



**DECISIVE
ANALYTICS**

Solutions For Success

*A Systems Engineering
Company Providing
Analytical Solutions To
Complex Problems*

Requirements for SCADA Cyber Security Self Assessment

Matt Earley

**Security Consultant
Decisive Analytics Corporation
matt.earley@dac.us**

Background

- **Process Control Security Exposure Self-Assessment Tool (Beta)**
 - **Technical Architect for the Water Environment Research Foundation (WERF)/Awwa RF 03-CTS-3SCO Research Project**
- **DHS Cyber Security Protection Framework (Draft)**
 - **National Cyber Security Division mission to reduce cyber security risk in control systems**
 - **Systematic methodology for assessing the cybersecurity posture of control systems**
 - **Self-assessment performed against a database of categorized security requirements (technical, management & operational)**

Requirement Categories

- **Generally the requirements fit into one of three categories:**
 - **Business requirements**
 - **Security requirements**
 - **Usability requirements**
- **Note: Scope of cyber security and the physical problem cannot be easily separated**
- **Note: The SCADA cyber security problem does not differ much from the general security domain**
 - **Or does it?**

Business Requirements

- **The need for a business case**
 - **Abstract threat versus specific threat (e.g. Y2K)**
 - **Return on Investment (ROI)**
 - **Fuelled by compliance requirements (?)**
- **Methodology must take a risk management approach**
 - **Must be clear linkage to business AND security risk**
- **Need to scope the problem**
 - **Prioritize the self assessment process according to critical assets**
 - **Business Impact Analysis**
 - **Primary assets versus Secondary assets**

Security Requirements

- **Technical Requirements**
 - **Access Control**
 - **Data Authentication**
 - **Boundary Protection**
- **Management Requirements**
 - **Security Policy & Organization**
- **Operational Requirements**
 - **Security Procedures**
- **Cross-cutting Requirements**
 - **Many of the above apply to all components within the system e.g. Security Policy, Configuration Management, Audit, etc**

Usability Requirements

- **Process control network boundary/definition**
 - **Distributed systems**
 - **Interconnections with corporate network, 3rd parties, etc**
 - **Supporting operational systems e.g. LIMS, CMMS**
 - **Difficult to define (!)**
- **Terminology**
 - **Differ even amongst similar industry sectors**
- **Ease of Use & Delivery**
 - **KISS**
- **Compatibility**
 - **Existing standards and methodologies**
 - **No need to re-invent the wheel (!)**