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

October 27, 2005

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

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Agenda

- Rational for Cyber Requirements IG
- IG Charter
- Panel Discussion: SCADA cyber self assessments requirements
- Open Discussion
- Next steps

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

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

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 CYBER Self Assessment Working Group (SCySAG) - Charter

- Develop the <u>requirements for the SCADA cyber self assessment</u> 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.

Panel Discussion

Topic: Views on SCADA cyber self assessments requirements

- **Martin Stoddard, P.E.**
  PNL - Energy Science and Technology Directorate
  martin.stoddard@pnl.gov
- **Mark C. Morgen**
  3M - Optical Systems Division IT
  mark.morgen@mmm.com
- **Carol Muehrcke**
  Cyber Defense Agency, LLC
  cmuehrcke@cyberdefenseagency.com
- **Matt Earley**
  Decisive Analytics Corporation
  matt.earley@dac.us

SCySAG - Plan Forward

- Recruit active volunteers
- Finalize the charter
- Develop strategy to make an impact
- Get to work!

Move briskly, build on past, & complement other activities

Discussion