Mission-Critical Control System (MCCS) Cybersecurity

Mitigating Legacy & Securing Next-Generation Operational Technology/MCCS

17 August 2022

Michael Dransfield
Control Systems Cybersecurity
National Security Agency

MCCS Cybersecurity

Mission-Critical Control Systems (MCCSs) are information systems owned by the U.S. government (USG) which monitor and/or control physical infrastructures critical to the direct fulfillment of military or intelligence missions.

Mission-Critical - Facility-Related Control Systems (MC-FRCSs) are a critical type of MCCSs; others include, industrial, process, and utility control systems.

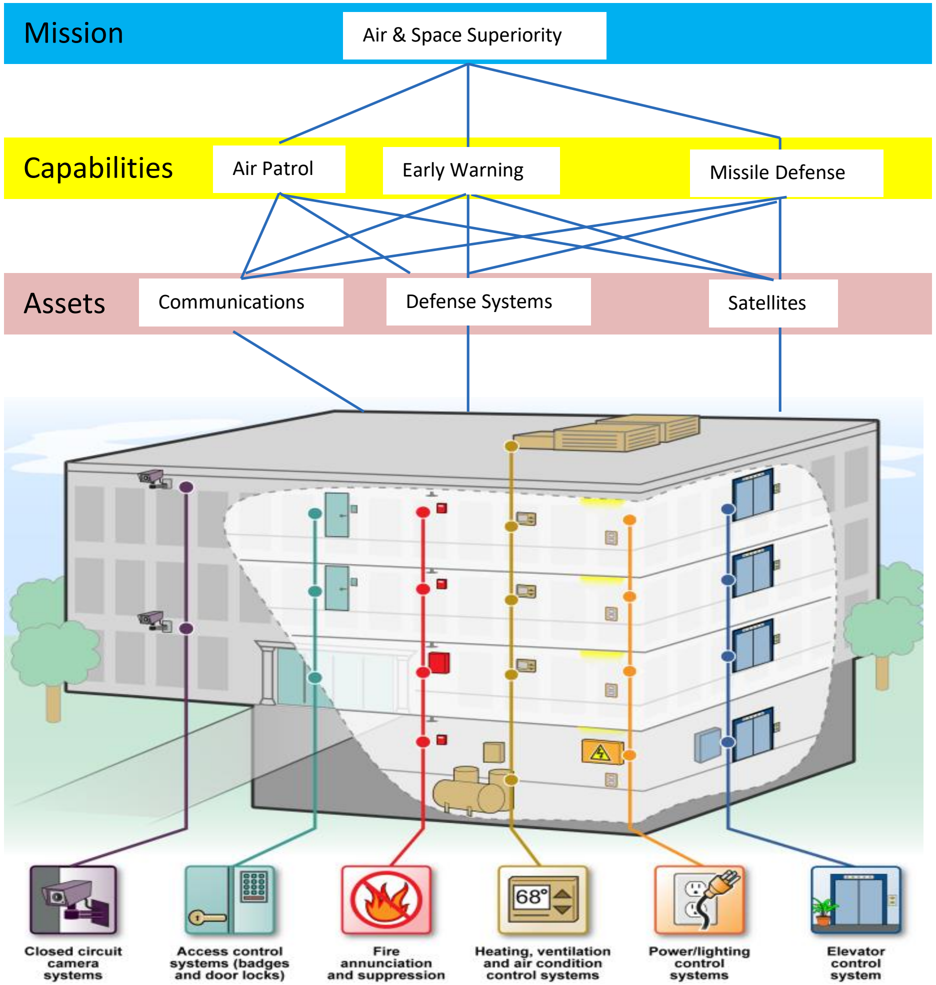
Intelligence Community Standard 706-02 for MC-FRCS Cybersecurity:

https://www.odni.gov/files/NCSC/documents/Regulations/20200114-ICS_706-02_Protecting_MCFRC_in_MCF.pdf

