

Requirements for Effective SCADA Cyber Self-Assessment

**Dr. Carol Muehrcke
Cyber Defense Agency LLC**



**PROCESS CONTROL
SYSTEMS FORUM**

Collaborating to Advance Control System Security

Categories of Requirements

- ◆ **Output**
- ◆ **Scope**
- ◆ **Approach**
- ◆ ...

Risk Assessment Output

◆ Identifies Risks

- Feasible *attacks*
- Consequences *in terms of business mission*

◆ Assesses Risks

- Priority ordering or grouping of feasible attacks
- *Vulnerabilities* that underlie attack feasibility
- Analysis of cost and other impacts of solutions, vs. attack consequences

Scope of Risk Assessment Analysis

- ◆ **Considers all interfaces to SCADA systems**
- ◆ **Considers insider and outsider attacks**
- ◆ **Supports broader risk assessment**
 - Considers hybrid physical/cyber attacks
 - Considers impact of related administrative processes such as password management
- ◆ **Identification of possible solutions is process input**

Complimentary Analysis Approaches

● Bottom up, defender viewpoint

- Address checklist of typical vulnerabilities
- Solves an (unknown) percentage of the problem
- Raises the bar over time via best practices
- Checklist must evolve over time
- Sources for evolution:
 - Actual attacks
 - Taking the adversary viewpoint

● Top down, adversary viewpoint

- Postulate attacks based on list of adversaries and their objectives
- Addresses attacks and business consequences unique to each organization
- Addresses problem of “failure of imagination”