FRCS CYBERSECURITY IN MILCON

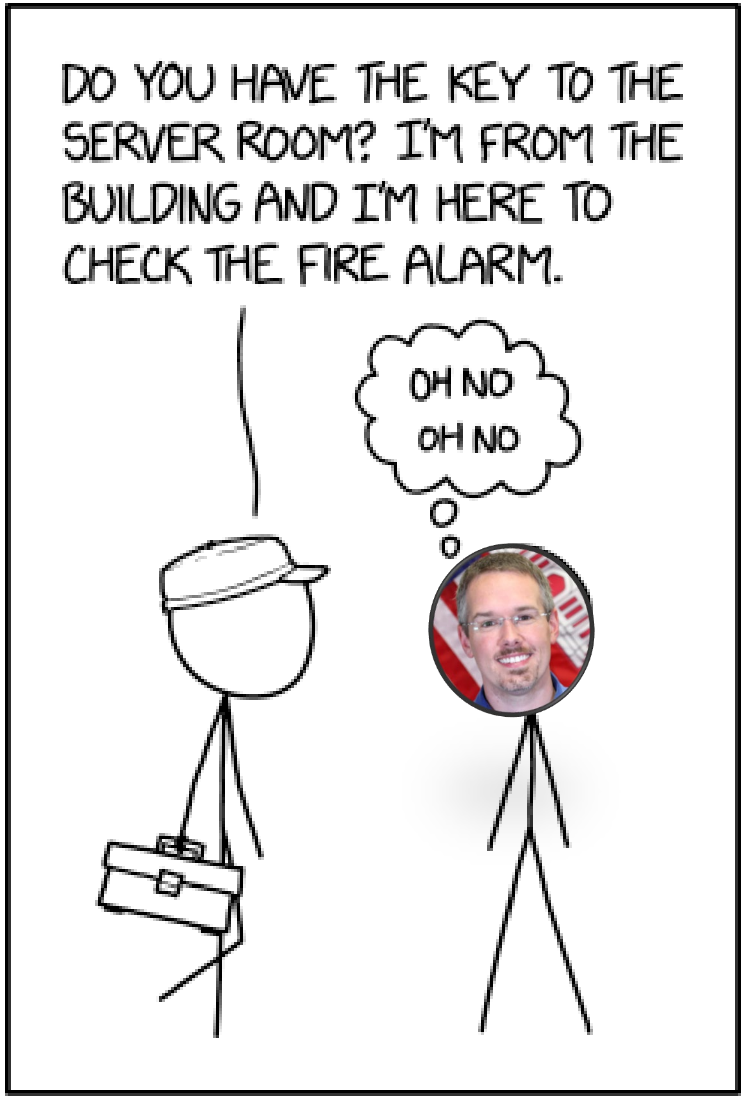
14 DEC 2023

(Facility Related Control System Cybersecurity in Military Construction)

Elliot McConnell

Control System Cybersecurity Mandatory Center of Expertise
U.S. Army Corps of Engineers

Email: elliot.j.mcconnell@usace.army.mil


DO YOU HAVE THE KEY TO THE SERVER ROOM? I'M FROM THE BUILDING AND I'M HERE TO CHECK THE FIRE ALARM.
OH NO OH NO

THANKS TO MOVIES, WHENEVER ANYONE ASKS ME TO OPEN ANY DOOR, I IMMEDIATELY ASSUME I'M A MINOR CHARACTER IN A HEIST.

Image adapted from "Heist" by Randall Munroe
Used under CC 2.5 License https://xkcd.com/2077/

BLUF (BOTTOM LINE UP FRONT)

1. Cybersecurity is an aspect of the project, not the primary objective.*
   **This does not imply that it is unnecessary or unimportant!*

2. I don’t care if it’s “standalone”, “cyber” is required.

3. Our goal [in construction] is meeting defined technical requirements, not “get an ATO.”

THIS TALK IS ABOUT:

1. Goals of Cybersecurity in DoD FRCS Construction

2. DoD FRCS Cybersecurity Construction Guidelines
   - Design Requirements and Expectations
   - Key Construction Submittals

BIG PICTURE

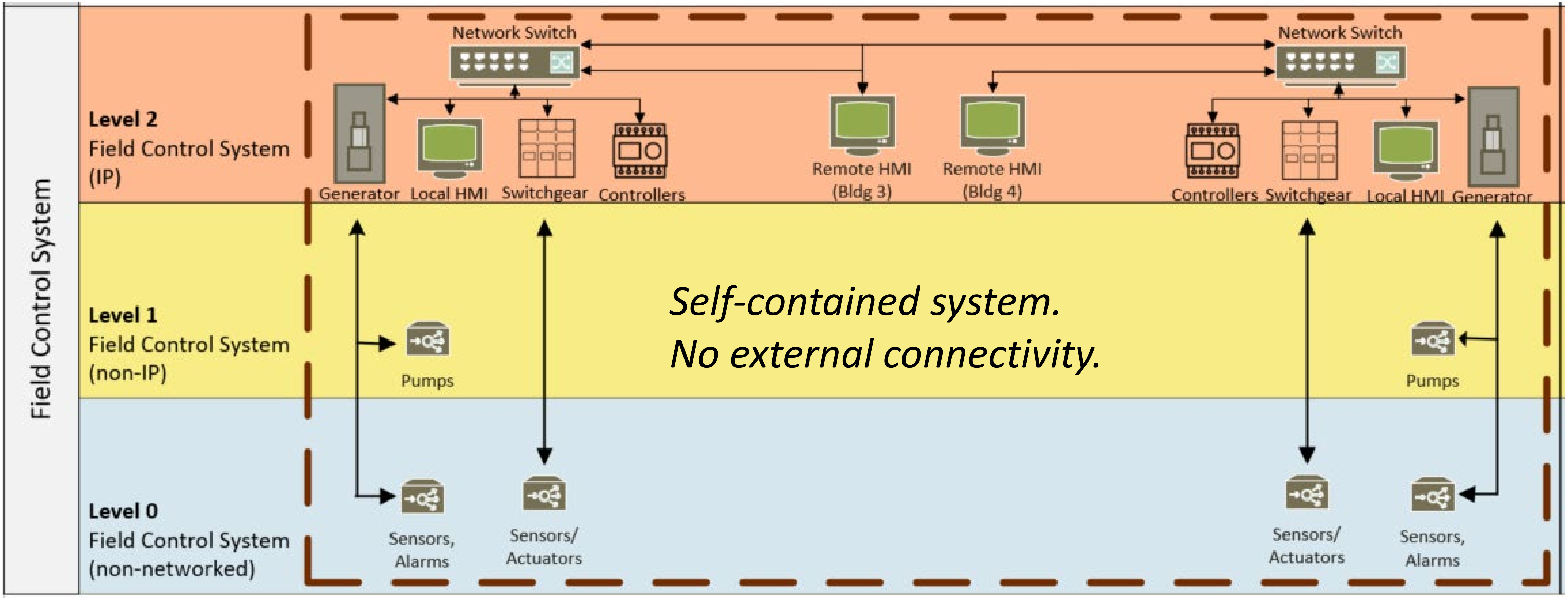
1. Buildings have Control Systems. 🙂
2. Control Systems have vulnerabilities. 😐
3. Threats + Vulnerabilities = Risk. 😈
4. Risks can impact mission. 😮
5. Cybersecurity helps reduce risk. 🙂

BIG PICTURE

5. Risk Management Framework (RMF) seeks an acceptable level of risk. 🙂
6. RMF has both Technical requirements and Policy/Procedural requirements. 😐
7. An Authority to Operate (ATO) means someone has accepted that risk. 😎
8. All systems must obtain an ATO. 🥺

BUT MY SYSTEM IS "STANDALONE"...

