

SAME Japan Industry Forum

Facility-Related Control System (FRCS) Cybersecurity

施設制御システム(FRCS) サイバーセキュリティ

Topics

- Why Cybersecurity for Facility-Related Control Systems (FRCS)?
- What Do We Need To Follow – Design Criteria
- Who Incorporates Cybersecurity? Certification Requirements
- How Do We Incorporate Cybersecurity Into Control System Design?
- Specifications During Construction
- Questions

項目

- なぜ施設制御システム(FRCS)におけるサイバーセキュリティを必要とするか？
- 設計基準として従わなければならない事項
- 誰がサイバーセキュリティを設計に取り入れる事が出来るか？ 資格条件
- どのようにサイバーセキュリティを制御システム設計に取り入れるべきか？
- 建築仕様書
- 質疑応答

Why Cybersecurity for Facility-Related Control Systems (FRCS)?

“Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.

– Presidential Executive Order 13636

“The Department's computer networks and systems are under incessant cyber attack...Recognizing the increased threats, vulnerabilities, and risks the Department recently updated the DOD Instructions 8500.01 and 8510.01...these instructions mandate that Industrial Control Systems (ICS) be made secure against cyber attacks by implementing a Risk Management Framework (RMF). Damage to or compromise of any ICS may be a mission disabler.”

– USD (AT&L) Memo, Real Property-related ICS Cybersecurity

なぜ施設制御システム(FRCS)におけるサイバーセキュリティを必要とするか？

重要なインフラへの度重なるサイバー攻撃がサイバーセキュリティの改善の必要性を示している。重要なインフラに対するサイバー脅威は拡大し続け、私達が直面しなければいけない最も深刻な国家安全保障上の課題の一つである。

- 大統領行政命令 13636

国防総省のコンピュータネットワークおよびコンピューターシステムは絶え間ないサイバー攻撃を受けている。増加する脅威、脆弱性、リスクを認識し、リスクマネジメントフレームワーク(RMF)を実行する事で産業制御システム(ICS)に対するサイバー攻撃からの安全を確保する為に、近年国防総省指示書8500.01及び8510.01は改定された。いかなる産業制御システムへの損傷及び侵害は任務を無効にする可能性がある。

- USD (AT&L) 国防次官 (調達、技術、兵站担当) メモ、不動産関連産業制御システムサイバーセキュリティ

Why Cybersecurity for Facility-Related Control Systems (FRCS)?

“Today’s cyber threat reaches beyond traditional information technology and data, to include supporting operational technology networks and systems that enable nearly every aspect of the Navy’s mission... Cybersecurity discipline should be part of each Command’s warfighting culture to protect the Navy shore enterprise from persistent cyber threat.”

– OPNAV N4 NAVADMIN 136/16

“The purpose of this memorandum is to direct all Department of the Navy (DON) military construction (MILCON) to fully address facility-related control system (FRCS) cybersecurity requirements during the planning, design and construction phases to include cybersecurity commissioning. We must use every MILCON as an opportunity to improve the DON's cybersecurity posture...”

– Todd Mellon, Acting ASN (EI&E)

なぜ施設制御システム(FRCS)におけるサイバーセキュリティを必要とするか？

今日のサイバー脅威は、従来の情報技術や情報に対してだけでなく、**ほぼ全ての米海軍の任務を作動させるオペレーショナルテクノロジーを支える技術や情報にも影響を及ぼす**。継続的なサイバー脅威から米海軍の沿岸活動を守るために、サイバーセキュリティ規律は各コマンドの戦闘訓練の一部であるべきだ。

- 海軍作戦部長 N4 米海軍行政命令 136/16

この覚書の目的は、全ての米海軍建設（MILCON）において、**サイバーセキュリティコミッショニングを含む計画、設計、建設段階で施設制御システム(FRCS)サイバーセキュリティ条件を十分に取り組まなければならない**ことを命令する。

全ての米軍建設（MILON）を米海軍のサイバーセキュリティ姿勢を向上させる機会とするべきだ。

- Todd Mellon米海軍次官補(EI&E)

Why Cybersecurity for Facility-Related Control Systems (FRCS)?

“We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe **will have serious consequences on our ability to execute assigned missions if not addressed - cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS)**”

– Joint Memo from NORTHCOM & PACOM to SECDEF

THE WHITE HOUSE



JULY 28, 2021

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

<https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/>

なぜ施設制御システム(FRCS)におけるサイバーセキュリティを必要とするか？

重要な産業制御システム（ICS）インフラのサイバーセキュリティに取り組まなければ、与えられた任務を実行する能力に重大な影響を及ぼすことになるかと理解しており、新たな脅威へ集中し、可視性を確保する為の協力を必要としている

– Joint Memo from NORTHCOM & PACOM to SECDEF

THE WHITE HOUSE



JULY 28, 2021

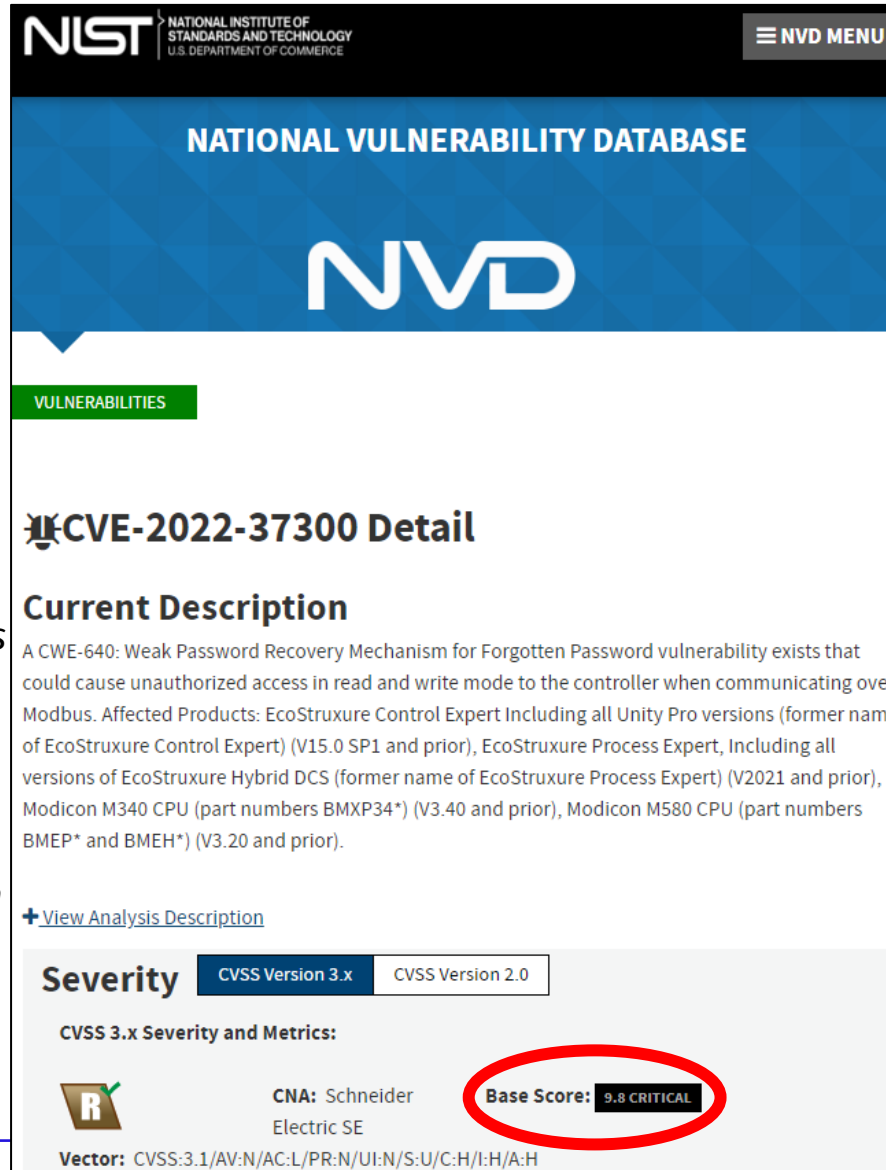
National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

