

Common Security Requirement Language for Procurements & Maintenance Contracts

Julio Rodriguez – Idaho National Laboratory

National Cyber Security Division (NCSD)

Control Systems Security Program (CSSP)

December 8, 2006



**Homeland
Security**

1

Background

Contributors:

- *Department of Homeland Security National Cyber Security Division*
- *New York State (Will Pelgrin – CSCIC)*
- *SANS (Alan Paller - Director of Research)*
- *Idaho National Laboratory (Michael Assante - Strategic Lead)*

Project Website:

<http://www.msisac.org/scada/>



**Homeland
Security**

2

Risk Reduction
Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks

Software Assurance
A Strategic Initiative to Promote Integrity, Security, and Reliability in Software

Procurement Specification for Control Systems
Initiative to develop procurement language for control systems (hardware and software)

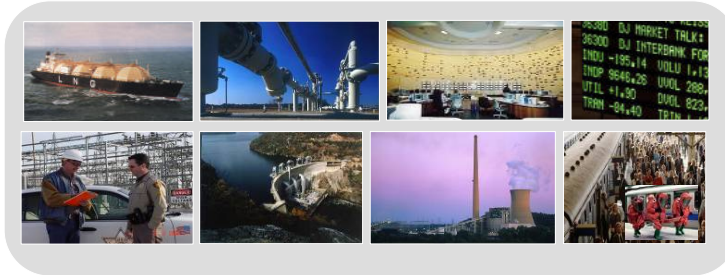


Homeland Security

3

Control System Security Project

Providing owner & operators more secure systems...



... to manage the risk & head off tomorrow's legacy problem

- ▶ Asset owner driven with participation from all stakeholders (100+ team members)
- ▶ Launched at the SANS SCADA Summit in Orlando in March
- ▶ Will provide a specific deliverable to buyers & operators ("Asset Owners")
 - Common security requirement language for procurements & maintenance contracts
 - Designed as a "Tool Kit" or desk reference



Homeland Security

4

Project Goal & Scope

The Goal

Develop common procurement requirements and contractual language that the owners can use to ensure control systems they are buying or maintaining have the best available security

Scope of the project

- ▶ *New control systems*
- ▶ *Maintenance of systems*
- ▶ *Legacy systems*
- ▶ *Information and personnel security*



**Homeland
Security**

5

SCADA Procurement Objectives

Deliverables:

- ▶ *Initial Focus – April 2006 – Completed*
- ▶ *Develop a straw Document – May 2006 – Completed*
- ▶ *Identify Critical Components (opportunities for immediate progress) – May 2006 – Completed*
- ▶ *Publish Security Specification for Key Components of Control Systems – June 2006 – Completed*
 - *Including but not Limited to:*
 - *Lock down services*
 - *Patch management services*
 - *Vulnerability scans*
 - *Code reviews*



**Homeland
Security**

6

SCADA Procurement Objectives (Cont.)

Deliverables:

- ▶ *Created link on MS-ISAC Website for Publishing Deliverables*
 - *June 2006 – Completed*

<http://www.msisac.org/scada/>
- ▶ *Develop a procurement and Maintenance desk reference*
 - *DRAFT Version 1.5 is posted. Additional topics and comments continue to be incorporated*
- ▶ *Solicit State and Local Governments – in process*
 - *Identify which Entities will Participate in an Aggregate Procurement – in process*



Homeland
Security

7

SCADA Procurement Objectives (Cont.)

Guiding Principles:

- ▶ *Collaboration*
- ▶ *Everyone at the table*
- ▶ *Owners, regulators, vendors*




Win-Win



Homeland
Security

8

The Time is Right for this Action

- 98  ► **Risks being characterized & understood**
- Demonstrations & validation of risks
 - Education & awareness activities
 - Development of tools to understand the problem
 - Identifying requirements to better manage the risk
- 05  ► **“Turning the corner” moving towards risk management**
- Standards development across some industries
 - Solution exploration / limited development
 - Vulnerabilities & risks are becoming better understood
- 06  ► **Organizing & working to deliver/manage more secure systems**
- Procurement & maintenance project launched
 - Stakeholders coming together “to act”
 - Leveraging our combined knowledge



**Homeland
Security**

9

Control Systems Procurement Cycle

	Request for Proposal	Proposal Submittal	Bid Review	Contract Award	Statement of Work (SOW)	Design Review	Document Review	Factory Acceptance Test (FAT)	Site Acceptance Test (SAT)
Asset Owner	X		X	X	X	X	X	X	X
Consultant	X		X		X			*	*
Vendor / Integrator		X		X	X	X	X	X	X

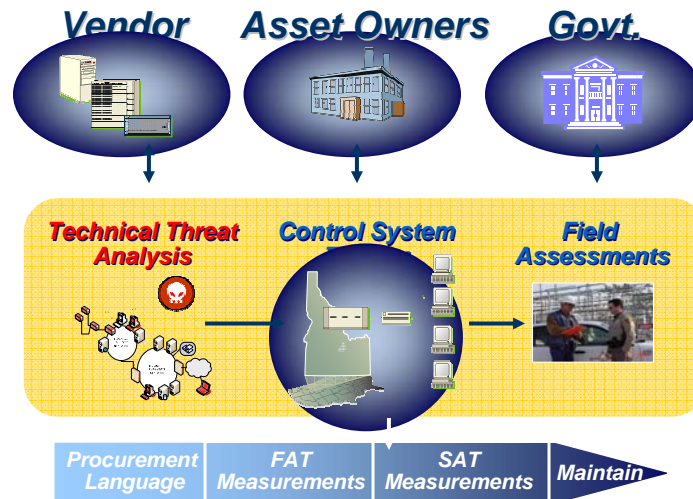
* Occasionally participate



**Homeland
Security**

10

Working Together to Deliver & Operate Secure Systems



Homeland
Security

11

Procurement Language

- ▶ *Aggressive project designed to provide a “buyers” tool kit*
- ▶ *Provide security requirements for inclusion into RFPs*
- ▶ *Use common, grounded and valuable language*
- ▶ *Support Bid Reviews (gauge responsiveness)*
- ▶ *Provide the detailed required to support SOW development and Design Creation & Review*
- ▶ *Starting with greatest risk that can be addressed*