Mission's Dependency on Critical Control Systems

Current W&S Oversight

Current Facilities Oversight



Mission: Air & Space Superiority

Capabilities: Air Patrol, Early Warning, Missile Defense

Assets: Communications, Defense Systems, Satellites

Closed circuit camera systems
Access control systems (badges and door locks)
Fire annunciation and suppression
Heating, ventilation and air condition control systems
Power/lighting control systems
Elevator control system
68°

Image: GAO-15-6 Federal Facility Cybersecurity (December 2014)

Mission’s Dependency on Critical Control Systems

Future DoD Strategic Oversight

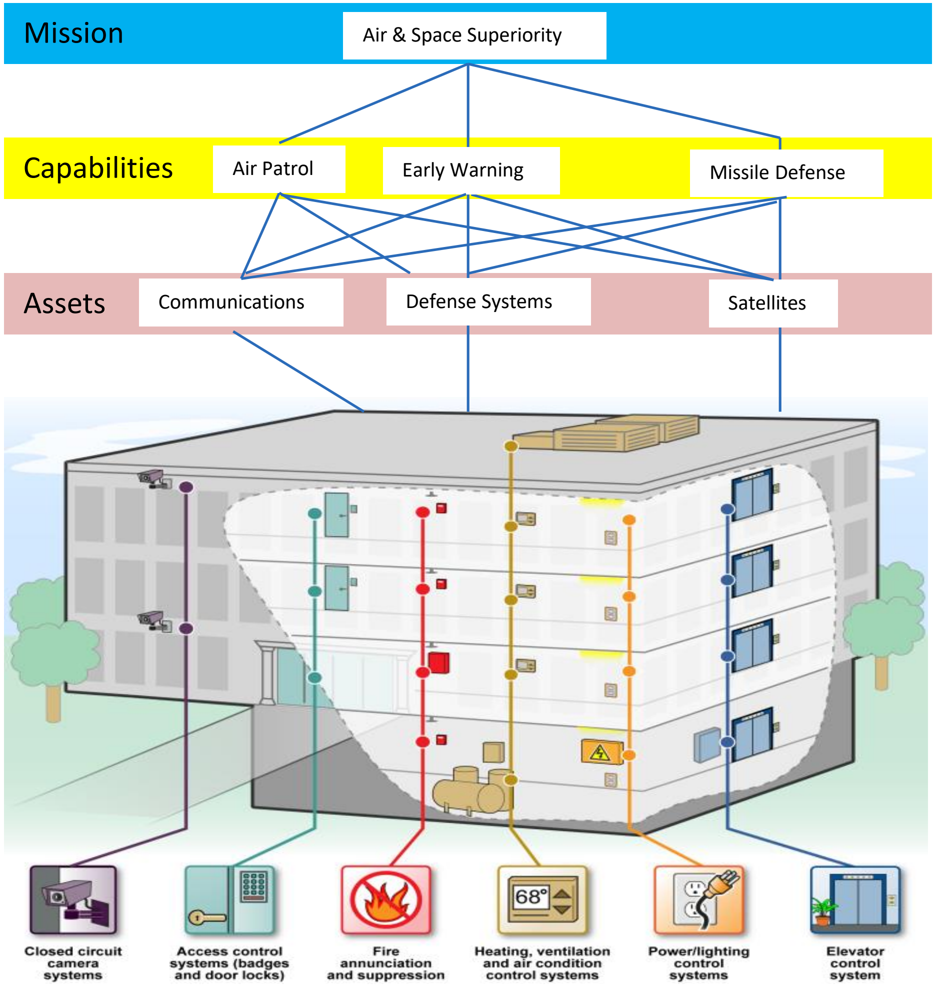

Mission
Air & Space Superiority
Capabilities
Air Patrol
Early Warning
Missile Defense
Assets
Communications
Defense Systems
Satellites
68°
Closed circuit camera systems
Access control systems (badges and door locks)
Fire annunciation and suppression
Heating, ventilation and air condition control systems
Power/lighting control systems
Elevator control system

Image: GAO-15-6 Federal Facility Cybersecurity (December 2014)

MCCS Cybersecurity

Current Two-Pronged Strategy:

- Tactical: Mitigate Vulnerable Legacy MCCSs
- Strategic: Design & Build Future Cybersecure MCCSs

MCCS Cybersecurity

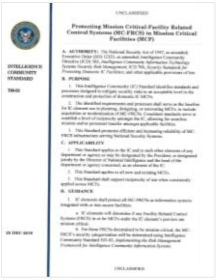
Tactical: Mitigate Vulnerable Legacy MCCSs

- Complex problem (People, Process, Technology)
- Current Efforts:
  - NSA's National Manager Memo (NMM) for MC-FRCS Cybersecurity
  - Operational Technology (OT) Defensive Capability Suite
    - Shared through NSA TTSA (OT tools, SOP, OT-STIGs)
  - Applied Control System Mitigations (ACSM) Methodology
    - Identify/Harden MCCS Boundary
    - Establish MCCS Security Controls
      - Leverage IC MC-FRCS Standard (MODERATE+ baseline)
    - Prioritize, Design, & Assist Implementation of Operational Risk Mitigations
      - Leverage MC-FRCS Technical Implementation Guide v1.0 DRAFT
      - Leverage Partner Solutions

MCCS Cybersecurity

Strategic: Design & Build Cybersecure MCCSs

- IC Facilities Cybersecurity Standard (ICS 706-02)
- ICS 706-02 Technical Implementation Guide (v1.0 DRAFT)
- International Standards
  - ISA 62443 Multi-Part Standard, Security & Maturity Levels
  - ASHRAE – Secure Connect (BACNet Protocol)
- ISA Security Compliance Institute (ISCI)
  - ISA-SECURE Conformance Testing
- Zero Trust Architecture for MCCSs
  - White paper in development



UNCLASSIFIED

INTELLIGENCE COMMUNITY STANDARD

706-02

20 DEC 2018

Protecting Mission Critical-Facility Related Control Systems (MC-FRCS) in Mission Critical Facilities (MCF)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management*; ICD 705, *Security Standards for Protecting Domestic IC Facilities*; and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community (IC) Standard identifies standards and processes designed to mitigate security risks to an acceptable level in the construction and protection of domestic IC MCFs.

2. [illegible]

3. This Standard promotes efficient and increasing reliability of MC-FRCS infrastructure serving National Security Systems.

C. APPLICABILITY

1. [illegible]

2. This Standard applies to all new and existing MCFs.

3. [illegible]

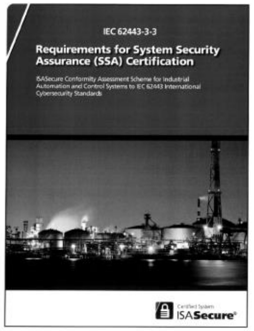
D. GUIDANCE

1. [illegible]

a. [illegible]

b. [illegible]