<https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/>

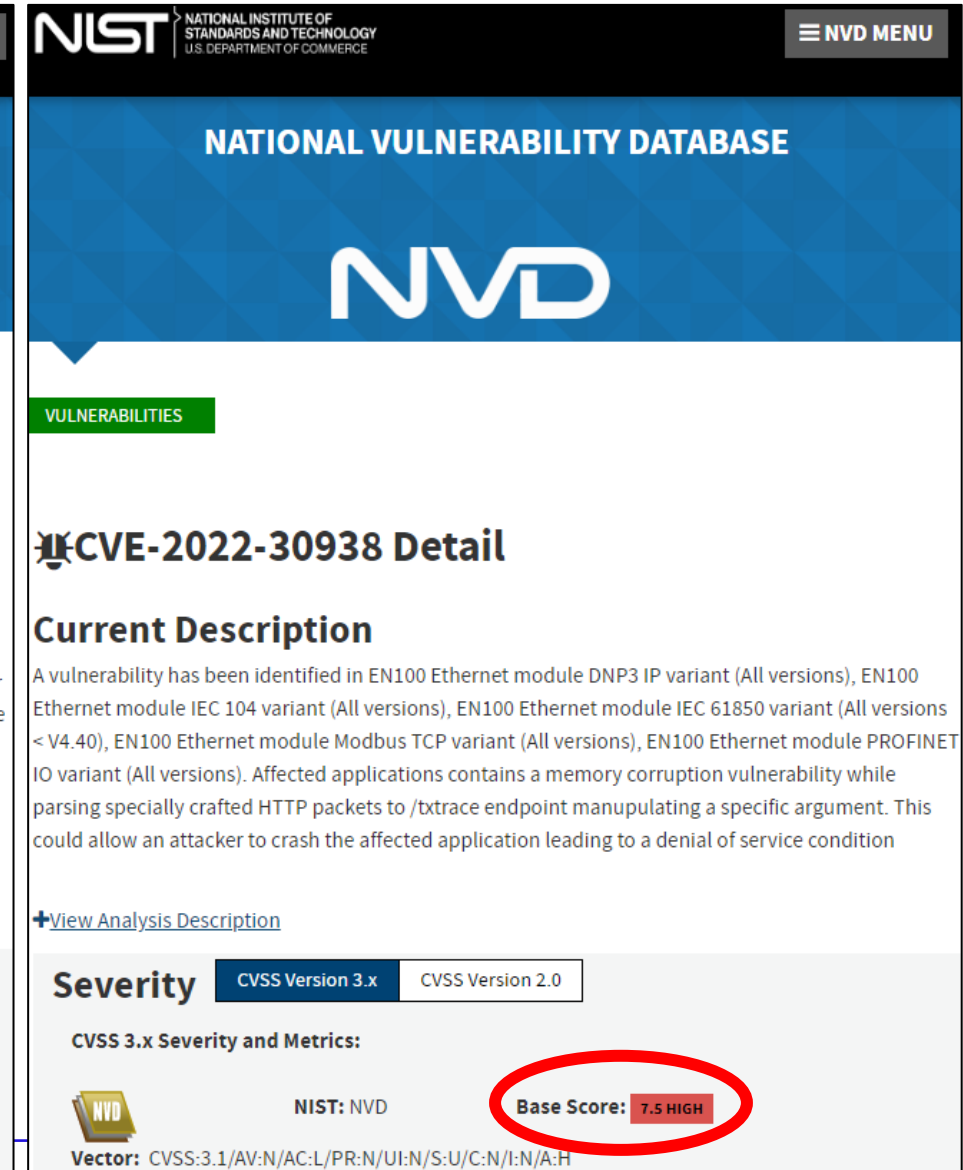
Why Cybersecurity for Facility-Related Control Systems (FRCS)?

- Two 2022 Examples of Common Vulnerabilities and Exposures (CVE)
- General Search using keyword "Modbus" returned 115 CVE Records

Modbus is a data communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs). Modbus has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices.



The screenshot shows the NVD detail page for CVE-2022-37300. The page header includes the NIST logo and 'NATIONAL VULNERABILITY DATABASE'. Below the header is a green 'VULNERABILITIES' tab. The main heading is 'CVE-2022-37300 Detail'. Under 'Current Description', it states: 'A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists that could cause unauthorized access in read and write mode to the controller when communicating over Modbus. Affected Products: EcoStruxure Control Expert Including all Unity Pro versions (former name of EcoStruxure Control Expert) (V15.0 SP1 and prior), EcoStruxure Process Expert, Including all versions of EcoStruxure Hybrid DCS (former name of EcoStruxure Process Expert) (V2021 and prior), Modicon M340 CPU (part numbers BMXP34*) (V3.40 and prior), Modicon M580 CPU (part numbers BMEP* and BMEH*) (V3.20 and prior)'. Below the description is a '+View Analysis Description' link. The 'Severity' section shows 'CVSS Version 3.x' selected and a 'Base Score: 9.8 CRITICAL' circled in red. The 'Vector' is 'CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H'.

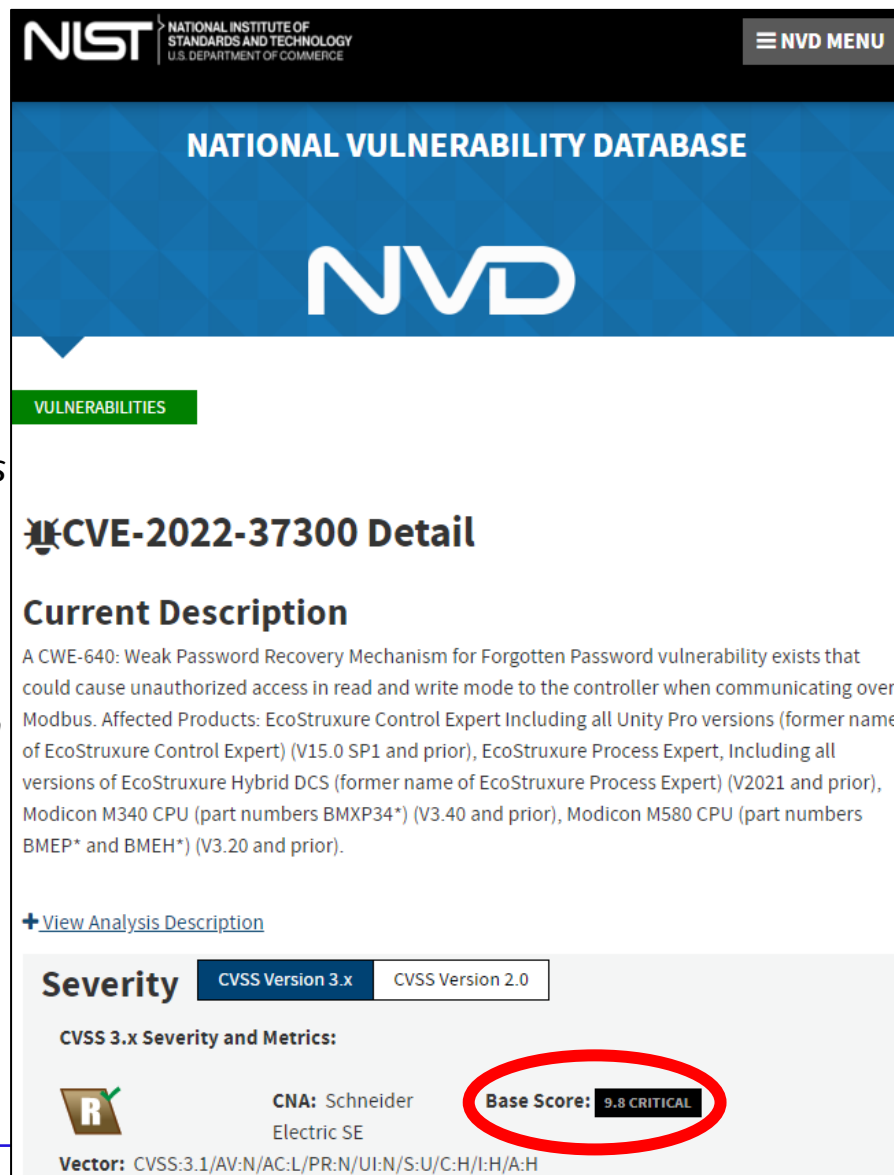


The screenshot shows the NVD detail page for CVE-2022-30938. The page header includes the NIST logo and 'NATIONAL VULNERABILITY DATABASE'. Below the header is a green 'VULNERABILITIES' tab. The main heading is 'CVE-2022-30938 Detail'. Under 'Current Description', it states: 'A vulnerability has been identified in EN100 Ethernet module DNP3 IP variant (All versions), EN100 Ethernet module IEC 104 variant (All versions), EN100 Ethernet module IEC 61850 variant (All versions < V4.40), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module PROFINET IO variant (All versions). Affected applications contains a memory corruption vulnerability while parsing specially crafted HTTP packets to /txtrace endpoint manipulating a specific argument. This could allow an attacker to crash the affected application leading to a denial of service condition'. Below the description is a '+View Analysis Description' link. The 'Severity' section shows 'CVSS Version 3.x' selected and a 'Base Score: 7.5 HIGH' circled in red. The 'Vector' is 'CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H'.