(or "air-gapped" or "isolated" or "a closed-network")



Self-contained system.

No external connectivity.

BIG PICTURE

9. Responsibility lies with System Owner (RMF/ATO, funding, staffing). 😐
10. Contractors deliver and sustain systems and are technical experts. 🙂

GOALS IN DOD Control System DESIGN/CONSTRUCTION:

#1: Meet the functional requirements.

- Requirements should be driven by the mission.
  - Example: If the mission doesn’t need a redundant system, the cybersecurity controls shouldn’t prescribe one.
- Keep it simple.
  - If you can meet the requirements without a “smart system”, do so.
  - We can’t afford to secure and continuously monitor unnecessary systems.

GOALS IN DOD Control System DESIGN/CONSTRUCTION:

#2: Provide a secured/hardened system.

- Goal **IS NOT** to get an ATO (Authority to Operate)

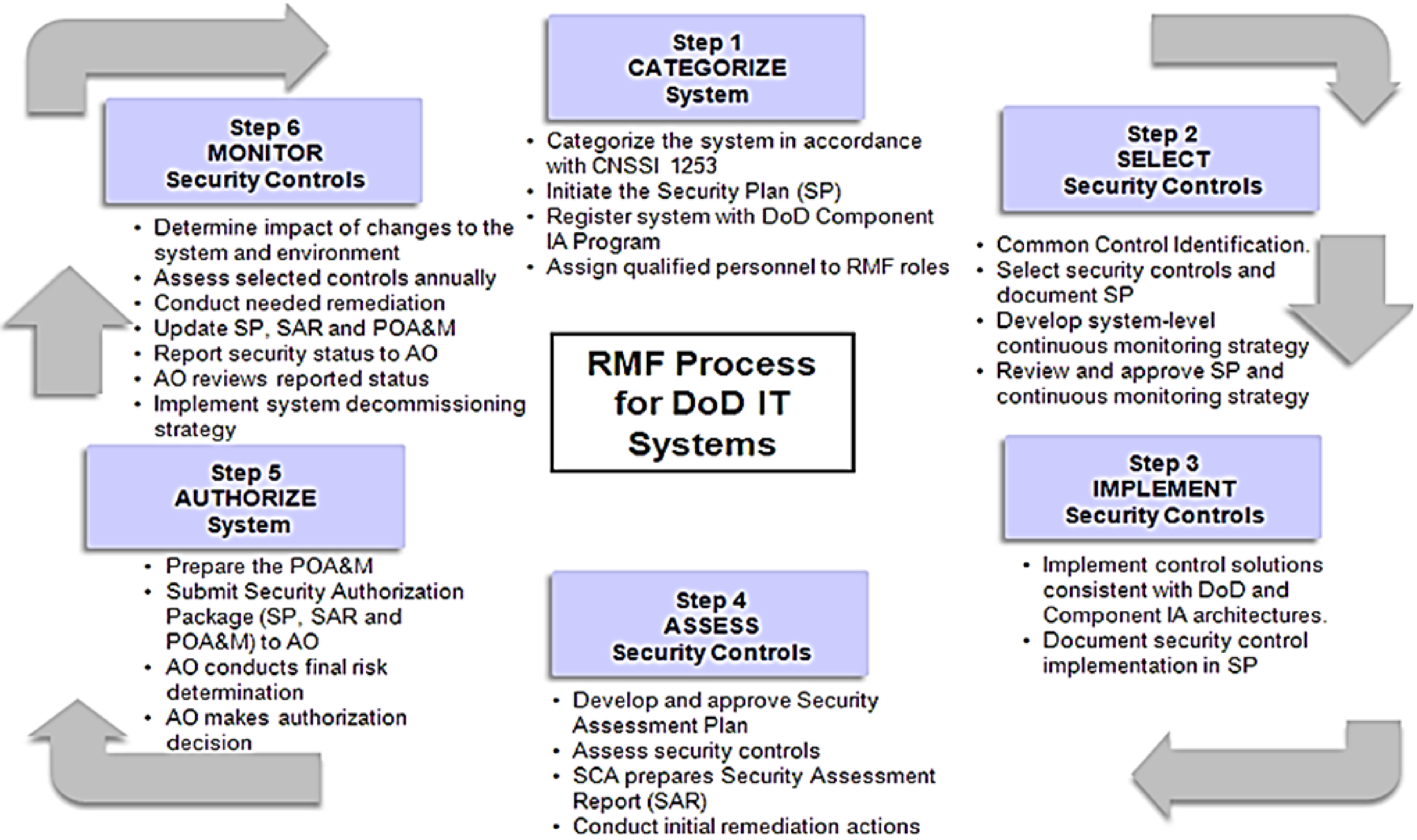
- Goal **IS** to provide a secured system with supporting documentation so that the system is technically capable of receiving an ATO without the need for reconfiguration.

WHY NOT INCLUDE AN ATO IN THE CONTRACT SCOPE?

- Contractor CANNOT guarantee or independently deliver.
- Contractor cannot implement organizational policy.
- Huge dependencies on System Owner, ISSM
- Huge dependencies on the Authorizing Official (AO) chain.
- AO chains are overtasked, understaffed, and backlogged.

Unmet Expectations, Inability to Closeout Contract

RISK MANAGEMENT FRAMEWORK (RMF)



RMF Process for DoD IT Systems

Step 1 CATEGORIZE System

- Categorize the system in accordance with CNSSI 1253
- Initiate the Security Plan (SP)
- Register system with DoD Component IA Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification.
- Select security controls and document SP
- Develop system-level continuous monitoring strategy
- Review and approve SP and continuous monitoring strategy

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD and Component IA architectures.
- Document security control implementation in SP

