Process Control Systems Forum

Self Assessment Development, Process, Standards, and Tools 2005 Spring Meeting

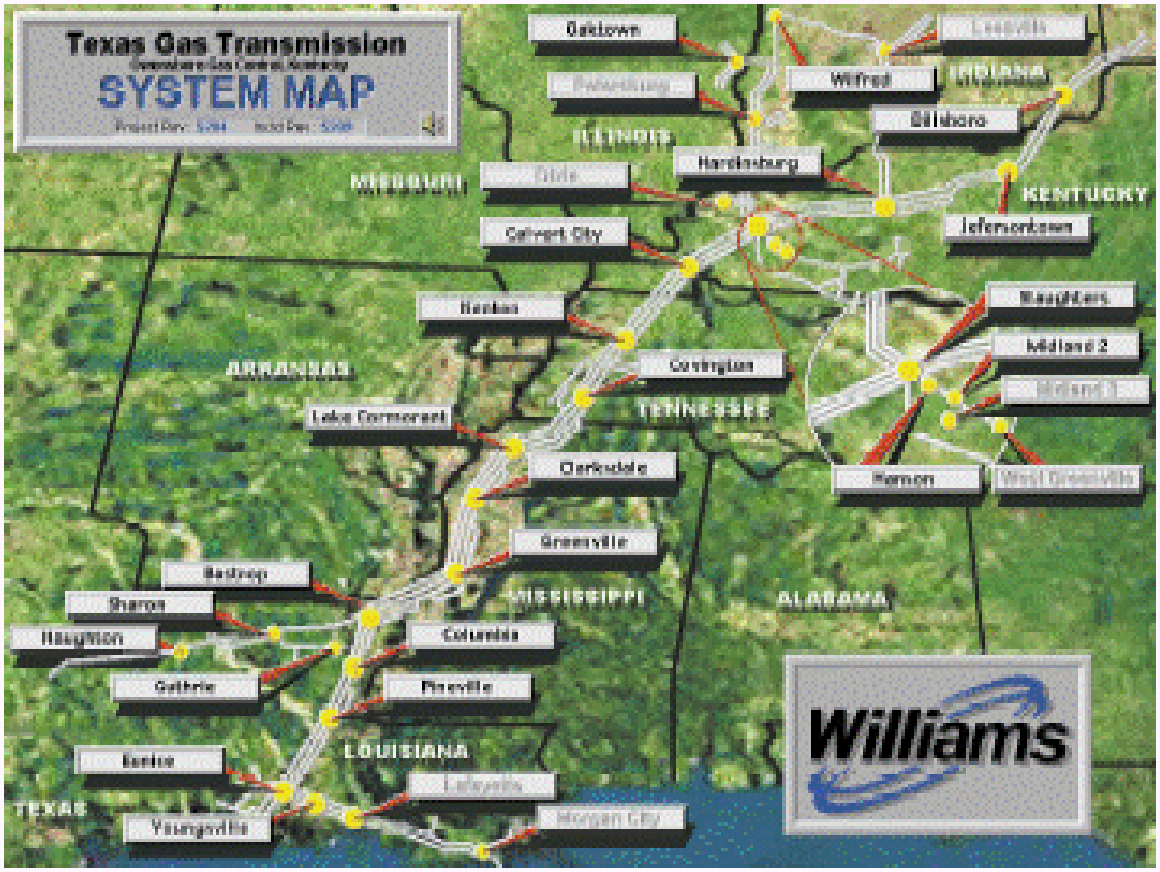
May 17 - 19, 2005

Brian Isle
brian.isle@adventiumlabs.org
www.adventiumlabs.org

Agenda

- Is the threat real?
- SCADA specific cyber issues
- Self Assessment Interest Group
- Discussion

SCADA is Critical to the Nation



Texas Gas pipeline system

- Citect SCADA
- 6,200 miles of pipe
- 26 compressor stations
- 7 states
- Monitor 68,480 control points
- 24/7 operations center

http://www.citect.com/__data/page/1806/Texas_Gas_Citect_Case_Study.pdf

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

Cyber Attacks Are Real

What does it take?

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

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

Self Assessment Interest Group

- **This I.G. will addresses and develop guidelines, methods, and tools for SCADA vulnerability assessment including the means and metrics to measure and compare cyber operational readiness both within and across systems as threats change.**
- **The output is envisioned to be directly applicable by SCADA end-users and as inputs to standards organizations.**

SCADA Users – "Know thyself"

Self Assessment IG - Plan Forward

- Form an IG – need active volunteers
- Refine the problem statement
- Define 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

Self Assessment IG - Questions

- Who are the players?
- Which standards and activities are relevant?
- What can we build on?
- Who do we need to recruit?
- What are the schedule drivers?
- Special needs of control systems?
- Common yard stick for assessing readiness?
- How to make an impact?

No reinventing wheels

Self Assessment IG – Scope?

- External threat? Internal threat?
- Linkage to physical vulnerability assessment?
- All SCADA systems and communication media?
- Training and roll-out of results to users?
- Characterization and measurement of the threat?

Discussion