なぜ施設制御システム(FRCS)におけるサイバーセキュリティを必要とするか？

- 2022年度 共通脆弱性識別子(CVE) 2例
- "モdbus(Modbus)"をキーワードとして検索すると115のCVE結果

Modbus is a data communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs). Modbus has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices.



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2022-37300 Detail


Current Description

A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists that could cause unauthorized access in read and write mode to the controller when communicating over Modbus. Affected Products: EcoStruxure Control Expert Including all Unity Pro versions (former name of EcoStruxure Control Expert) (V15.0 SP1 and prior), EcoStruxure Process Expert, Including all versions of EcoStruxure Hybrid DCS (former name of EcoStruxure Process Expert) (V2021 and prior), Modicon M340 CPU (part numbers BMXP34*) (V3.40 and prior), Modicon M580 CPU (part numbers BMEP* and BMEH*) (V3.20 and prior).

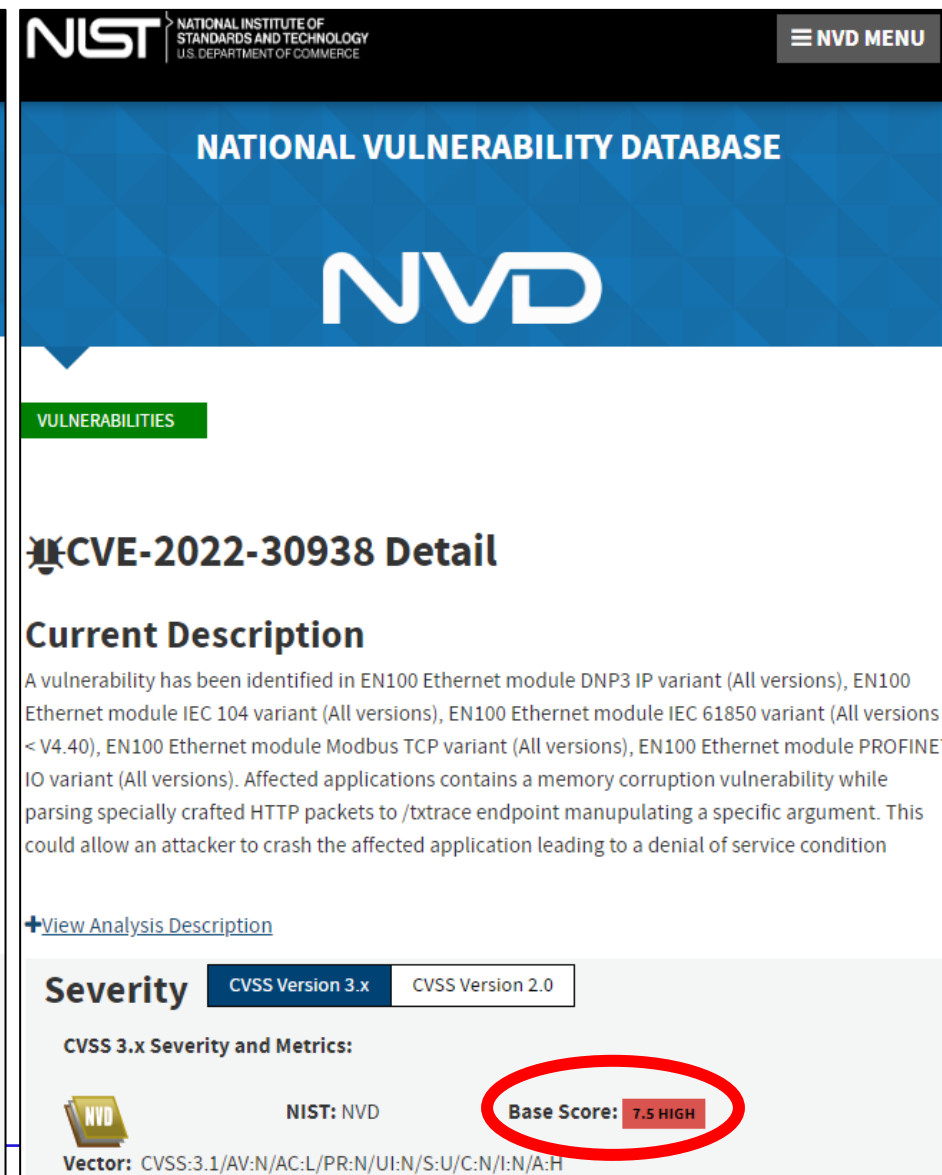
[+View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 CNA: Schneider Electric SE **Base Score: 9.8 CRITICAL**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2022-30938 Detail


Current Description

A vulnerability has been identified in EN100 Ethernet module DNP3 IP variant (All versions), EN100 Ethernet module IEC 104 variant (All versions), EN100 Ethernet module IEC 61850 variant (All versions < V4.40), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module PROFINET IO variant (All versions). Affected applications contains a memory corruption vulnerability while parsing specially crafted HTTP packets to /ttrace endpoint manipulating a specific argument. This could allow an attacker to crash the affected application leading to a denial of service condition