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

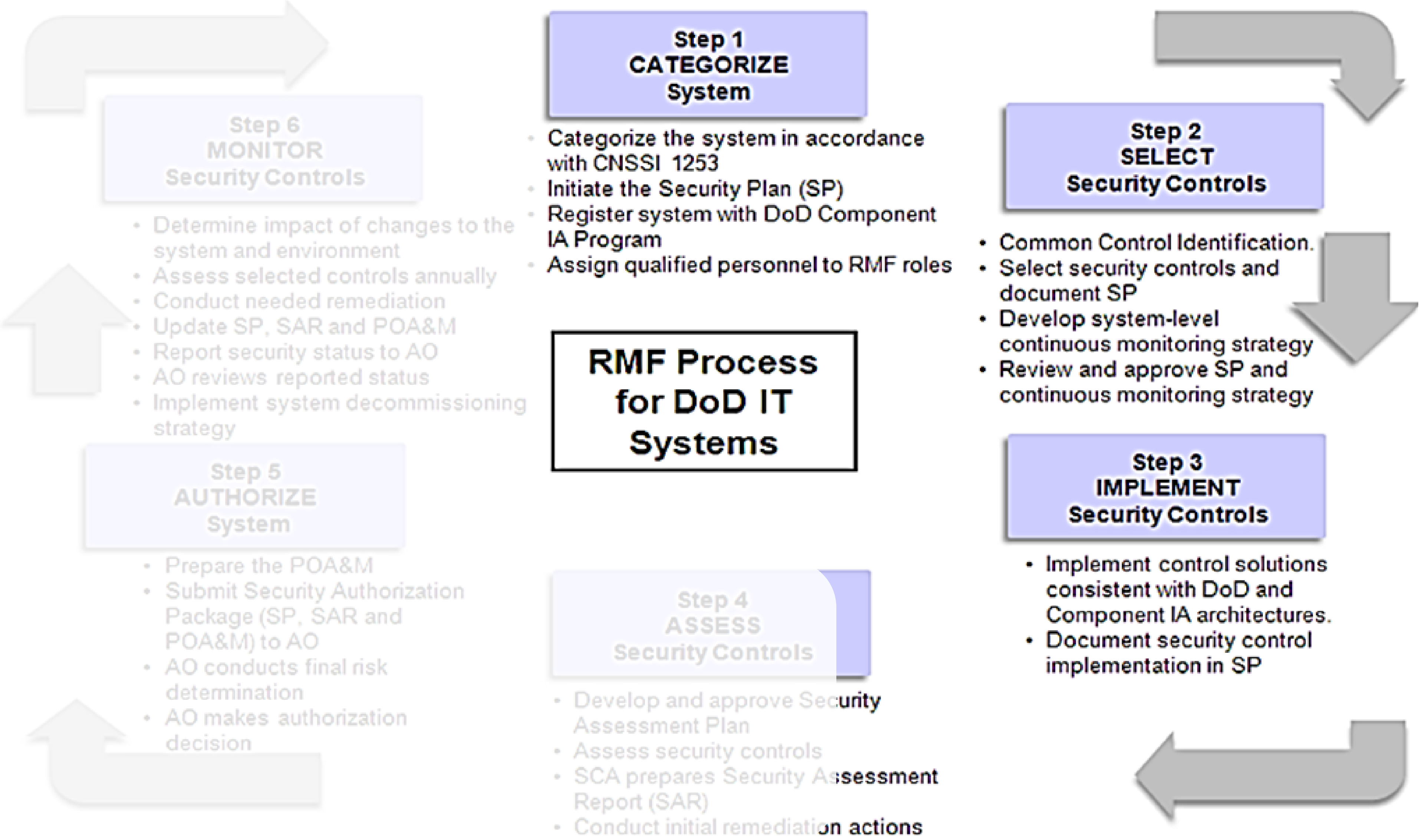
Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (SP, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update SP, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RISK MANAGEMENT FRAMEWORK (RMF)



Step 1 CATEGORIZE System

- Categorize the system in accordance with CNSSI 1253
- Initiate the Security Plan (SP)
- Register system with DoD Component IA Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification.
- Select security controls and document SP
- Develop system-level continuous monitoring strategy
- Review and approve SP and continuous monitoring strategy

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD and Component IA architectures.
- Document security control implementation in SP

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (SP, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

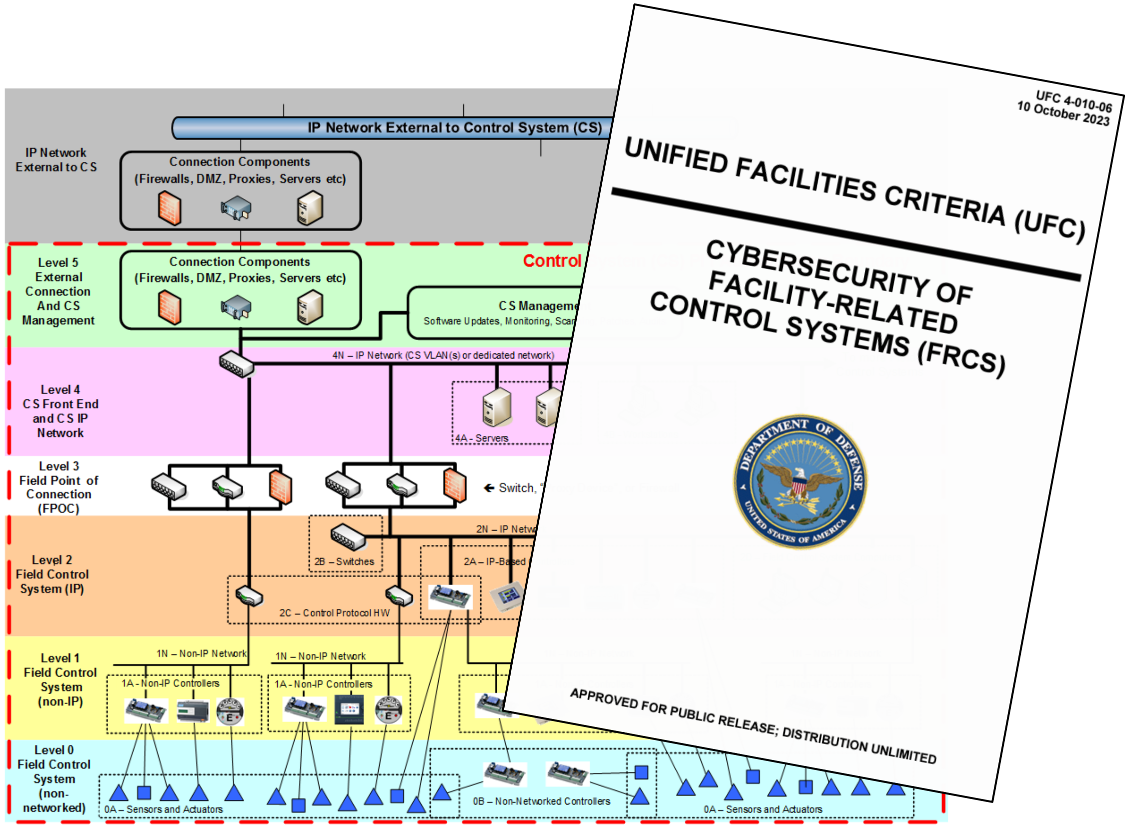
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update SP, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF Process for DoD IT Systems

DOD FRCS CYBERSECURITY CONSTRUCTION GUIDELINES

UFC 4-010-06

- Theory/Concept/Framework
- Minimum requirements:
  - Minimize Network Dependency
  - Reduce Extraneous Functionality
  - Design for Graceful Failure
  - No "IT" functions (VoIP, internet, etc.)
  - No Remote Access


