PARSONS

Optimizing IT in MILCON contracting

Cybersecurity Perspective

Juan Espinosa, P.E., PMP,GICSP

Parsons-Critical Infrastructure Cyber Security

delivering a better world

Agenda

- Current Standards/Guidance
- Why is this important
- Gap/Current experiences
- Existing Specifications
- Recommendations

Current Guidance

UFC 4-010-06
19 September 2016
Change 1, 18 January 2017

CHAPTER 3 APPLYING CYBERSECURITY IN DESIGN

3-1 OVERVIEW.

The design of cybersecurity for facility-related control systems is a five step process. In some cases a specific step may be performed by someone other than the designer, but may still require input from the designer. Documentation of cybersecurity-related design decisions and input to others is described in CHAPTER 5.

In addition to requirements specific to Control Correlation Identifier (CCIs), design all control systems according to the minimum cybersecurity design requirements in CHAPTER 4 and cybersecurity requirements otherwise standard for the type of control system being designed.

3-1.1 Five Steps for Cybersecurity Design.

The five steps for cybersecurity design are:

Step 1: Based on the organizational mission and details of the control system, the System Owner (SO) and Authorizing Official (AO) determine the Confidentiality, Integrity, and Availability (C-I-A) impact levels (LOW, MODERATE, or HIGH) for the control system.

Step 2: Use the impact levels to select the proper list of controls from NIST SP 800-82.

Step 3: Using the DoD master Control Correlation Identifier (CCI) list, create a list of relevant CCIs based on the controls selected in Step 2.

Step 4: Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.

Step 5: Include cybersecurity requirements in the project specifications and provide input to others as required.

APPENDIX H contains tables covering steps 2 – 4 for LOW and MODERATE systems, assuming the existence of a Platform Enclave. These tables, with additional information in a filterable format, are also available in Excel format on the RMF Knowledge Service (https://rmfks.osd.mil). This website is CAC-enabled; designers without a CAC must request assistance from the Service if tables and information were not provided. 0 provides additional guidance on the implementation of specific controls.

3-1.2 Definition of "Organization".

Security controls often refer to the "organization" in identifying responsibilities and risk. Unless otherwise indicated, for the purposes of implementation of the RMF to control systems:

9

UNIFIED FACILITIES CRITERIA (UFC)

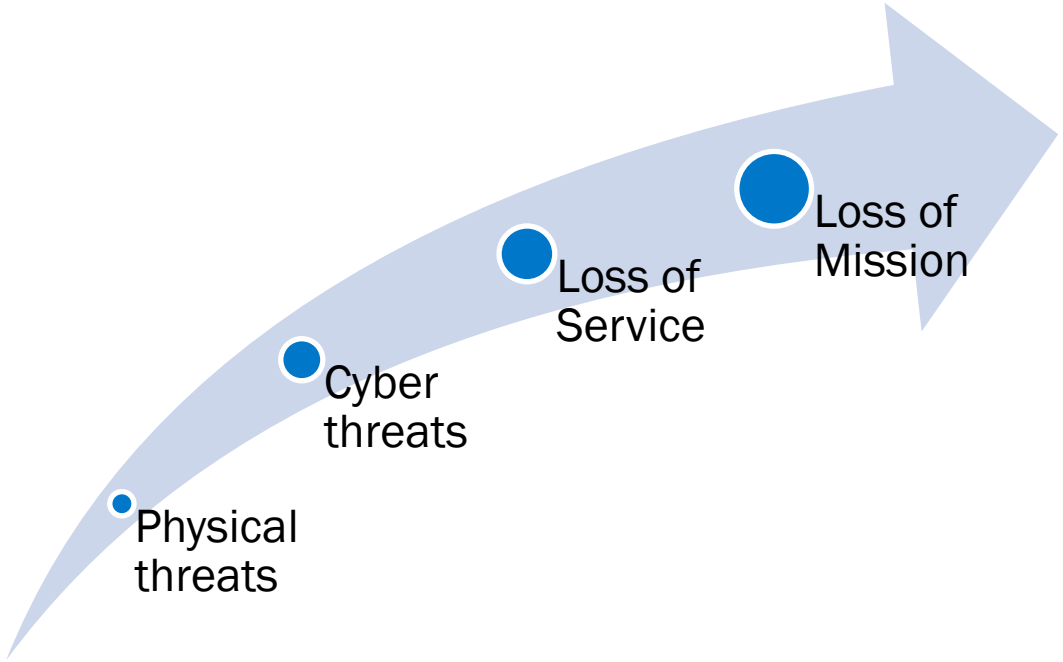
CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Step 5: Include cybersecurity requirements in the project specifications and provide input to others

Why is this Important?

Evolution of ICS



Network connectivity is the main threat to ICS

Gap/Current experiences

- Is your critical infrastructure supported by a robust IT infrastructure?
- Was it installed based on project specifications?
- NIST is a guidance not a specification

Current UFC Specifications

****
USACE / NAVFAC / AFCEC / NASA UFGS-25 10 10 (February 2019)

Preparing Activity: USACE Superseding
UFGS-25 10 10 (November 2015)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated April 2019
****

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 10 10

UTILITY MONITORING AND CONTROL SYSTEM (UMCS) FRONT END AND INTEGRATION

02/19

****
USACE / NAVFAC / AFCEC / NASA UFGS-25 05 11 (November 2017)

Preparing Activity: USACE

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated April 2019
****

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

11/17

Current Specifications really do not include software and ICS network specific requirements.

Typical IT requirements

- Active Directory implemented-every user has a unique ID, and privileged users have separate credentials and use proper escalation procedures
- Centrally managed industrial grade switches (ability to push security patches)
- Use of fiber instead of copper when infrastructure leaves buildings/dual communication paths
- Separation of networks (Physical and or Logical)
- LVANs & Firewalls

Recommendations

Optimizing IT in MILCON contracting

Cybersecurity Perspective

- Generate a UFC ICS IT specification
- Include requirements for Hardware, Network Devices, UPSs and Software specific for ICS
- Leverage developments in other organizations (i.e. Intelligence Community)