[+View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

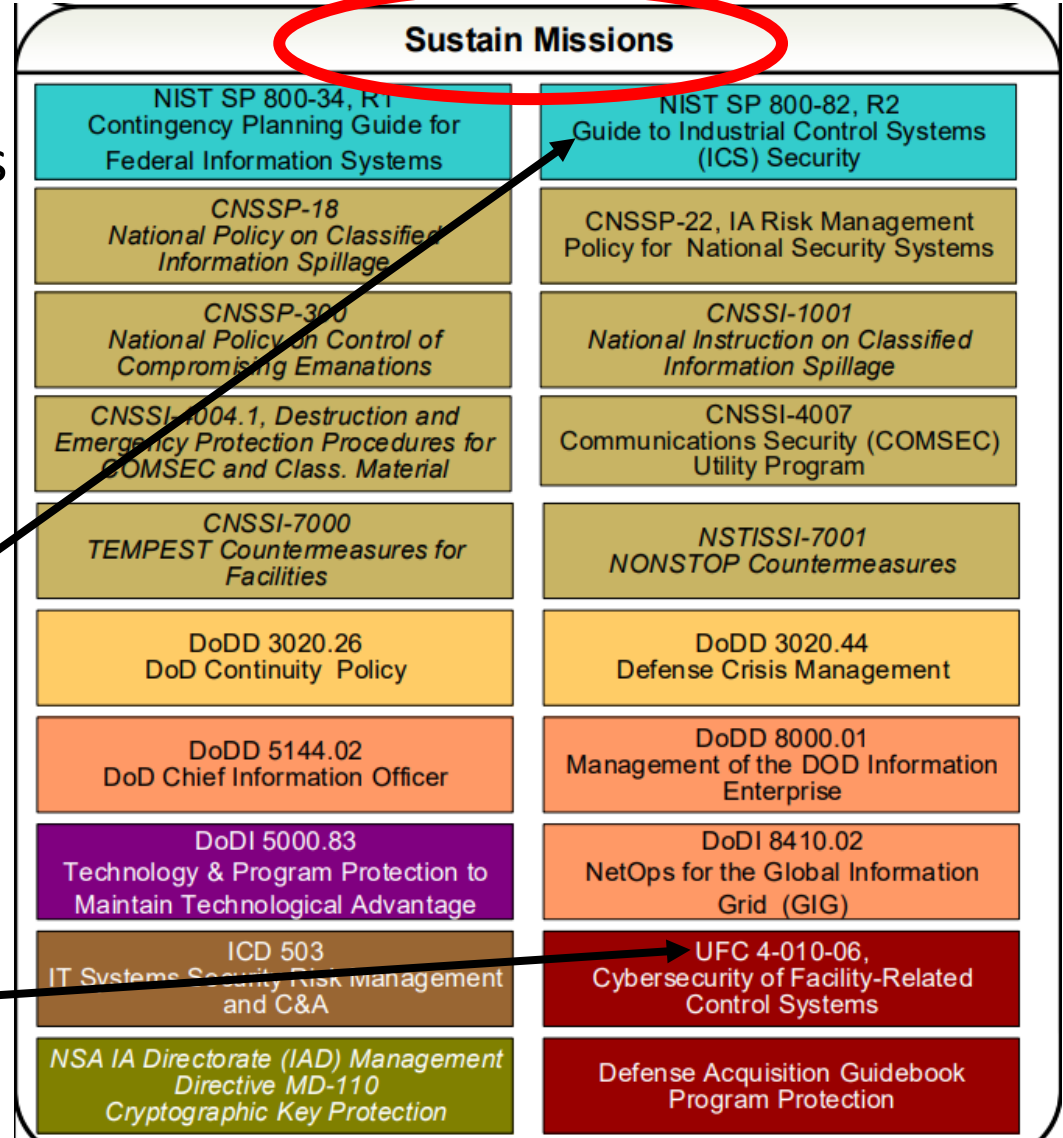
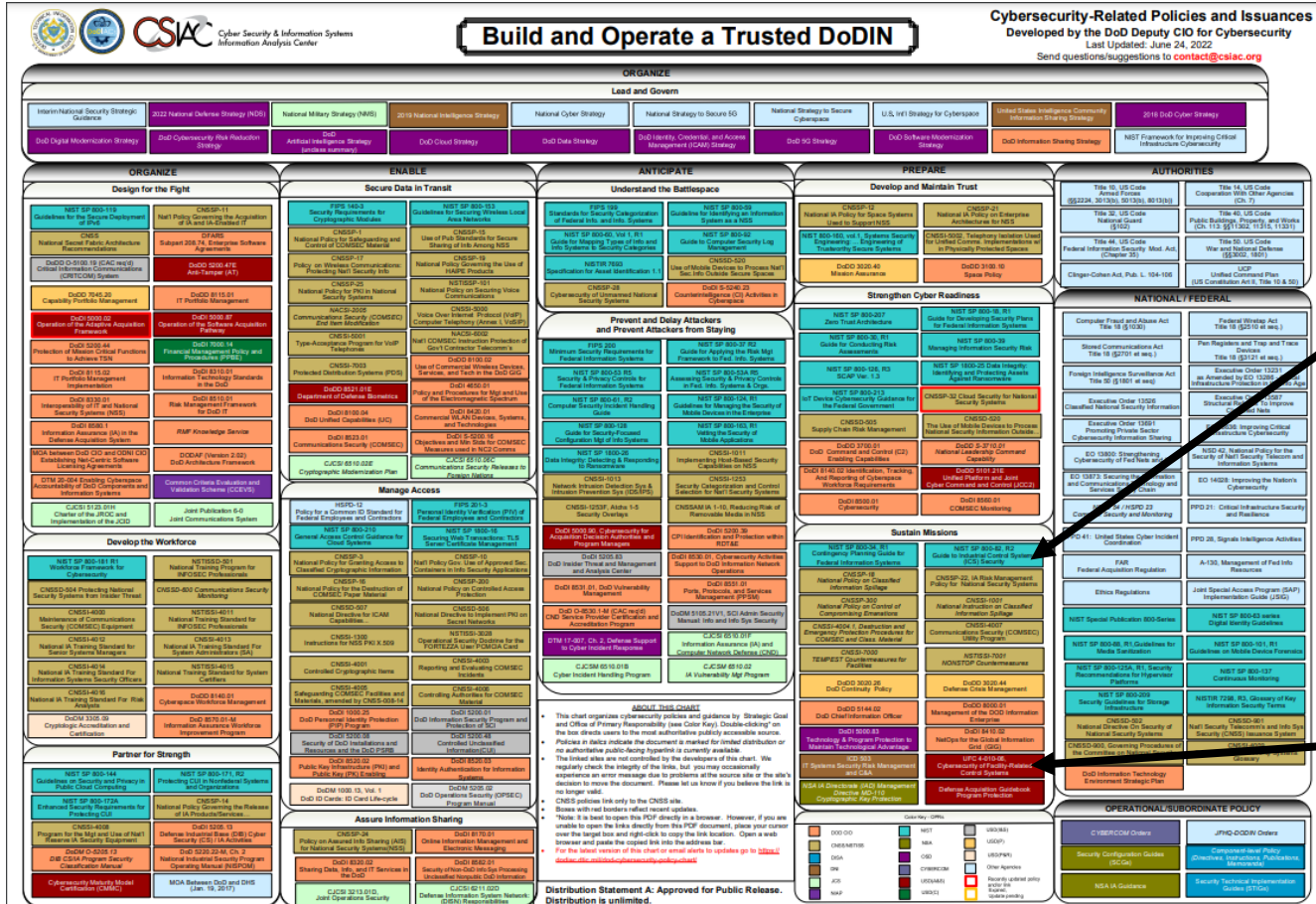
CVSS 3.x Severity and Metrics:

 NIST: NVD **Base Score: 7.5 HIGH**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

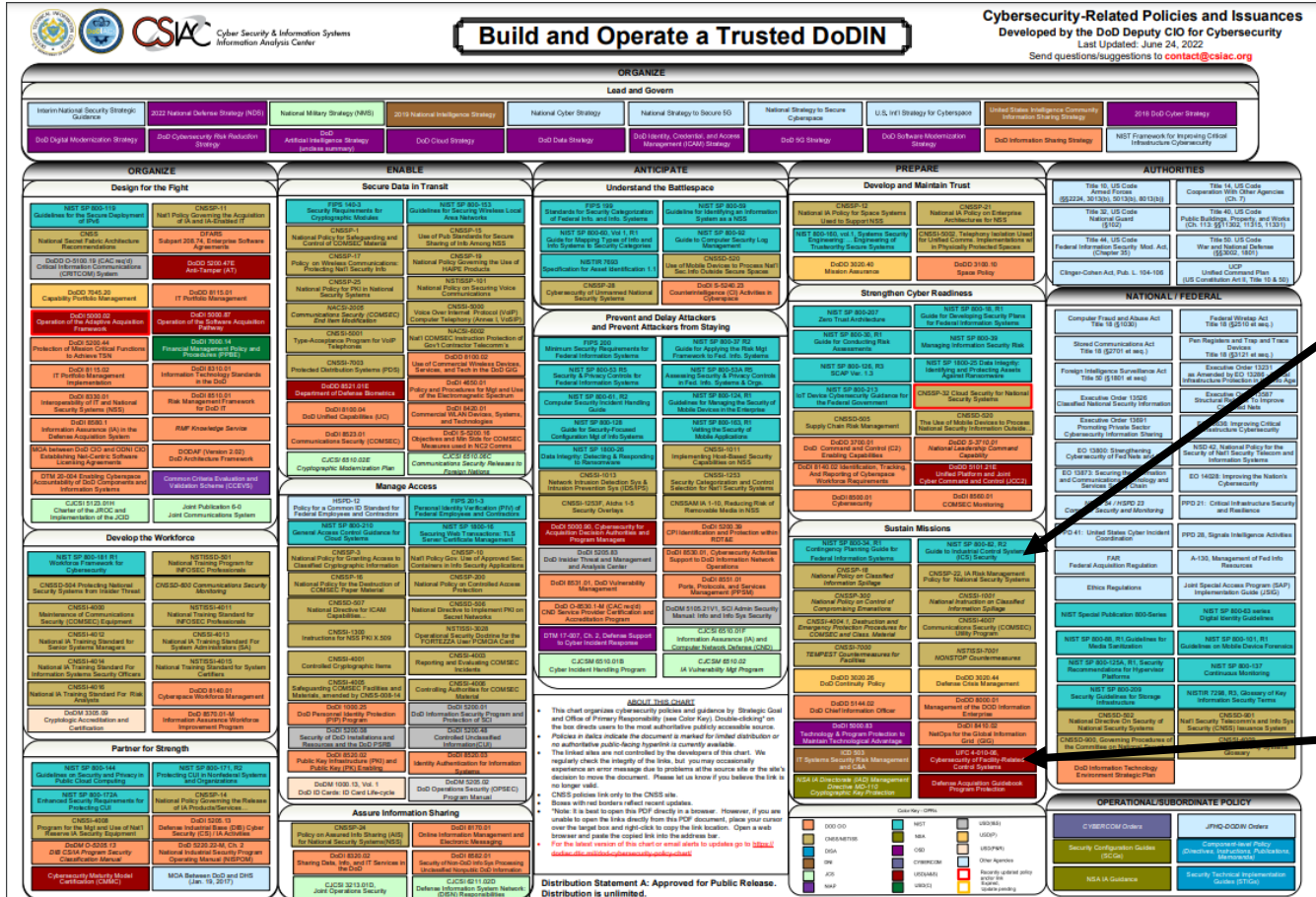
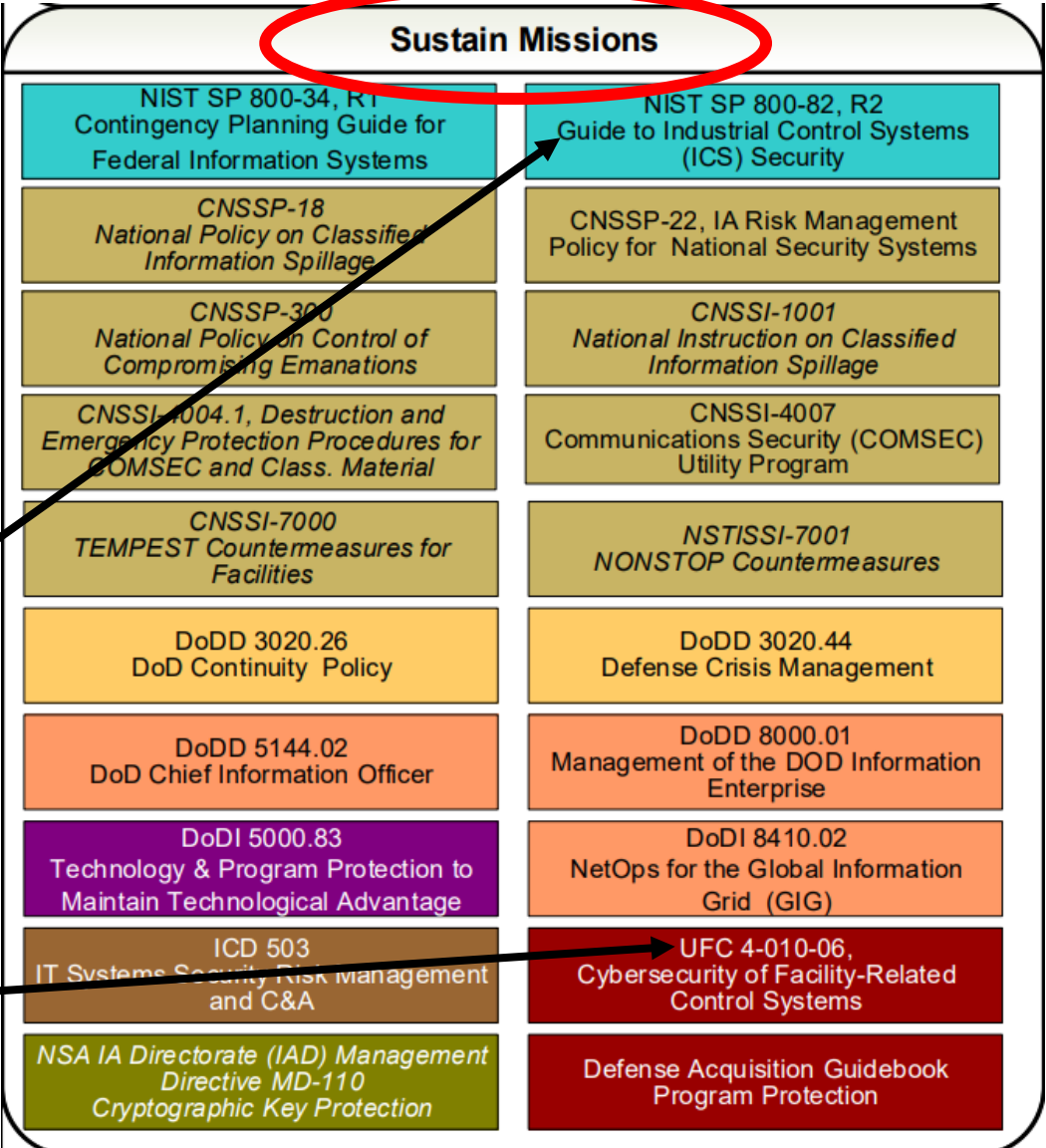
DOD Cybersecurity Policy Chart