IP Network External to Control System (CS)
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control
CS Management
Software Updates, Monitoring, Scan
4N – IP Network (CS VLAN(s) or dedicated network)
Level 4 CS Front End and CS IP Network
4A - Servers
Level 3 Field Point of Connection (FPOC)
Switch,
Level 2 Field Control System (IP)
2B – Switches
2N – IP Netw
2A – IP-Based
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1N – Non-IP Network
1A - Non-IP Controllers
1A – Non-IP Controllers
Level 0 Field Control System (non-networked)
0A – Sensors and Actuators
0B – Non-Networked Controllers
0A – Sensors and Actuators

UFC 4-010-06
10 October 2023

UNIFIED FACILITIES CRITERIA (UFC)

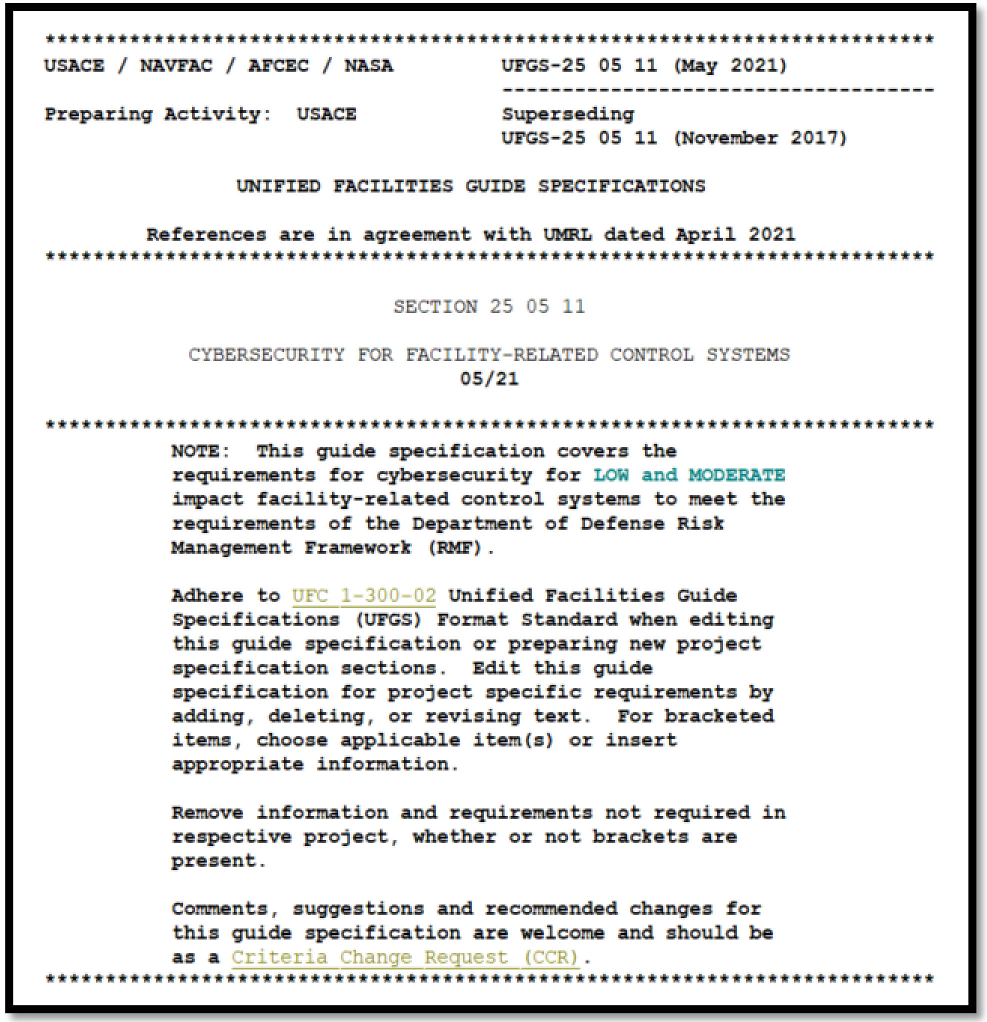
CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS (FRCS)

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

DOD FRCS CYBERSECURITY CONSTRUCTION GUIDELINES

UFGS 25 05 11

- Must be tailored to the system!
- Built on the tailored CCI list.
- Tailoring options available:
  - Low/Moderate
  - Fire/ESS/HVAC/Lighting
  - Army/Air Force

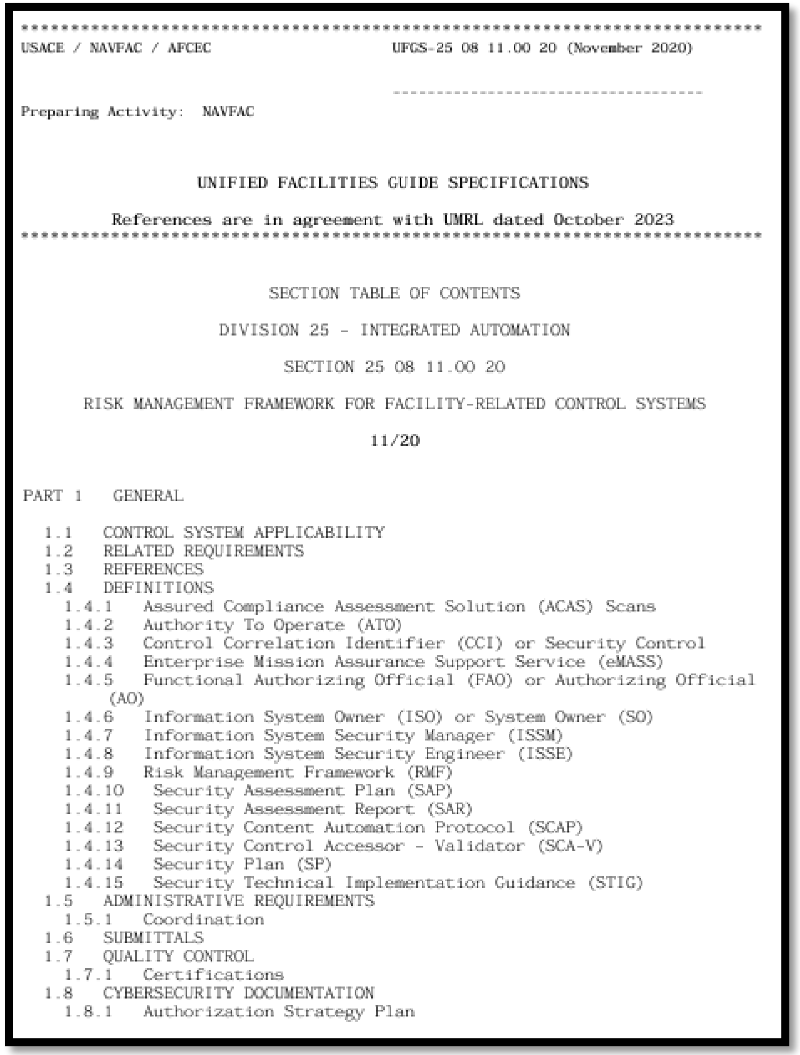


```
**************************************************************************
USACE / NAVFAC / AFCEC / NASA            UFGS-25 05 11 (May 2021)
                                         ------------------------------------
Preparing Activity:  USACE               Superseding
                                         UFGS-25 05 11 (November 2017)

                   UNIFIED FACILITIES GUIDE SPECIFICATIONS

          References are in agreement with UMRL dated April 2021
**************************************************************************

                             SECTION 25 05 11

               CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
                                   05/21

**************************************************************************
           NOTE:  This guide specification covers the
           requirements for cybersecurity for LOW and MODERATE
           impact facility-related control systems to meet the
           requirements of the Department of Defense Risk
           Management Framework (RMF).

           Adhere to UFC 1-300-02 Unified Facilities Guide
           Specifications (UFGS) Format Standard when editing
           this guide specification or preparing new project
           specification sections.  Edit this guide
           specification for project specific requirements by
           adding, deleting, or revising text.  For bracketed
           items, choose applicable item(s) or insert
           appropriate information.

           Remove information and requirements not required in
           respective project, whether or not brackets are
           present.

           Comments, suggestions and recommended changes for
           this guide specification are welcome and should be
           as a Criteria Change Request (CCR).
**************************************************************************
```

