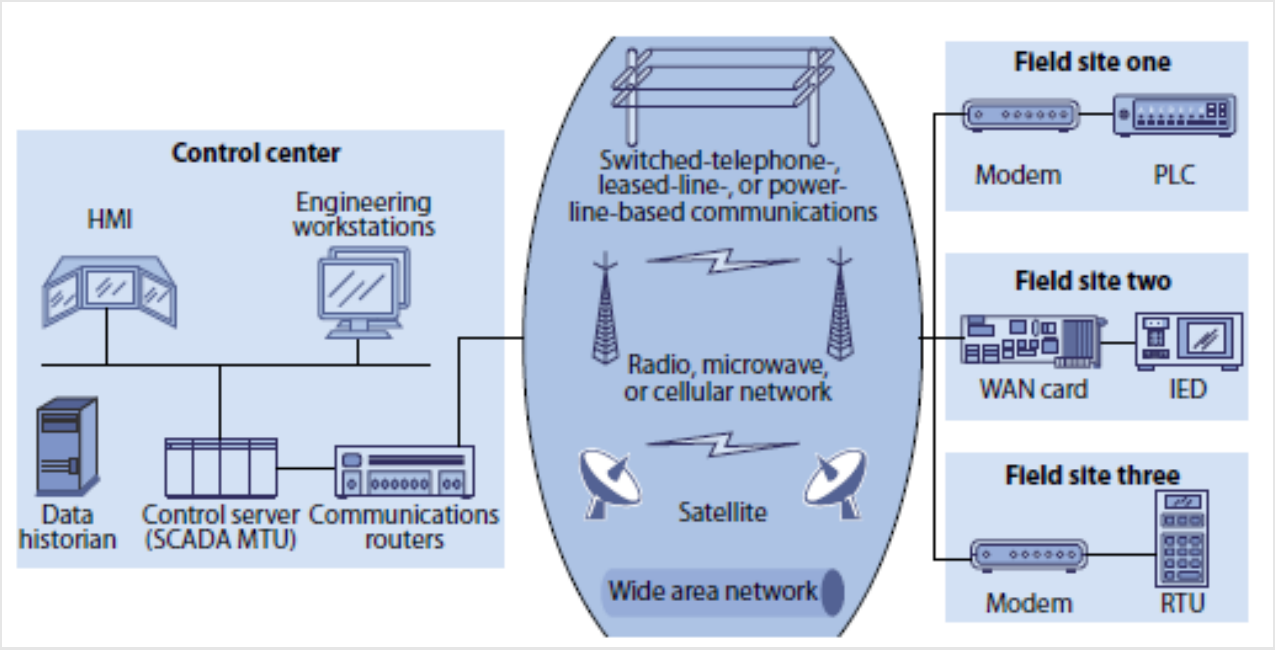
- Data leakage
- Comm infrastructure security
- Asset management

- Physical security
- Managed security
- RFID
- Access Control

SCADA—Energy, Utilities, Oil & Gas, Chemical Impact

Supervisory control and data acquisition (SCADA) systems—a computer system monitoring the controls and data are typically used across various CENR industries and involves security at every level.

SCADA example layout—security involved at every level



- Typical threats to the SCADA systems include—hackers, bot-network operators, spammers, spyware/malware, phishers, industrial spies, terrorists, and foreign intelligence services, employee's lack of adherence to established processes and procedures..
- All threats link massive concern for security and how to manage and control the breach.
- With the support of the NIST, a guide to industrial control systems security is currently being published.

Why are SCADA systems particularly vulnerable?

SCADA systems are more vulnerable to attack; the consequences to the business can be extreme

- SCADA systems have historically been stand-alone systems operated by the business, not IT; operator mindset is not steeped in the security discipline of classic IT
- SCADA systems are using more and more common system designs and protocols as corporate IT functions; more subject to larger population of potential hackers
- SCADA systems have now been integrated into business systems to provide real-time information for today's accelerated decision processes; making them mission-critical to the business
- SCADA systems are typically distributed physically and logically, allowing more opportunities for data interception, spoofing, and denial of service

A Recent Security Assessment of “Smart Meters”

CSC performed a recent assessment of Smart Meters that revealed some very interesting (and concerning) findings that are applicable to end-to-end SCADA systems security

- Hardware Security Module on NIC not functional yet
- Network Management Service does not provide accurate timestamp of events
- All devices use the same authentication credentials
- There are no “end of life” function to blank devices that are removed from service
- A stolen device could provide access to the network
- Physical tampering controls may be able to be bypassed, and cold tamper records only one event no matter how many occur
- Meter configuration data contains sensitive information
- One particular vendor model has a “denial of service” attack vulnerability

CENR Future Outlook

Data security and cybersecurity become top issues across all of CENR.

	2012 and Beyond	Forecasted Threat
Energy	• Proactive energy companies are rising to the challenge and will implement packaged applications to help manage carbon • Smart grid technology ignites • Intelligent grid technology advances	• Information security • Energy storage • Application software security used to operate the grid, software to manage grid data, and advanced energy storage security systems
Utilities	• Intelligent grid technology spending will reach $70 billion in 2013 • Utilities will place greater emphasis on distributed energy as a grid support tool • Web portals will be the fastest way to enable active consumer energy management • Self-powered RFID tags will emerge to detect information about assets and equipment • Smart metering increases (Google PowerMeter)	• Concerns and investments enhancing energy security and reliability • Access management (controls) will advance • Cybersecurity becomes eye-opening while Web 2.0 and social networking increases • Communication/identity protection • Hackers
Oil and Gas	• Data for carbon management will increase as companies respond to climate change • Climate change issues will drive increased investment in energy and information technologies • IT spending will increase at a greater-than-average rate	• Information security • Data loss protection becomes inevitable • Data management security • Identity and access management

Hardening Your SCADA Network:

Steps To Take Now…

- **Raise Awareness and Alertness to Threats**
  - Leadership must define responsibilities and hold people accountable
  - Security policies must be defined and clearly and frequently communicated
- **Isolate SCADA Networks**
  - Identify all connection and disconnect unnecessary links and services
  - Strengthen security of all remaining links
  - Limit or ban access by non-SCADA devices like laptops
- **Establish Proactive Security Management**
  - Define detailed security requirements
  - Work with system vendors to fully implement capabilities
  - Document system architecture to understand key data storage and protections
  - Have rigorous risk management and configuration management processes
  - Conduct routine audits, both internal and external
  - Review application development methods to ensure vulnerabilities are not being introduced
  - Have a disciplined backup and disaster recovery process

Secure SCADA Summit

THANK YOU

Dan Mintz

dmintz@csc.com

Twitter: technogeezer