The goal of the DoD Cybersecurity Policy Chart is to capture the tremendous breadth of applicable policies



国防総省(DoD)サイバーセキュリティ政策チャート

国防総省(DoD)サイバーセキュリティ政策チャートは適切な政策の膨大な範囲を把握する事を目的としている



What Do We Need To Follow? Cybersecurity Design Criteria

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

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

- [UFC 4-010-06 Cybersecurity of Facility-Related Control Systems](#) provides requirements for incorporating cybersecurity into the design of facility-related control systems
- Published by DoD 19 September 2016, Change 1, 18 January 2017
- Revision Anticipated by the End of Calendar Year

サイバーセキュリティ設計基準として従わなければならない事項

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

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

- [UFC 4-010-06 Cybersecurity of Facility-Related Control Systems](#) provides requirements for incorporating cybersecurity into the design of facility-related control systems
- Published by DoD 19 September 2016, Change 1, 18 January 2017
- Revision Anticipated by the End of Calendar Year

What Do We Need To Follow? Cybersecurity Design Criteria

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

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

- Provides Criteria for Inclusion of Cybersecurity in Design of Control Systems to Address Risk Management Framework (RMF) Security Controls During Design and Subsequent Construction
- Chapter 3, Paragraph 3-1.1
Outlines the Five Steps for Cybersecurity Design
- Chapter 5, Paragraph 5-2
Outlines Requirements by Design Phase
- Appendix H Provides Control Correlation Identifier (CCI) Tables for LOW and MODERATE impact systems

OBJECTIVE: To deliver secured systems that allow the System Owner (SO) to obtain an Authority to Operate (ATO) without rework and having to rebuild/reconfigure the system.

サイバーセキュリティ設計基準として従わなければならない事項

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

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

- 設計及びその後の施工時にリスクマネジメントフレームワーク（RMF）を取り組む為に制御システムの設計においてサイバーセキュリティを含む基準を定める
- Chapter 3, Paragraph 3-1.1
Outlines the Five Steps for Cybersecurity Design
- Chapter 5, Paragraph 5-2
Outlines Requirements by Design Phase
- Appendix H Provides Control Correlation Identifier (CCI) Tables for LOW and MODERATE impact systems

Who Incorporates Cybersecurity? Certification Requirements

Cybersecurity Subject Matter Expert (SME) is required to hold DoD 8140 and DoDI 8570 Information Assurance Management (IAM) Level II or Information Assurance System Architect and Engineer (IASAE) Level II Certification

Example
1

Individuals performing cybersecurity design functions shall meet certification and skills requirements for IAM Level II Certified Professional outlined in DoD 8140 Information Assurance Workforce Improvement Program. It is the Contractor's responsibility to ensure the latest DoD, Component and installations policies and guidance are met for the requirements.

Example
2
SAES was
revised to
include
this

Cybersecurity: In accordance with the Basic IDIQ Contract SAES. Provide cybersecurity requirements for all applicable facility-related control systems in accordance with UFC 4-010-06 (Cybersecurity of Facility-Related Control Systems). Utilize a qualified Cybersecurity Subject Matter Expert (SME) who will be responsible for meeting all design requirements for Cybersecurity of Facility-Related Control Systems, to include editing of UFGS 25 05 11 and 25 08 11.00 20. This position requires that the individual currently meets Information Assurance Manager (IAM) Level II or Information Assurance System Architect and Engineer (IASAE) Level II Certification in accordance with DoDI 8570 Information Workforce Improvement Program. Individuals for this position must have experience with Risk Management Framework and Facility-Related Control Systems Cybersecurity.

誰がサイバーセキュリティーを設計に取り入れる事が出来るか？

サイバーセキュリティー内容領域専門家(SME)は国防省(DoD)8140又は国防省指令(DoDI) 8540に準ずる情報保障管理(IAM)レベルII又は情報保障システム建築士又は設計士(IASAE)レベルIIを持つ者とする

Example
1

Individuals performing cybersecurity design functions shall meet certification and skills requirements for IAM Level II Certified Professional outlined in DoD 8140 Information Assurance Workforce Improvement Program. It is the Contractor's responsibility to ensure the latest DoD, Component and installations policies and guidance are met for the requirements.

Example
2
SAES was
revised to
include
this

Cybersecurity: In accordance with the Basic IDIQ Contract SAES. Provide cybersecurity requirements for all applicable facility-related control systems in accordance with UFC 4-010-06 (Cybersecurity of Facility-Related Control Systems). Utilize a qualified Cybersecurity Subject Matter Expert (SME) who will be responsible for meeting all design requirements for Cybersecurity of Facility-Related Control Systems, to include editing of UFGS 25 05 11 and 25 08 11.00 20. This position requires that the individual currently meets Information Assurance Manager (IAM) Level II or Information Assurance System Architect and Engineer (IASAE) Level II Certification in accordance with DoDI 8570 Information Workforce Improvement Program. Individuals for this position must have experience with Risk Management Framework and Facility-Related Control Systems Cybersecurity.