DOD FRCS CYBERSECURITY CONSTRUCTION GUIDELINES

UFGS 25 08 11.00 20

- Navy-Specific (NAVFAC)
- Used in conjunction with 25 05 11
- Additional RMF requirements
- Limited Use



```
**************************************************************************
USACE / NAVFAC / AFCEC                    UFGS-25 08 11.00 20 (November 2020)
                                          -----------------------------------
Preparing Activity:  NAVFAC

                UNIFIED FACILITIES GUIDE SPECIFICATIONS

         References are in agreement with UMRL dated October 2023
**************************************************************************

                       SECTION TABLE OF CONTENTS

                  DIVISION 25 - INTEGRATED AUTOMATION

                        SECTION 25 08 11.00 20

   RISK MANAGEMENT FRAMEWORK FOR FACILITY-RELATED CONTROL SYSTEMS

                                 11/20
```

DESIGN REQUIREMENTS & EXPECTATIONS

Step 1: Determine the System's Impact Rating [Categorization]

Cybersecurity: Practices designed to protect the **confidentiality**, **integrity,** and **availability** of information systems and data.

C-I-A (aka "Impact Rating")

L-M-H (Low – Moderate – High)

DESIGN REQUIREMENTS & EXPECTATIONS

Step 1: Determine the System’s Impact Rating [Categorization]

- This is the customer’s responsibility!
  - Ideally, this is defined during the 1391 development.
  - If a rating is not provided [for each system], submit an RFI.
  - If they fail to respond, document that in the Design Analysis (DA) and make an assumption.
  - Each system’s impact rating and how it was obtained should be documented in the DA.

Note:

If you’re modifying an existing system, there is a [small, but growing] chance that an ATO exists for that system. If so, then there will be an already approved Impact Rating. May need to discuss with the customer whether the project will significantly change the system or its impact on mission.

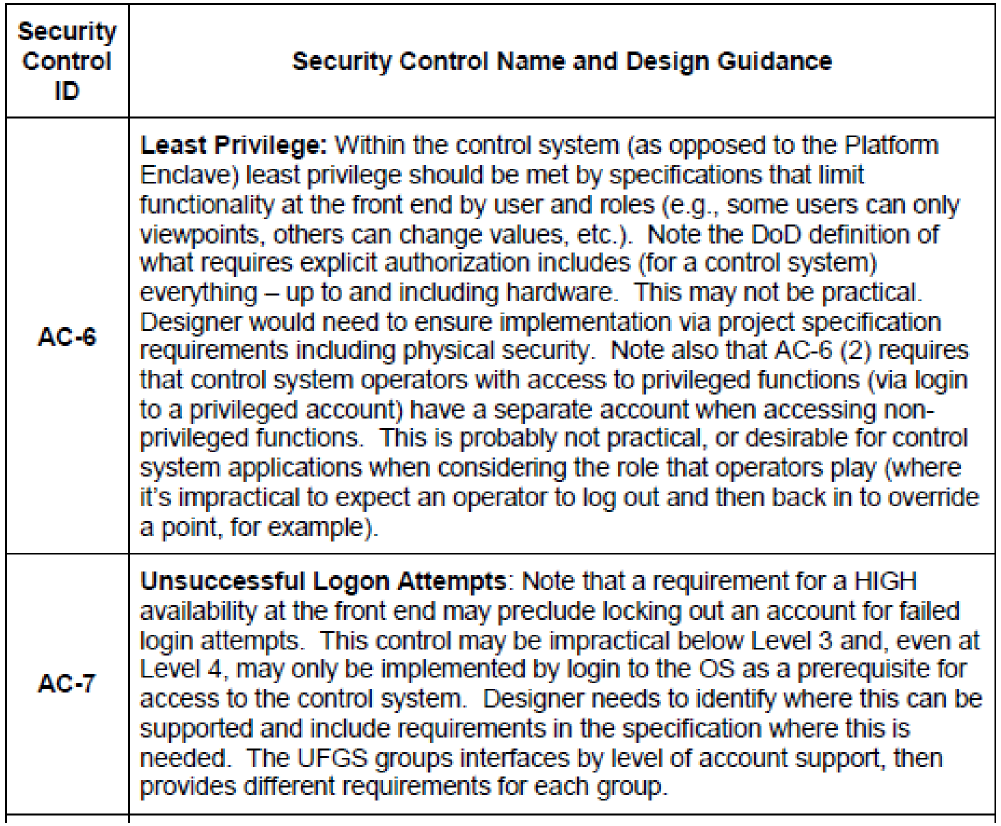
DESIGN REQUIREMENTS & EXPECTATIONS

Step 2: Generate the list of *potentially* applicable controls.

- UFC 4-010-06, Appendix F
- High-Level Policy Requirements

Note:

If you're modifying an existing system with an existing ATO, there will be an already approved controls list that may apply.

