

Users Speak, II

Users Define Requirements for Manufacturers
– Audit, Measurement, Monitoring, and
Detection Tools, Computer Software, and
Physical Security Controls

John E. Allen
Ernst & Young
(602) 625-2044
john.allen@ey.com



Today's Objectives

- Provide a forum for users to identify what is needed from control systems vendors
- Organized around types of technologies useful to provide or improve control system security (based on technology types in TR99.00.01)

Discussion Topics this afternoon

- **Audit, Measurement, Monitoring, and Detection Tools**
Log auditing, malicious code and virus detection, intrusion detection, network vulnerability scanners, network forensics and analysis tools, host configuration management tools, automated software management tools
 - [SCADA Needs – Al Rivero, ChevronTexaco](#)
 - [Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks - Dale Peterson, Digital Bond, Inc.](#)

- **Computer Software**
Server and workstation operating systems, real time embedded operating systems, web and internet technologies
 - [Better OS coordination – Richard Eisenach, Chevron Phillips Chemical Co., LP](#)
 - [OPC Security: Controlling Access to Critical System Data – Sean Leonard, Matrikon](#)

- **Physical Security Controls**

Future vision ideas

- Give me every control system object such that:
 - Security functions are integrated and seamless
 - Every object can be secure and includes all these attributes, as routinely as controllers include setpoint, gain, and reset rate
 - Security is already a key design criteria that I don't need to add later
 - Security can be configured by the user
 - "Strong" security is enabled by default

Future vision ideas, continued

- Multiple security technologies are built in every object, to provide defense in depth to the level required by the user's configuration
 - Authentication and authorization can be required to send another object data or to use another object's data or to communicate with humans
 - All object's are capable of "strong" filtering, blocking, and access control for all communications with other network objects and humans
 - Any object's communications with other objects can be encrypted outside of it's physical boundaries (from transmitters to HMIs – any device on the control network)
 - All object's physical boundaries provide physical security or awareness of physical security
 - All objects provide for audit, measurement, monitoring, and detection



Discussion