How Do We Incorporate Cybersecurity?

- Step 1: Information System Security Manager (ISSM) and/or System Owner (SO) determine C-I-A Impact Level (Not Designer of Record)
- Steps 2-4: Use UFC 4-010-06, Appendix H to develop CCI list(s)
 - Use Table H-4 for a LOW Impact system
 - Use Table H-4 and Table H-5 for a MODERATE Impact system
 - CCI list(s) identify “Applicable”, Designer CCIs incorporated into the UFGS 25 05 11, Cybersecurity for FRCS specification

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.

どのようにサイバーセキュリティを取り入れるべきか？

- Step 1: 情報システムセキュリティ管理者(ISSM) 又はシステムオーナー(SO) がC-I-A(秘匿性、完全性、可用性)インパクトレベルを決める(設計業務責任者(Designer of Record)ではない)
- Steps 2-4: 米国施設基準(UFC)4-010-06, 別表H を基にCCIリストを作成する
 - Use Table H-4 for a LOW Impact system
 - Use Table H-4 and Table H-5 for a MODERATE Impact system
 - CCI list(s) identify “Applicable”, Designer CCI’s incorporated into the UFGS 25 05 11, Cybersecurity for FRCS specification

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.

What is C-I-A?

- **C – Confidentiality:** A loss of confidentiality is the *unauthorized disclosure* of information.
- **I – Integrity:** A loss of integrity is the *unauthorized modification or destruction* of information.
- **A – Availability:** A loss of availability is the *disruption of access to or use of information or a system*.

Examples: FRCS supporting an administrative facility is determined to have a potential impact from a loss of confidentiality as low, integrity as low and availability as low. C-I-A is LOW-LOW-LOW

A SCADA system is determined to have a potential impact from a loss of confidentiality as moderate, integrity as moderate and availability as high. C-I-A is MODERATE-MODERATE-HIGH

[FIPS 199, Standards for Security Categorization of Federal Information and Information Systems](#)

What is Impact Level?

The loss of confidentiality, integrity or availability could be expected to have a...

LIMITED (LOW)

SERIOUS (MODERATE)

SEVERE or CATASTROPHIC (HIGH)

...adverse effect on organizational operations, organizational assets, or individuals.

C-I-Aとは何か?

- **C – Confidentiality (秘匿性):** 秘匿性を失う事は情報の不当開示につながる
- **I – Integrity (完全性):** 完全性を失う事は情報の無断変更及び情報破棄につながる
- **A – Availability(可用性):** 可用性を失う事は情報又はシステムへのアクセス及び使用途絶につながる

Examples: FRCS supporting an administrative facility is determined to have a potential impact from a loss of confidentiality as low, integrity as low and availability as low. C-I-A is LOW-LOW-LOW

A SCADA system is determined to have a potential impact from a loss of confidentiality as moderate, integrity as moderate and availability as high. C-I-A is MODERATE-MODERATE-HIGH

[FIPS 199, Standards for Security Categorization of Federal Information and Information Systems](#)

インパクトレベルは何か?

秘匿性、完全性、可用性を失うという事は...

LIMITED (限定的)

SERIOUS (重大)

SEVERE or CATASTROPHIC (重度)

...組織活動、組織資産および人員に限定的、重大、重度の悪影響を及ぼすことになる

How Do We Incorporate Cybersecurity?

Verify Everything via Coordination with Government Cybersecurity POCs and Requests for Information (RFIs)

Basis of Design should identify:

- FRCS
- Network Transport
- Known (*or Assumed*) C-I-A per FRCS
- System Owner(s) (SO)
- Who is Responsible - Contractor or Government
- Any existing Authority to Operate (ATO) for any FRCS
- The Level the FRCS Performs at Based on the Control System Diagram in UFC 4-010-06

5-2 REQUIREMENTS BY DESIGN PHASE.

Cybersecurity documentation requirements are indicated here by typical Design-Build or Design-Bid-Build design submittals. If the design is using a different submittal schedule, adjust accordingly.

The requirements here reference the five step cybersecurity design process defined in CHAPTER 3.

5-2.1 Basis of Design.

Provide a single submittal indicating the C-I-A impact level for the control system and listing the security controls generated during Step 2 along with recommendations and justifications for further tailoring of the security control set.

どのようにサイバーセキュリティを取り入れるべきか？

政府サイバーセキュリティ担当者との調整
及び情報提供依頼書(RFI)を通して全てを確認
しなければならない

Basis of Design should identify:

- FRCS
- Network Transport
- Known (*or Assumed*) C-I-A per FRCS
- System Owner(s) (SO)
- Who is Responsible - Contractor or Government
- Any existing Authority to Operate (ATO) for any FRCS
- The Level the FRCS Performs at Based on the Control System Diagram in UFC 4-010-06

5-2 REQUIREMENTS BY DESIGN PHASE.

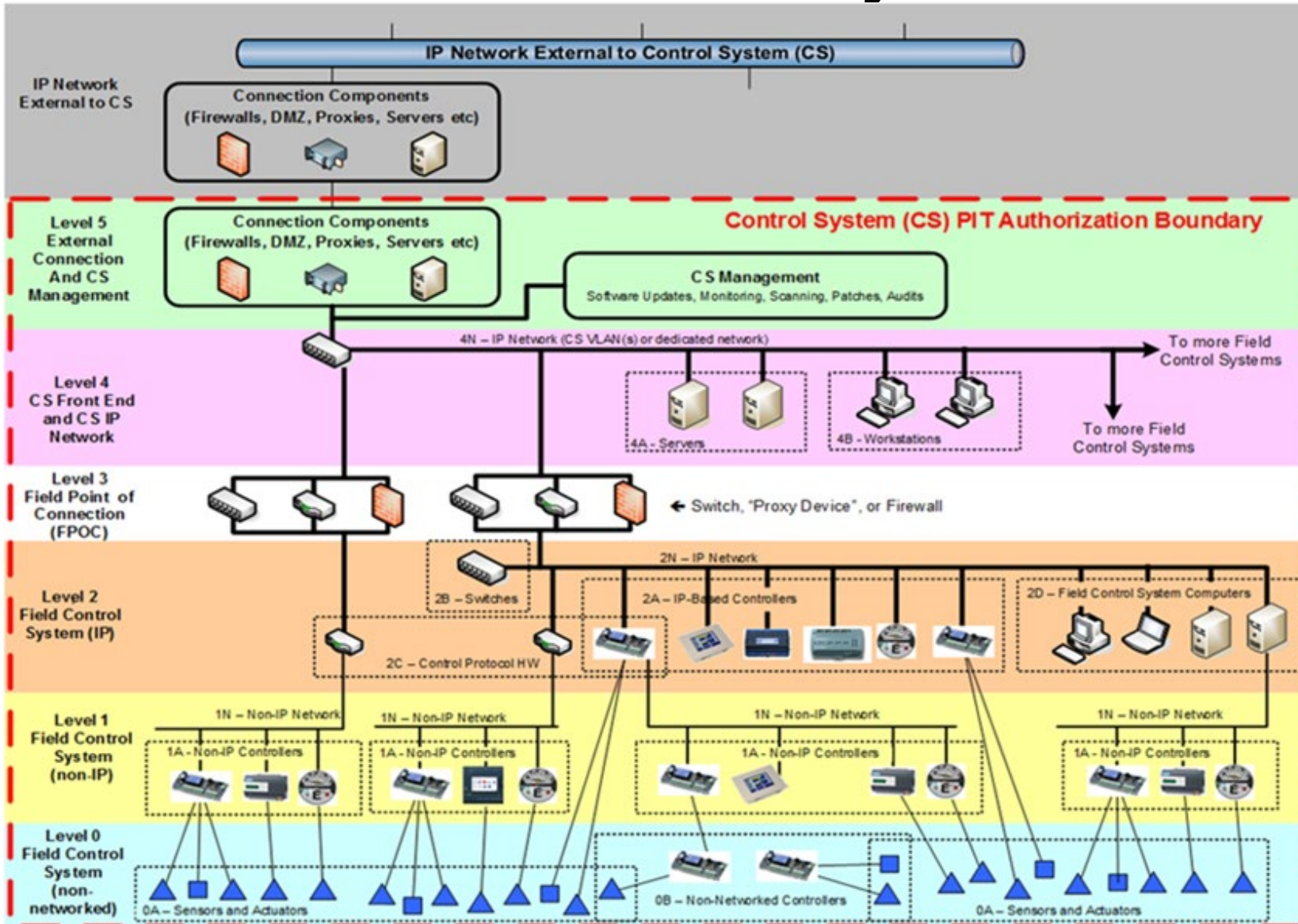
Cybersecurity documentation requirements are indicated here by typical Design-Build or Design-Bid-Build design submittals. If the design is using a different submittal schedule, adjust accordingly.