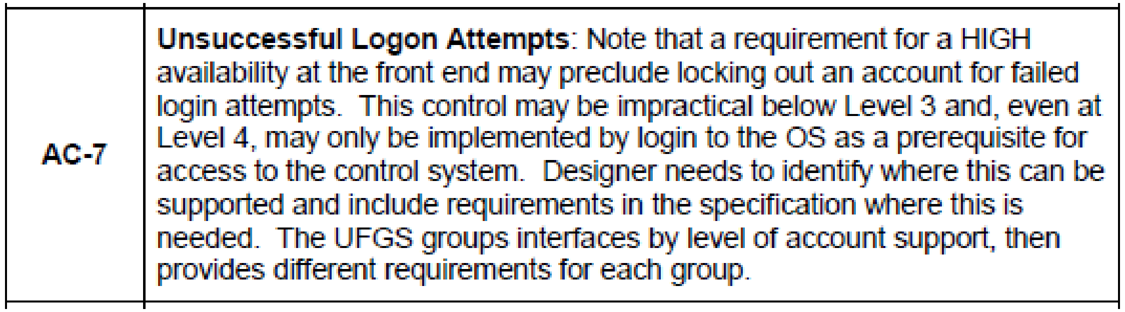


Security Control ID	Security Control Name and Design Guidance
AC-6	**Least Privilege:** Within the control system (as opposed to the Platform Enclave) least privilege should be met by specifications that limit functionality at the front end by user and roles (e.g., some users can only viewpoints, others can change values, etc.). Note the DoD definition of what requires explicit authorization includes (for a control system) everything – up to and including hardware. This may not be practical. Designer would need to ensure implementation via project specification requirements including physical security. Note also that AC-6 (2) requires that control system operators with access to privileged functions (via login to a privileged account) have a separate account when accessing non-privileged functions. This is probably not practical, or desirable for control system applications when considering the role that operators play (where it's impractical to expect an operator to log out and then back in to override a point, for example).
AC-7	**Unsuccessful Logon Attempts**: Note that a requirement for a HIGH availability at the front end may preclude locking out an account for failed login attempts. This control may be impractical below Level 3 and, even at Level 4, may only be implemented by login to the OS as a prerequisite for access to the control system. Designer needs to identify where this can be supported and include requirements in the specification where this is needed. The UFGS groups interfaces by level of account support, then provides different requirements for each group.

DESIGN REQUIREMENTS & EXPECTATIONS

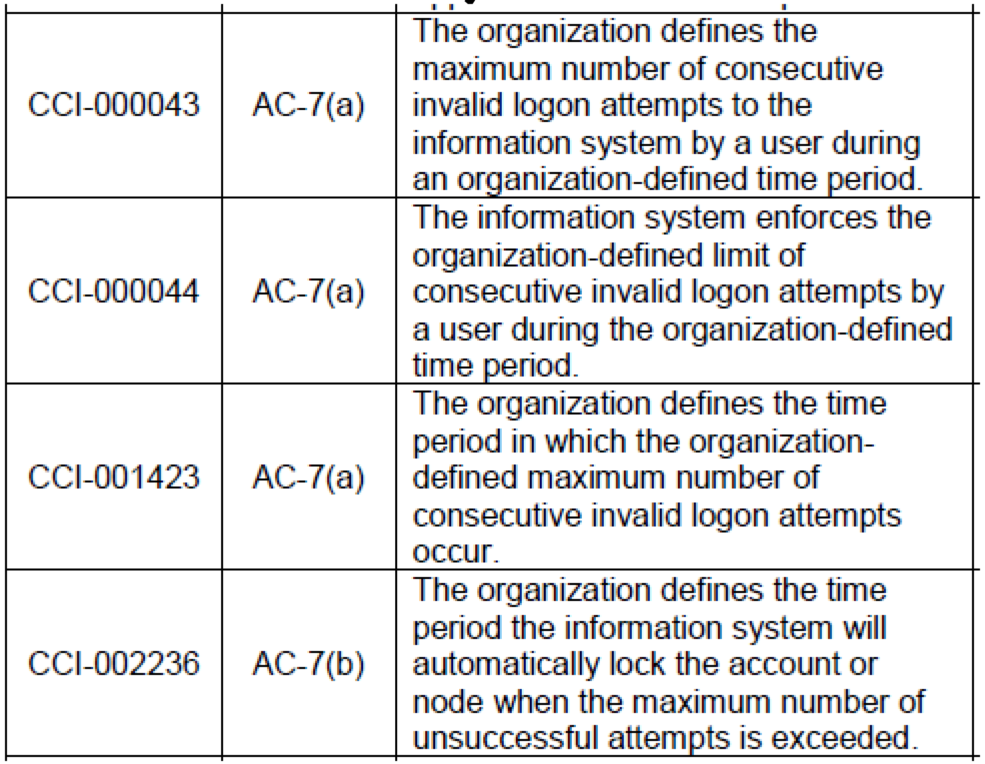
Step 3: Get CCIs (Control Correlation Indicators)

- Tangible Action



AC-7	**Unsuccessful Logon Attempts**: Note that a requirement for a HIGH availability at the front end may preclude locking out an account for failed login attempts. This control may be impractical below Level 3 and, even at Level 4, may only be implemented by login to the OS as a prerequisite for access to the control system. Designer needs to identify where this can be supported and include requirements in the specification where this is needed. The UFGS groups interfaces by level of account support, then provides different requirements for each group.

Control AC-7



CCI-000043	AC-7(a)	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.
CCI-000044	AC-7(a)	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.
CCI-001423	AC-7(a)	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occur.
CCI-002236	AC-7(b)	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.

[some] Corresponding CCIs

DESIGN REQUIREMENTS & EXPECTATIONS

Step 3: Start tailoring the applicable CCIs.

- UFC 4-010-06, Appendix G
  - Which CCIs apply to FRCS and are the designer's responsibility.
  - Which impact level specific CCIs apply to (LOW or MODERATE).
  - After filtering these down, this is your **baseline** CCI set.

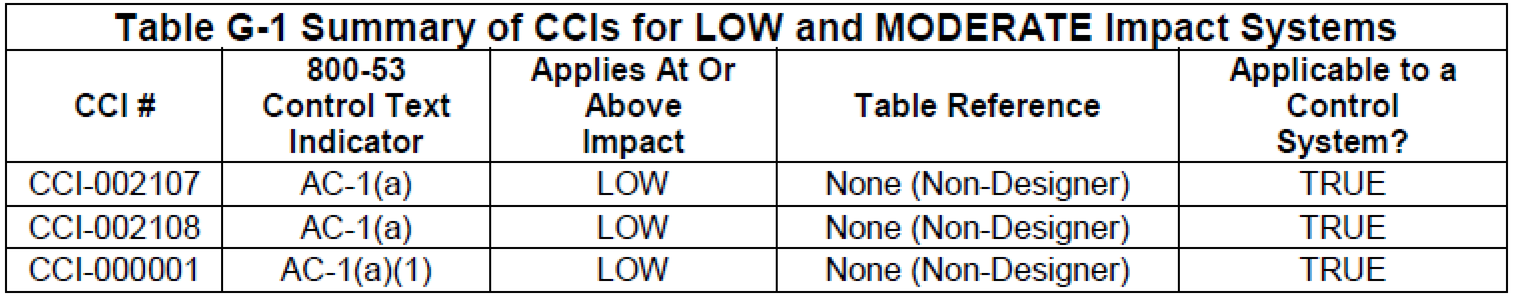


Table G-1 Summary of CCIs for LOW and MODERATE Impact Systems

CCI #	800-53 Control Text Indicator	Applies At Or Above Impact	Table Reference	Applicable to a Control System?
CCI-002107	AC-1(a)	LOW	None (Non-Designer)	TRUE
CCI-002108	AC-1(a)	LOW	None (Non-Designer)	TRUE
CCI-000001	AC-1(a)(1)	LOW	None (Non-Designer)	TRUE