UNCLASSIFIED



IEC 62443-3-3

Requirements for System Security Assurance (SSA) Certification

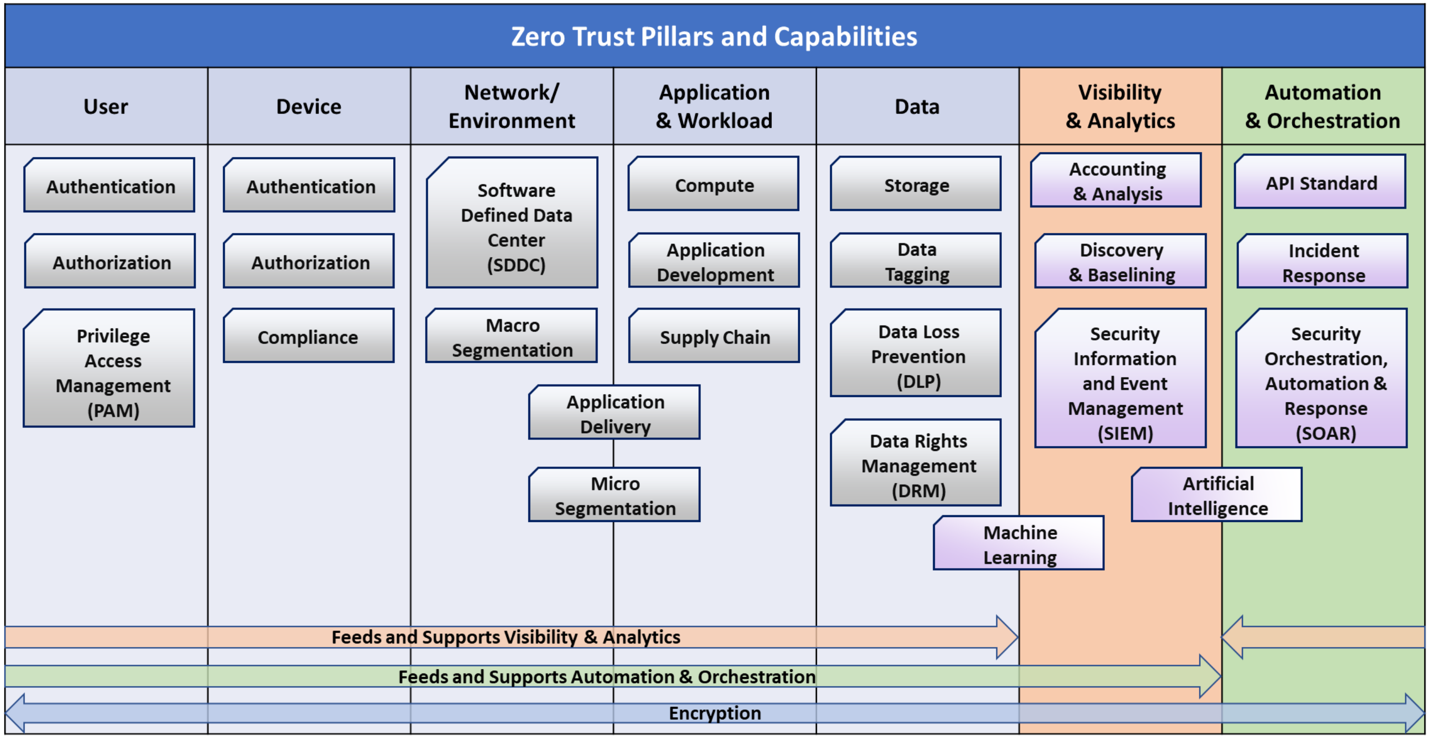
ISASecure Conformity Assessment Scheme for Industrial Automation and Control Systems to IEC 62443 International Cybersecurity Standards

Certified System ISASecure®

Zero Trust (ZT) Fundamentals

Principles:

- Assume hostile environment
- Assume breach
- Least privilege accesses
- Persistent engagement
- MFA with contextual assessment