The requirements here reference the five step cybersecurity design process defined in CHAPTER 3.

5-2.1 Basis of Design.

Provide a single submittal indicating the C-I-A impact level for the control system and listing the security controls generated during Step 2 along with recommendations and justifications for further tailoring of the security control set.

UFC 4-010-06 5-Level Control System Architecture



What Level is the FRCS at?

Level 5: External Connection and Control System Management

Level 4: Control System Front End and Control System IP Network

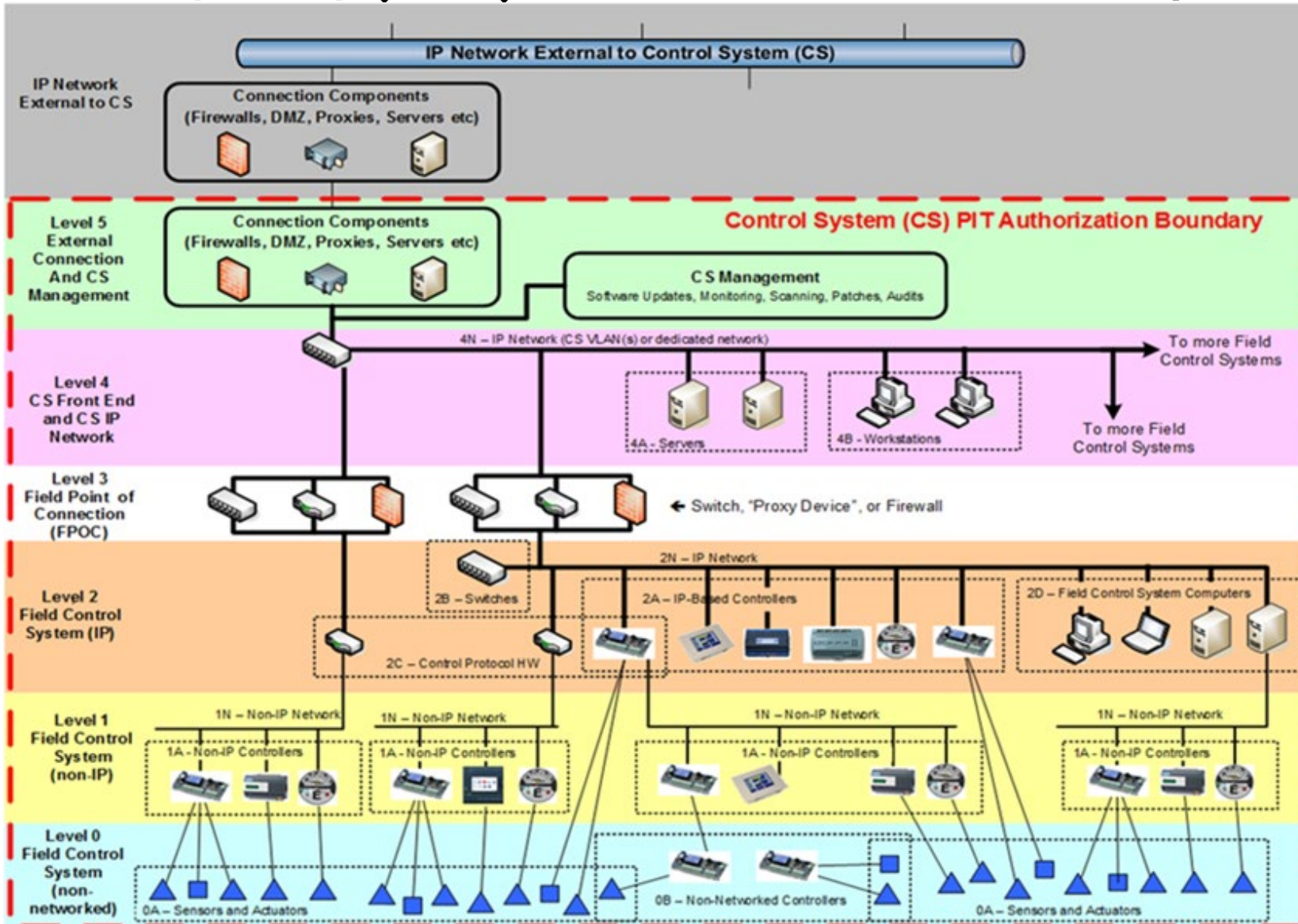
Level 3: Field Point of Connection (FPOC)

Level 2: Field Control System (IP)

Level 1: Field Control System (Non-IP)

Level 0: Sensors and Actuators

米国施設基準(UFC) 4-010-06 5-レベル別制御システム構造



What Level is the FRCS at?

Level 5: External Connection and Control System Management

Level 4: Control System Front End and Control System IP Network

Level 3: Field Point of Connection (FPOC)

Level 2: Field Control System (IP)

Level 1: Field Control System (Non-IP)

Level 0: Sensors and Actuators

How Do We Incorporate Cybersecurity?

Coordinate with Government Cybersecurity POCs for any “**HIGH**” Impact Level CCIs Required **Design Submittals** typically:

- ❑ 10-15% Submittal should include BOD, Initial CCI List per C-I-A for Each FRCS
- ❑ 35% Submittal should include BOD, Final CCI List per C-I-A for Each FRCS
- ❑ 50-65% Submittal should include all Each FRCS
- ❑ 90-100% Submittal should include Updates for Complete Final Information

5-2.2 Design Submittals.

5-2.2.1 Concept Design Submittal (10-15%).

Provide a single submittal indicating the CCIs resulting from the approved tailored security control list (Step 3) and an initial classification for each CCI (Step 4).

5-2.2.2 Design Development Submittal (35-50%).

Provide a single submittal documenting the following:

- The final classification of each CCI (Step 4).
- The changes to standard CCI requirements identified in Step 5, along with an explanation of the changes.
- The CCIs which have been incorporated into the control system design (Step 5). Document changes from standard requirements, or selections made when multiple options are available. Otherwise, it is not necessary to document the details of the requirement, just whether a specific CCI has been incorporated.
- Information for others as required (Step 5)

どのようにサイバーセキュリティを取り入れるべきか？

全ての**ハイ**インパクトレベルのCCIIに
関しては政府サイバーセキュリティ
担当者と調整しなければならない

Design Submittals typically:

- 10-15% Submittal should include BOD, Initial CCI List per C-I-A for Each FRCS
- 35% Submittal should include BOD, Final CCI List per C-I-A for Each FRCS
- 50-65% Submittal should include all of 35% and UFGS 25 05 11 Specifications for Each FRCS
- 90-100% Submittal should include Updates for Complete Final Information

5-2.2 Design Submittals.

5-2.2.1 Concept Design Submittal (10-15%).

Provide a single submittal indicating the CCIs resulting from the approved tailored security control list (Step 3) and an initial classification for each CCI (Step 4).

5-2.2.2 Design Development Submittal (35-50%).

Provide a single submittal documenting the following:

- The final classification of each CCI (Step 4).
- The changes to standard CCI requirements identified in Step 5, along with an explanation of the changes.
- The CCIs which have been incorporated into the control system design (Step 5). Document changes from standard requirements, or selections made when multiple options are available. Otherwise, it is not necessary to document the details of the requirement, just whether a specific CCI has been incorporated.
- Information for others as required (Step 5)

UFGS 25 05 11 Cybersecurity of Facility-Related Control Systems

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 TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

05/21

PART 1 GENERAL

- 1.1 CONTROL SYSTEM APPLICABILITY
- 1.2 RELATED REQUIREMENTS
- 1.3 REFERENCES
- 1.4 DEFINITIONS
 - 1.4.1 Administrator Account
 - 1.4.2 Computer
 - 1.4.3 Controller
 - 1.4.4 Mission Space
 - 1.4.5 Network
 - 1.4.6 Network Connected
 - 1.4.6.1 Wireless Network Connected
 - 1.4.7 Network Media
 - 1.4.8 User Account Support Levels
 - 1.4.8.1 FULLY Supported
 - 1.4.8.2 MINIMALLY Supported
 - 1.4.8.3 NOT Supported
 - 1.4.9 Manual Local Input
 - 1.4.10 Card Reader
 - 1.4.11 User Interface
 - 1.4.11.1 Local User Interface
 - 1.4.11.2 Remote User Interface
 - 1.4.11.3 Types of User Interface (by capability)
 - 1.4.11.3.1 Read-Only User Interface
 - 1.4.11.3.2 Limited User Interface
 - 1.4.11.3.3 Full User Interface
 - 1.4.11.3.4 View-Only User Interface
 - 1.4.11.4 Other User Interface Terminology
 - 1.4.11.4.1 Writable User Interface
 - 1.4.11.4.2 Privileged User Interface
 - 1.4.12 Wireless Network
 - 1.4.13 Wired Broadcast Network
- 1.5 ADMINISTRATIVE REQUIREMENTS
 - 1.5.1 Points of Contact
 - 1.5.2 Coordination