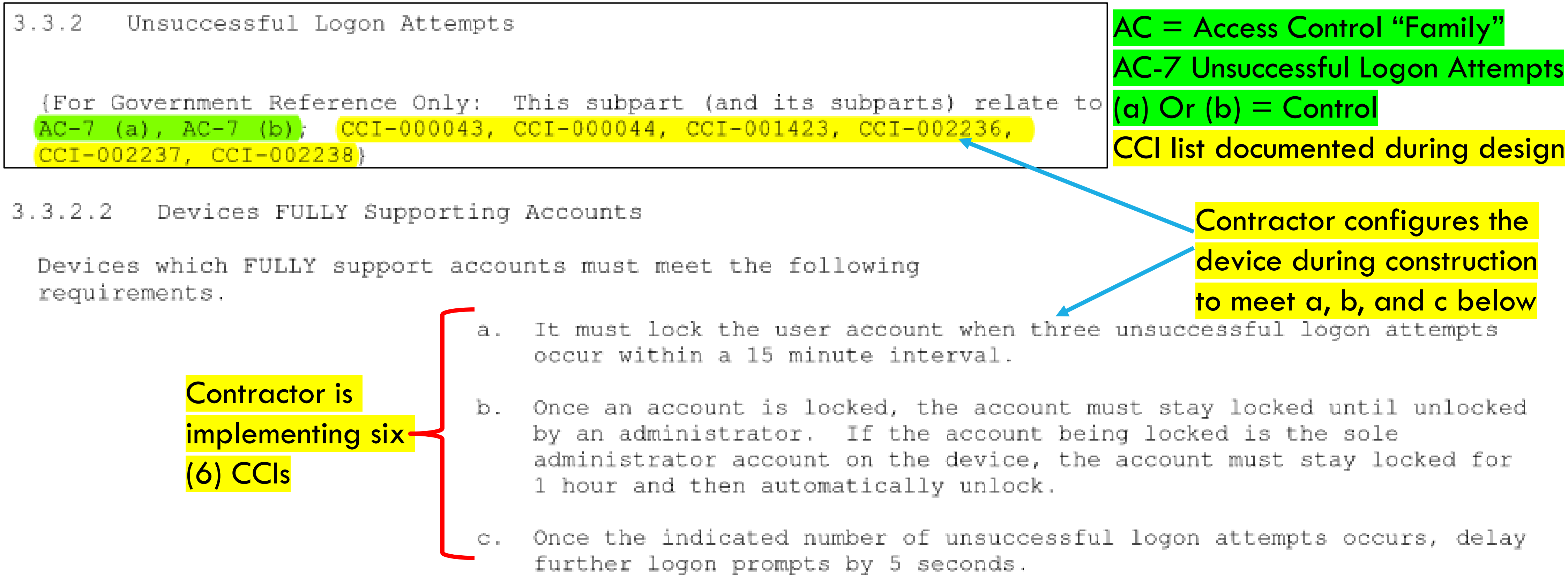
DESIGN REQUIREMENTS & EXPECTATIONS

Step 3: Start tailoring the applicable CCIs.

CCI	Control Text (Summarized)	Fire Alarm Panel	Full BAS w/PC
CCI-000399	Produce an Inventory	Applicable	Applicable
CCI-000200	Passwords can’t be reused for at least 5 generations.	Impractical	Applicable
CCI-001989	Change Default Credentials	Applicable	Applicable
CCI-001441	Maintain Audit Trail on Wireless Access	N/A*	N/A*

DESIGN REQUIREMENTS & EXPECTATIONS

Step 4: Start tailoring the 25 05 11 specification.



3.3.2 Unsuccessful Logon Attempts

{For Government Reference Only: This subpart (and its subparts) relate to AC-7 (a), AC-7 (b); CCI-000043, CCI-000044, CCI-001423, CCI-002236, CCI-002237, CCI-002238}

3.3.2.2 Devices FULLY Supporting Accounts

Devices which FULLY support accounts must meet the following requirements.

a. It must lock the user account when three unsuccessful logon attempts occur within a 15 minute interval.

b. Once an account is locked, the account must stay locked until unlocked by an administrator. If the account being locked is the sole administrator account on the device, the account must stay locked for 1 hour and then automatically unlock.

c. Once the indicated number of unsuccessful logon attempts occurs, delay further logon prompts by 5 seconds.

AC = Access Control "Family"

AC-7 Unsuccessful Logon Attempts

(a) Or (b) = Control

CCI list documented during design

Contractor configures the device during construction to meet a, b, and c below

Contractor is implementing six (6) CCIs

DESIGN REQUIREMENTS & EXPECTATIONS

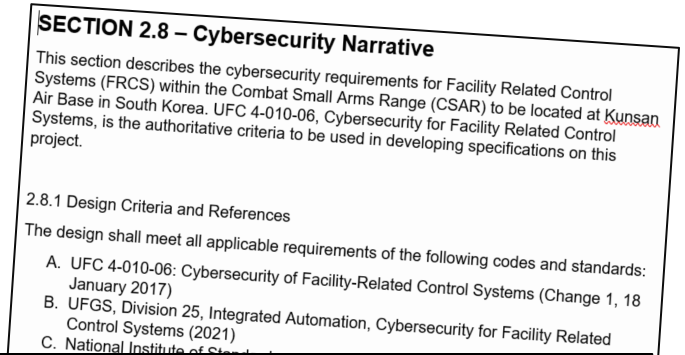
Step 4: Start tailoring the 25 05 11 specification.

- Eliminate the paragraphs for ‘N/A’ or ‘Impractical’ CCIs
- Include any site or system-specific requirements.
  - Ex. An existing ATO’s Configuration Management requirements
  - Ex. The office/department responsible for issuing IP addresses.

DESIGN REQUIREMENTS & EXPECTATIONS

Concept Design Expectations (10-35%)

- Separate Cybersecurity chapter in the DA
  - Functional description/narrative of each system
    - Impact rating and how it was determined.
    - Interconnection requirements and responsibilities.
  - Preliminary CCI lists
  - High-Level/Notional Diagram
- UFGS: Table of Contents
  - One 25 05 11 entry for each control system



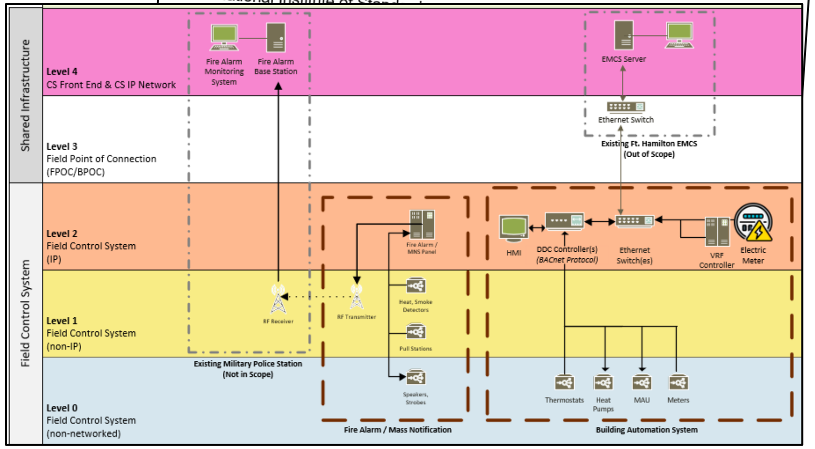
SECTION 2.8 – Cybersecurity Narrative

This section describes the cybersecurity requirements for Facility Related Control Systems (FRCS) within the Combat Small Arms Range (CSAR) to be located at Kunsan Air Base in South Korea. UFC 4-010-06, Cybersecurity for Facility Related Control Systems, is the authoritative criteria to be used in developing specifications on this project.