Zero Trust Pillars and Capabilities

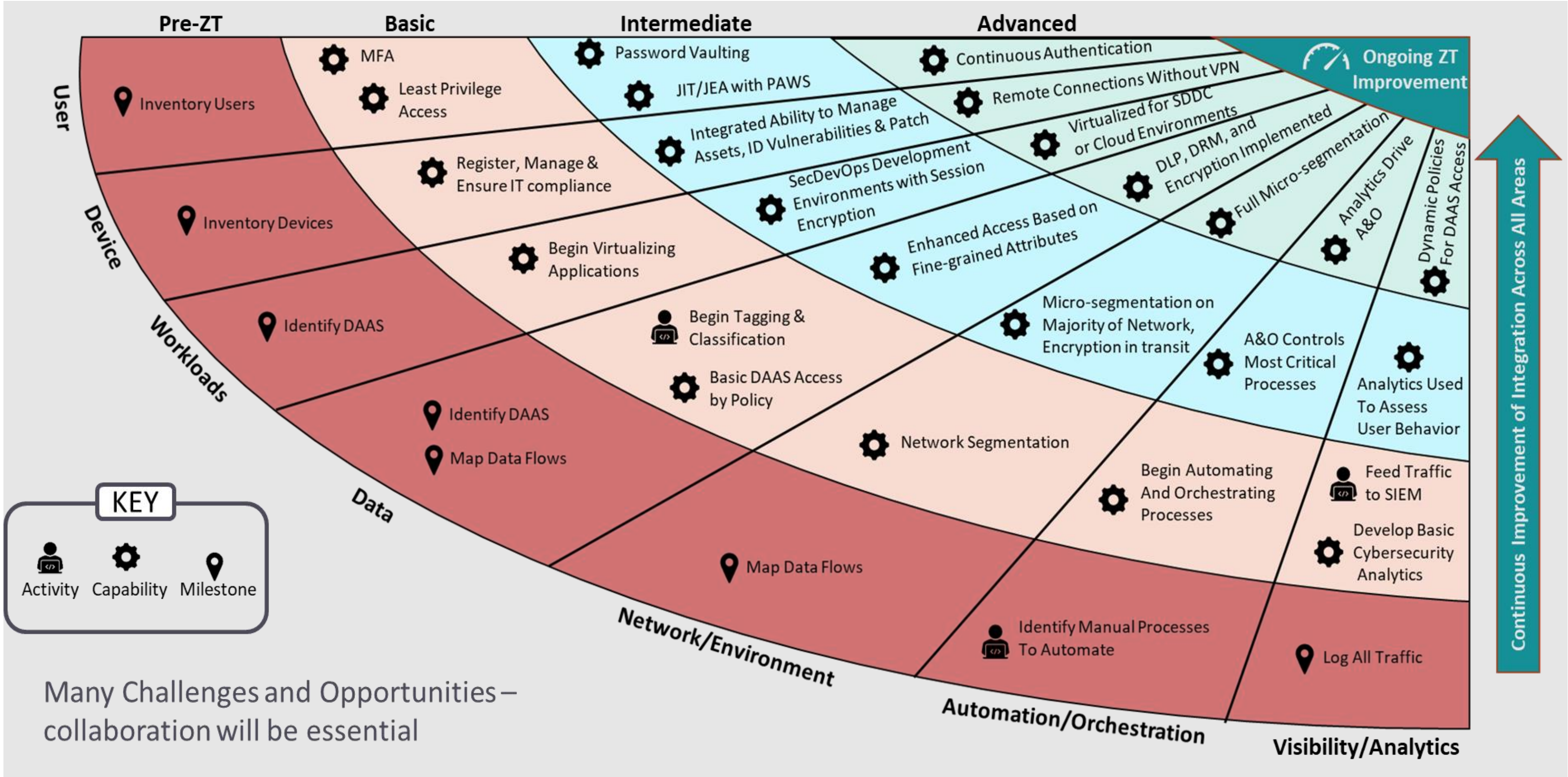
User	Device	Network/ Environment	Application & Workload	Data	Visibility & Analytics	Automation & Orchestration
Authentication	Authentication	Software Defined Data Center (SDDC)	Compute	Storage	Accounting & Analysis	API Standard
Authorization	Authorization		Application Development	Data Tagging	Discovery & Baselining	Incident Response
Privilege Access Management (PAM)	Compliance	Macro Segmentation	Supply Chain	Data Loss Prevention (DLP)	Security Information and Event Management (SIEM)	Security Orchestration, Automation & Response (SOAR)
		Application Delivery		Data Rights Management (DRM)	Artificial Intelligence	
		Micro Segmentation		Machine Learning		