Homeland
Security

12

Factory Acceptance Test Measurements

- ▶ *Linked to the procurement requirement*
- ▶ *Provides language to include in Factory Acceptance Testing requirements and specifications*
- ▶ *Designed to validate the requirement has been met*
- ▶ *Allows for rigorous security testing in an isolated environment*
- ▶ *Gives the vendor the opportunity to verify the product meets the security requirements prior to installation in the field.*



Homeland
Security

13

Site Acceptance Test Measurements

- ▶ *Linked to the procurement requirement*
- ▶ *Provides language to include in Site Acceptance Testing requirements and specifications*
- ▶ *Designed to validate the risk reducing requirement is not lost during implementation in the Asset Owners environment*
- ▶ *Important step that requires an understanding of “why it was delivered that way”*
- ▶ *First hand-off from the procurement / provider team to the actual operator and maintainer*



Homeland
Security

14

- ▶ *Linked to the procurement requirement*
- ▶ *Provides language to include in maintenance contracts*
- ▶ *Designed to further reduce the risk to control systems during their life-time*
- ▶ *Critical step to ensure the benefits of the security requirements are not lost during the technologies operational lifespan*
- ▶ *Requires an understanding of “why it was delivered that way”*



Homeland Security

15

Project Risk Reduction Scheme



Homeland Security

16

Security Areas Covered

- ▶ *System Hardening*
- ▶ *Perimeter Protection*
- ▶ *Account Management*
- ▶ *Coding Practices*
- ▶ *Flaw Remediation*
- ▶ *Malware Detection and Protection*
- ▶ *Host Name Resolution*



**Homeland
Security**

17

Future Topics

- ▶ *Configuration management*
- ▶ *Recovery and backup*
- ▶ *Disaster recovery*
- ▶ *Wireless networks and communications*
- ▶ *End network devices*
- ▶ *Lifecycle issues*
- ▶ *System integration*
- ▶ *Logging and auditing*
- ▶ *Training*



**Homeland
Security**

18

Future Topics (Cont.)

- ▶ *Least privilege*
- ▶ *Enumeration*
- ▶ *Physical access*
- ▶ *Contract services*
- ▶ *Redundancy*
- ▶ *Policies and procedures*
- ▶ *Network partitioning*
- ▶ *Remote access*



Homeland
Security

19

A Page From the Tool Kit: Format

- ▶ *Procurement Topic*
- ▶ *Security Risk or Basis Description*
- ▶ *Procurement Language*
- ▶ *Language Guidance*
- ▶ *Factory Acceptance Test Measurements*
- ▶ *Site Acceptance Test Measurements*
- ▶ *Maintenance and Operations Guidance*
- ▶ *References or Standards*
- ▶ *Dependencies*



Homeland
Security

20

Page from the Tool Kit : Example (1 of 2)

Changes to File System and OS Permission

2.3.1 Basis

Configurations for out-of-the-box OS and file systems normally are more permissive than necessary.

2.3.2 Procurement Language

The vendor shall provide hosts with least privilege file and account access. Necessary system services shall be configured to execute at the least user privilege level possible for that service.

2.3.3 Language Guidance

In many cases, operating systems ship with default configurations that allow unneeded access to files, and loose configuration parameters that can be exploited in order to gain information for further attacks. Common examples include OS recovery procedures, elevated-permission user or system accounts, diagnostic tools, remote access tools, and direct access to network device addresses.

Hardening tasks include changing or disabling access to such files and functions.



**Homeland
Security**

21

Page from the Tool Kit : Example (2 of 2)

2.3.4 FAT Measures

FAT procedures shall include validation and documentation of the permissions assigned.

2.3.5 SAT Measures

SAT procedures shall include validation and documentation of the permissions assigned.

2.3.6 Maintenance Guidance

Anytime the system is upgraded, it is recommended that system vendors reassess permissions and security settings on their baseline system before delivery to asset owners. The above warrant is valid for the duration of the warranty and maintenance agreement period.

2.3.7 References

CIP-0071-1 R5.2

ISA-99.02: 5.3, B.14, C.3.

2.3.8 Dependencies

Section 4.1



**Homeland
Security**

22

Path Forward

- ▶ *Draft 1.5 released November, 2006 (Completed)*
- ▶ *Incorporate comments to Draft 1.5*
- ▶ *Create Industry specific sample templates*
- ▶ *Develop a topic matrix based on sector specific control system designs*
- ▶ *Continuation of the New York focus group website and volunteer group will develop additional topics for all stakeholders to use*
- ▶ *Finished Control Systems Procurement Language document*



**Homeland
Security**

23

Questions?

Contact information:

National Cyber Security Division

Julio Rodriguez, CSSP

Julio.Rodriguez@associates.dhs.gov



**Homeland
Security**

24



Homeland Security