SECTION 25 05 11 Page 1

- [UFGS 25 05 11 Cybersecurity For Facility-Related Control Systems](#), Published May 2021
- Incorporates CCIs into Specification
- Implements Cybersecurity During Construction
- Requires Cybersecurity SME with Information Assurance Management (IAM) Level II
- Cybersecurity Submittals Support RMF
 - Templates Available on Whole Building Design Guide <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>
- One (1) UFGS 25 05 11 tailored for each FRCS

UFGS 25 05 11 Cybersecurity of Facility-Related Control Systems

施設制御システム(FRCS)におけるサイバーセキュリティー

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 UMLR dated April 2021

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

05/21

PART 1 GENERAL

- 1.1 CONTROL SYSTEM APPLICABILITY
- 1.2 RELATED REQUIREMENTS
- 1.3 REFERENCES
- 1.4 DEFINITIONS
 - 1.4.1 Administrator Account
 - 1.4.2 Computer
 - 1.4.3 Controller
 - 1.4.4 Mission Space
 - 1.4.5 Network
 - 1.4.6 Network Connected
 - 1.4.6.1 Wireless Network Connected
 - 1.4.7 Network Media
 - 1.4.8 User Account Support Levels
 - 1.4.8.1 FULLY Supported
 - 1.4.8.2 MINIMALLY Supported
 - 1.4.8.3 NOT Supported
 - 1.4.9 Manual Local Input
 - 1.4.10 Card Reader
 - 1.4.11 User Interface
 - 1.4.11.1 Local User Interface
 - 1.4.11.2 Remote User Interface
 - 1.4.11.3 Types of User Interface (by capability)
 - 1.4.11.3.1 Read-Only User Interface
 - 1.4.11.3.2 Limited User Interface
 - 1.4.11.3.3 Full User Interface
 - 1.4.11.3.4 View-Only User Interface
 - 1.4.11.4 Other User Interface Terminology
 - 1.4.11.4.1 Writable User Interface
 - 1.4.11.4.2 Privileged User Interface
 - 1.4.12 Wireless Network
 - 1.4.13 Wired Broadcast Network
- 1.5 ADMINISTRATIVE REQUIREMENTS
 - 1.5.1 Points of Contact
 - 1.5.2 Coordination

SECTION 25 05 11 Page 1

- UFGS 25 05 11 Cybersecurity For Facility-Related Control Systems, 施設制御システムにおけるサイバーセキュリティー 2021年5月発行
- 制御相関ID (CCI)を仕様書に加える
- 建設過程でサイバーセキュリティーを実行する
- Information Assurance Management (IAM) Level IIの資格を有する専門家を必要とする
- リスクマネージメントフレームワーク(RMF)確認するサイバーセキュリティー提出書類
 - テンプレートはWhole Building Design Guide参照
<https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11>
- 各施設制御システム(FRCS)毎に"UFGS 25 05 11"を1部作成

UFGS 25 08 11.00 20 (NAVY Only) RMF for FRCS

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

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated January 2022
*****

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 08 11.00 20

RISK MANAGEMENT FRAMEWORK FOR FACILITY-RELATED CONTROL SYSTEMS

11/20

PART 1  GENERAL

1.1  CONTROL SYSTEM APPLICABILITY
1.2  RELATED REQUIREMENTS
1.3  REFERENCES
1.4  DEFINITIONS
1.4.1 Assured Compliance Assessment Solution (ACAS) Scans
1.4.2 Authority To Operate (ATO)
1.4.3 Control Correlation Identifier (CCI) or Security Control
1.4.4 Enterprise Mission Assurance Support Service (eMASS)
1.4.5 Functional Authorizing Official (FAO) or Authorizing Official
(AO)
1.4.6 Information System Owner (ISO) or System Owner (SO)
1.4.7 Information System Security Manager (ISSM)
1.4.8 Information System Security Engineer (ISSE)
1.4.9 Risk Management Framework (RMF)
1.4.10 Security Assessment Plan (SAP)
1.4.11 Security Assessment Report (SAR)
1.4.12 Security Content Automation Protocol (SCAP)
1.4.13 Security Control Accessor - Validator (SCA-V)
1.4.14 Security Plan (SP)
1.4.15 Security Technical Implementation Guidance (STIG)
1.5  ADMINISTRATIVE REQUIREMENTS
1.5.1 Coordination
1.6  SUBMITTALS
1.7  QUALITY CONTROL
1.7.1 Certifications
1.8  CYBERSECURITY DOCUMENTATION
1.8.1 Authorization Strategy Plan

PART 2  PRODUCTS

2.1  SPARE PARTS

SECTION 25 08 11.00 20 Page 1
```

- [UFGS 25 08 11.00 20 Risk Management Framework for Facility-Related Control Systems](#)
 - Published November 2020 – Navy Only specification
 - One (1) UFGS 25 08 11 for all FRCS requiring ATO
- Implements the Navy requirements to support the Risk Management (RMF) Cybersecurity During Construction
- Requires Information System Security Engineer (ISSE) with Information Assurance Technical (IAT) Level II and ability to obtain a Common Access Card (CAC).
- Cybersecurity Submittals Support RMF
 - Templates Available on Whole Building Design Guide <https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-08-11-00-20>

UFGS 25 08 11.00 20 (米海軍のみ)施設制御システム(FRCS)における リスクマネージメントフレームワーク(RMF)

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

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated January 2022
*****

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 08 11.00 20

RISK MANAGEMENT FRAMEWORK FOR FACILITY-RELATED CONTROL SYSTEMS

11/20

PART 1  GENERAL

1.1  CONTROL SYSTEM APPLICABILITY
1.2  RELATED REQUIREMENTS
1.3  REFERENCES
1.4  DEFINITIONS
1.4.1 Assured Compliance Assessment Solution (ACAS) Scans
1.4.2 Authority To Operate (ATO)
1.4.3 Control Correlation Identifier (CCI) or Security Control
1.4.4 Enterprise Mission Assurance Support Service (eMASS)
1.4.5 Functional Authorizing Official (FAO) or Authorizing Official
(AO)
1.4.6 Information System Owner (ISO) or System Owner (SO)
1.4.7 Information System Security Manager (ISSM)
1.4.8 Information System Security Engineer (ISSE)
1.4.9 Risk Management Framework (RMF)
1.4.10 Security Assessment Plan (SAP)
1.4.11 Security Assessment Report (SAR)
1.4.12 Security Content Automation Protocol (SCAP)
1.4.13 Security Control Accessor - Validator (SCA-V)
1.4.14 Security Plan (SP)
1.4.15 Security Technical Implementation Guidance (STIG)
1.5  ADMINISTRATIVE REQUIREMENTS
1.5.1 Coordination
1.6  SUBMITTALS
1.7  QUALITY CONTROL
1.7.1 Certifications
1.8  CYBERSECURITY DOCUMENTATION
1.8.1 Authorization Strategy Plan

PART 2  PRODUCTS

2.1  SPARE PARTS

SECTION 25 08 11.00 20 Page 1
```

- [UFGS 25 08 11.00 20 Risk Management Framework for Facility-Related Control Systems](#) 施設制御システムにおけるリスクマネージメントフレームワーク
 - 2020年11月発行 - 米海軍仕様書
 - 承認者(ATO)を必要とする全ての施設制御システム (FRCS) につき “UFGS 25 08 11”1部作成
- 建設過程でリスクマネージメントフレームワークサイバーセキュリティを維持する米海軍要件を実行する
- Information Assurance Technical (IAT) Level IIの資格を持ちコモンアクセスカード(CAC)を取得可能であるInformation System Security Engineer (ISSE)を必要とする
- リスクマネージメントフレームワーク(RMF)を確認するサイバーセキュリティ提出書類
- テンプレートはWhole Building Design Guide参照
<https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-08-11-00-20>

SAME Japan Industry Forum

Facility-Related Control System (FRCS) Cybersecurity

Thank you!

Lynn Wachi, APAC Federal Cybersecurity Discipline Lead
lynn.wachi@jacobs.com / (808) 440-0252



Challenging today.
Reinventing tomorrow.



©Jacobs 2020