Feeds and Supports Visibility & Analytics

Feeds and Supports Automation & Orchestration

Encryption

ZT Maturity Stages



Pre-ZT

Basic

Intermediate

Advanced

Ongoing ZT Improvement

User

Inventory Users

MFA

Least Privilege Access

Password Vaulting

JIT/JEA with PAWS

Continuous Authentication

Remote Connections Without VPN

Device

Inventory Devices

Register, Manage & Ensure IT compliance

Integrated Ability to Manage Assets, ID Vulnerabilities & Patch

Virtualized for SDDC or Cloud Environments

Workloads

Identify DAAS

Begin Virtualizing Applications

SecDevOps Development Environments with Session Encryption

DLP, DRM, and Encryption Implemented

Data

Identify DAAS

Map Data Flows

Begin Tagging & Classification

Basic DAAS Access by Policy

Enhanced Access Based on Fine-grained Attributes

Full Micro-segmentation

Network/Environment

Map Data Flows

Network Segmentation

Micro-segmentation on Majority of Network, Encryption in transit

Analytics Drive A&O

Automation/Orchestration

Identify Manual Processes To Automate

Begin Automating And Orchestrating Processes

A&O Controls Most Critical Processes

Dynamic Policies For DAAS Access

Visibility/Analytics

Log All Traffic

Feed Traffic to SIEM

Develop Basic Cybersecurity Analytics

Analytics Used To Assess User Behavior

Continuous Improvement of Integration Across All Areas

KEY

Activity

Capability

Milestone

Many Challenges and Opportunities – collaboration will be essential

MCCS & ZT

- MCCSs utilize both IT and OT components (within authorization boundary)
- ZT concepts can be applied to IT, not well to legacy OT
- Rip/replace is not an option for most USG MCCS owners
- NSA developing the OT Access Security Broker (OTASB) Concept
    - Support migration of legacy MCCS to meet ZT architecture goals
    - Provide cybersecurity properties to OT legacy components (e.g., access control, command authentication, encryption when needed, etc.)
    - OT SDN provides critical support for OTASB properties

MCCS Cybersecurity

How can NSA’s work on MCCS Cybersecurity help you?

Backup Slides

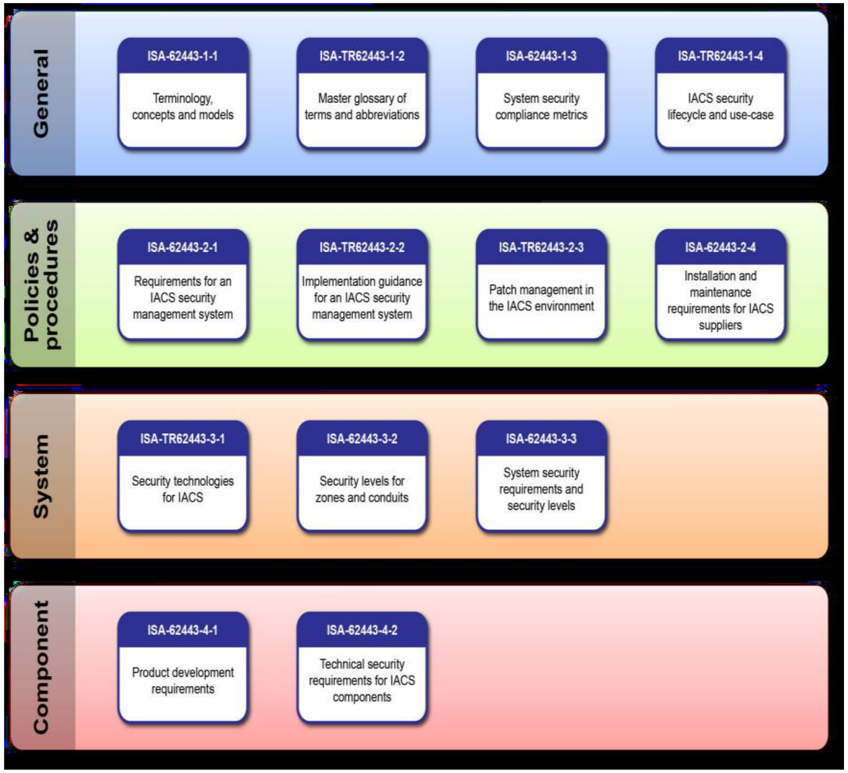
MCCS Cybersecurity

Leverage security controls into design concepts & solution:

- Define mission outcomes – Derive a zero trust architecture from organization-specific mission requirements that identify the critical data/assets/applications/services (DAAS);
- Architect from the "left-side (developmental-side)" out:
  - First, focus on protecting critical DAAS;
  - Second, secure all paths to access DAAS;
- Determine who/what needs access to the DAAS to create access control policies –
  - Create security procedures & policies;
  - Apply it consistently across all environments;
    (LAN, WAN, endpoint, perimeter, mobile, etc.)