2.8.1 Design Criteria and References

The design shall meet all applicable requirements of the following codes and standards:

A. UFC 4-010-06: Cybersecurity of Facility-Related Control Systems (Change 1, 18 January 2017)
B. UFGS, Division 25, Integrated Automation, Cybersecurity for Facility Related Control Systems (2021)
C. National Institute of Stand



DESIGN REQUIREMENTS & EXPECTATIONS

Design Development Expectations (50-65%)

- Updated DA that is consistent across disciplines and drawings
  - CCI lists are relatively finalized and properly annotated.
  - Basis-of-design products align with cybersecurity approach.
- Draft 25 05 11 specification for each system
  - 25 05 11 is generally tailored to the specific control system (in accordance with CCIs)
  - There are no inconsistencies between the 25 05 11 and other specs/drawings

DESIGN REQUIREMENTS & EXPECTATIONS

Pre-Final Design Expectations (90-95%)

- Each 25 05 11 is complete and fully tailored to each system.
  - The CCIs are finalized and fully incorporated into the specs
  - "N/A" or "Impractical" CCIs have been removed from the specs
  - <u>No inconsistencies</u> between spec sections
  - <u>No inconsistencies</u> between the 25 05 11 and the drawings

KEY 25 05 11 SUBMITTALS

SD-01 (Preconstruction) / SD-02 (Shop Drawings)

- Proposed STIG and SRG Applicability Report
- Network Communication Report (Ports & Protocols)
- Cybersecurity Riser Diagram
- Control System Inventory Report
- Cybersecurity Interconnection Schedule

KEY 25 05 11 SUBMITTALS

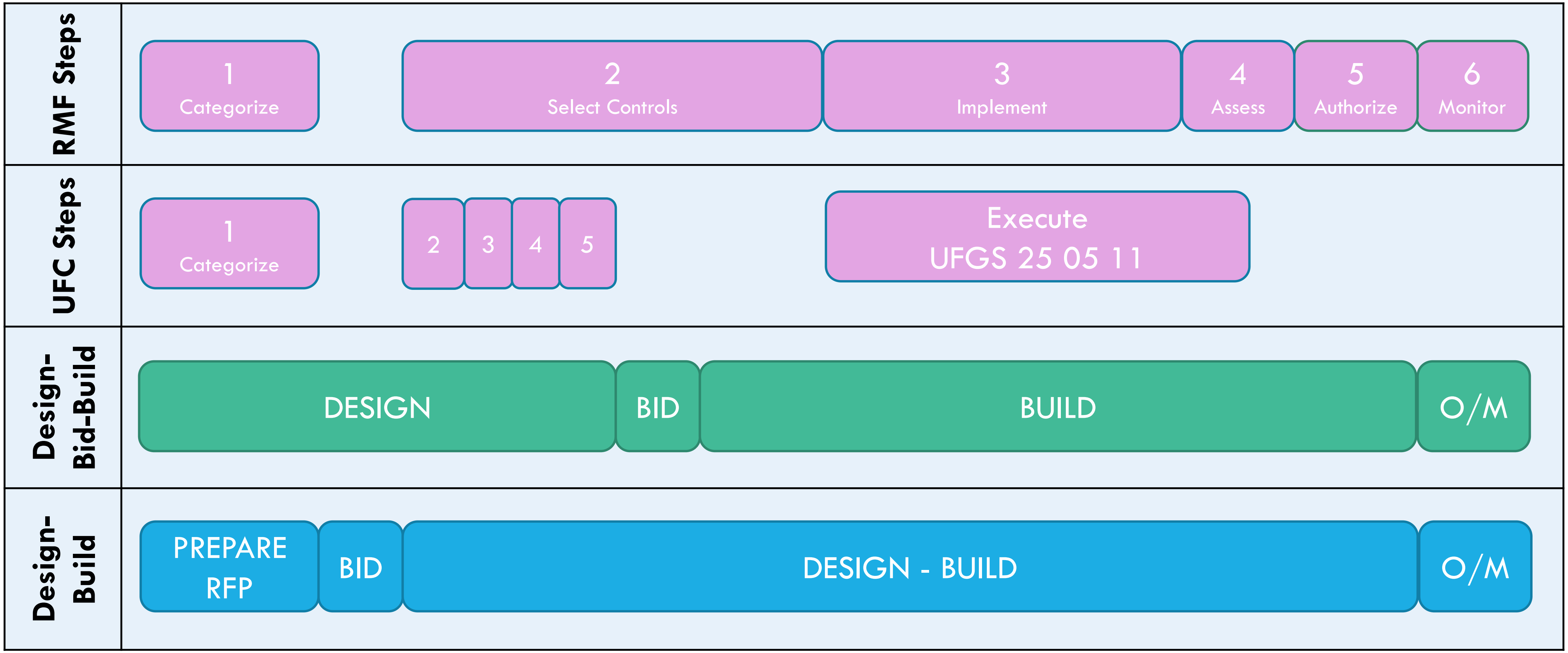
SD-03 (Product Data)

- Control System Cybersecurity Documentation
  - Technical Manual (user roles, permission matrix, security options)
  - Vendor Secure Configuration/Installation Guides
  - Known vulnerabilities (vendor releases, ICS-CERT, NIST NVD)

SD-06 (Test Reports) / SD-11 (Closeout)

- Cybersecurity Testing Procedures/Report
- Password Summary Report
- Software and Configuration Backups
- STIG/SRG/Vendor Guide Compliance Report

RMF VS DESIGN/CONSTRUCTION



RMF Steps: 1 Categorize · 2 Select Controls · 3 Implement · 4 Assess · 5 Authorize · 6 Monitor

UFC Steps: 1 Categorize · 2 · 3 · 4 · 5 · Execute UFGS 25 05 11

Design-Bid-Build: DESIGN · BID · BUILD · O/M

Design-Build: PREPARE RFP · BID · DESIGN - BUILD · O/M

</TALK>

1. Cybersecurity is an aspect of the project, not the primary objective.*

   **This does not imply that it is unnecessary or unimportant!*

2. I don’t care if it’s “standalone”, “cyber” is required.

3. Our goal [in construction] is meeting defined technical requirements, not “get an ATO.”