International CS Cybersecurity Standard

Control system vendor community must implement necessary cybersecurity functionality into products/systems. Many are currently using the ISA-62443 as a guide to their product/system cybersecurity frameworks.



General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Policies & procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Installation and maintenance requirements for IACS suppliers
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components

Why focus on ISA99 (creating the ISA-62443)?

Broad Community Membership

- EP, ONG, BMS, IOT customers and vendors
- NSA, NIST, CS security community

ISASecure

- Independent testing
- Conformance to ISA-62443 standard

IC Standard 706-2 for CS Cybersecurity

Development of the Standard - Signed in December 2019

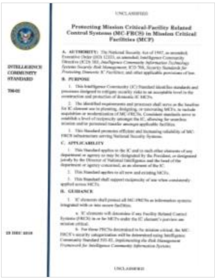
Driving Philosophy: Utilize and build upon existing standards

Building Blocks:

- NIST SP 800-37 : Applying RMF to Federal Information Systems
- NIST SP 800-53 : Security & Privacy Controls for IT Systems
- NIST SP 800-82 : Guide to Industrial Control System Security
- DOD UFC 4-010-06 : Cybersecurity of Facility-Related Control Systems

Technical Implementation Guide (TIG) – V1.0 (DRAFT)

- Prioritized security controls selected from
  - NIST 800-53 rev4 families
- Supplement to 800-82 rev 2 (currently, rev 3 in development)



UNCLASSIFIED

INTELLIGENCE COMMUNITY STANDARD

706-02

Protecting Mission Critical-Facility Related Control Systems (MC-FRCS) in Mission Critical Facilities (MCF)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management*; ICD 705, *Security Standards for Protecting Domestic IC Facilities*; and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community (IC) Standard identifies standards and processes designed to mitigate security risks to an acceptable level in the construction and protection of domestic IC MCFs.

2. The identified requirements and processes shall serve as the baseline for IC element use in planning, designing, or renovating MCFs, to include acquisition or modernization of MC-FRCSs. Consistent standards serve to establish a level of reciprocity amongst the IC, allowing for seamless mission and/or personnel transfer amongst applicable facilities.

3. This Standard promotes efficient and increasing reliability of MC-FRCS infrastructure serving National Security Systems.

C. APPLICABILITY

1. This Standard applies to the IC and to such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

2. This Standard applies to all new and existing MCFs.

3. This Standard shall support reciprocity of use when consistently applied across MCFs.

D. GUIDANCE

1. IC elements shall protect all MC-FRCSs as information systems integrated with or into secure facilities.

a. IC elements will determine if any Facility Related Control Systems (FRCS) in or for MCFs under the IC element's purview are mission critical.

b. For those FRCSs determined to be mission critical, the MC-FRCS's security categorization will be determined using Intelligence Community Standard 503-03, *Implementing the Risk Management Framework for Intelligence Community Information Systems*.

23 DEC 2019

UNCLASSIFIED

Zero Trust (ZT) in MCCS (NSA issued advisory memo in 2021):

Security of Mission-Critical – Facility-Related Control Systems (MC-FRCSs) directing owner/operators to immediately:

- Adopt IC Standard 706-02 for MC-FRCS Cybersecurity,[1]
- Implement specific cybersecurity risk mitigation guidance to address most risky access vectors, and
- Develop strategic Plan of Actions & Milestones (POA&Ms) to fully implement the MC-FRCS IC standard to strengthen mission resilience (consistent with ZTarchitecture concepts)

Note: MC-FRCSs are a critical type of MCCS; others include industrial, process, and utility control systems

[1] https://www.odni.gov/files/NCSC/documents/Regulations/20200114-ICS_706-02_Protecting_MCFRC_in_MCF.pdf