Tinker Air Force Base Facility Standard - Attachment C

BASE MECHANICAL STANDARD

Tinker Air Force Base, Oklahoma

ISSUED: AUG-2020

NOTICE

In addition to the TAFB Facility Standard, compliance with applicable United Facilities Criteria (UFC), Air Force Instruction (AFI) and other requirement in effect upon Contract Solicitation and/or Award, whichever applies, is required. The contractor shall be responsible to review all publications referenced herein to determine applicability to specific project requirements.

TABLE OF CONTENTS

Section	Title	Page
I	Energy Conservation Requirements	3
II	Fire Protection Engineering	7
III	Mechanical Engineering: *Plumbing Systems*	9
IV	Mechanical Engineering: *HVAC/R Systems*	15
V	Appendix	25

APPROVING OFFICIAL:

WILSON.STEPHANIE.PETERENIA.1063234377

Digitally signed by WILSON.STEPHANIE.PETERENIA.1063234377
Date: 2020.09.21 16:36:19 -05'00'

Stephanie Wilson
Base Civil Engineer
Civil Engineer Directorate, 72 ABW

[This page is intentionally blank]

I. Energy Conservation Requirements

A. Facilities shall include those energy conservation design features which can be economically justified or are otherwise required by UFC in conjunction with this TAFB Facility Standard. Principal considerations are building envelope and mechanical systems design and operation to minimize the use of fossil fuels.

1. Additional guidance may be found in prevailing Executive Orders in effect.

B. Minimum Efficiency Requirements

1. Minimum Energy Efficiency Requirements of buildings are established by the American National Standards Institute (ANSI), the American Society of Heating, Refrigerating & Air-Conditioning Engineers (ASHRAE) and the Illuminating Engineering Society (IES) and published in two separate standards. These standards are incorporated by reference into UFC 3-410-01 *Heating, Ventilating and Air Conditioning Systems.*
2. **ANSI/ASHRAE/IES Standard 90.1 - *Energy Standard for Buildings Except Low-Rise Residential Buildings*** (latest edition) establishes minimum efficiency and performance requirements for the following:
   a) Building Envelope
   b) Heating, Ventilating, Air-Conditioning, Refrigeration (HVAC/R)
   c) Service Water Heating (Boilers, Water Heaters)
   d) Power
   e) Lighting
   f) Other Equipment (Electric Motors, Service Water Pressure Booster Systems, Elevators, Escalators and Moving Walks)

   Note: *ASNI/ASHRAE/IES Standard 90.1 applies to new and existing building facilities at TAFB (except low-rise residential buildings).*
3. **ANSI/ASHRAE Standard 90.2** - ***Energy Efficient Design of Low-Rise Residential Buildings*** (latest edition) establishes design requirements for single-family houses, multi-family structures of three stories or fewer above grade, and manufactured houses (modular and mobile).

C. Energy Metering

1. Energy usage metering shall be provided for all projects in accordance with UFC 3-401-01 *Mechanical Engineering*, **ANSI/ASHRAE/IES Standard 90.1** - ***Energy Standard for Buildings Except Low-Rise Residential Buildings*****,** and the most recent Energy Policy Act.
2. Reference the most current version of the "Air Force Meter Data Management Plan" maintained by AFCEC. This can be found at the following link: https://cs2.eis.af.mil/sites/10159/SitePages/Service%20Page.aspx?Service=Air%20Force%20Facility%20Metering%20Program
3. All meters shall meet the minimum requirement of the AF's Advanced Meter Reading System (AMRS).
4. AMRS and Utility Metering Requirements include but are not limited to:
   a) New Gas and Water meters and replacement of existing analog Gas and Water meters shall, as a minimum, be equipped with pulse output which can be connected to an external pulse accumulator/counter. Pulse accumulators may be supplied by others. Pulse accumulators and digital "smart" Gas and Water meters must, as a minimum, communicate using Modbus TCP protocol with the AMRS system at Tinker AFB. Daily totalized consumption is required for a minimum of 90 days.
   b) Electric Meters; a) 15-minute interval data with 30 days memory, b) local, scrolling LED or LCD display, c) hand-held data reader support (Bluetooth wireless or Optical Port), d)

Minimum data recorded to include; kWh, kW demand, kVARh, kVAR demand, power factor, e) Communicate using Modbus TCP protocol with the AMRS system at Tinker AFB.

D. Energy Management Considerations

1. Other items for consideration for energy conservation are economy cooling cycle, variable volume systems, and night and weekend system shutdown. Controls for night and weekend setup/setback of space temperature shall be provided for all areas.
2. Air-Conditioning of Occupied Spaces. Occupancies where air conditioning is permitted shall be per UFC 3-410-01.

E. Computer Analysis

1. For all major Military Construction (MILCON) projects, computer dynamic analysis techniques shall be utilized to effectively evaluate all design parameters associated with energy conservation design.
2. In addition to the calculations and analysis requirements indicated in UFC 3-401-01, provide calculations listed in UFC 3-410-01 Chapter 5, part 5-1.2, including an Energy Compliance Analysis (ECA), "U" Factor calculations, HVAC Load Calculations, Outside Air Requirements/ Calculations, Building Air Balance Calculations, Duct Pressure Drop Calculations, Hydronic System Pressure Drop Calculations, Pipe Expansion Calculations, and Equipment Sizing Calculations.

F. Life Cycle Cost Analysis

1. Design features shall be evaluated via life-cycle cost analysis. The various alternatives and their costs evaluated during design shall be documented by the designer and included in submittals.
2. The National Institute of Standards and Technology (NIST) has prepared the Life Cycle Costing Manual for the Federal Energy Management Program (NIST Handbook 135), and annually issues real growth energy price indices and discount factors for life cycle cost analysis. As a companion product, NIST has also established the Building Life Cycle Cost (BLCC) computer program to perform LCC analyses. The latest versions of the BLCC program not only structure the analysis but also include current energy price indices and discount factor references. These NIST materials define all required LCC methodologies used in GSA design applications. The A/E may obtain the BLCC software and updates from NIST. The project team must integrate the LCC analysis into the concept design process, and the analysis must be completed by the design development phase. Facilities Standard for the Public Buildings Service P100 - Chapter 1.7 - Life-Cycle Costing by GSA.

G. Design and Construction of Energy Monitoring Control Systems (EMCS)

1. An energy monitoring control system shall be provided for all projects in accordance with UFC 3-401-01 *Mechanical Engineering*, ANSI/ASHRAE/IES Standard 90.1 - *Energy Standard for Buildings Except Low-Rise Residential Buildings*, and the most recent Energy Policy Act.
2. All stages of EMCS designs shall be coordinated with the Energy Management Program monitor in the Utility Engineering section (72 ABW / CECO) and HQ AFMC. All installed control systems shall be connected to the existing base wide Civil Engineering Community Of Interest Network Enclave (CE COINE). The control system contractor shall contact the base Information Technology (IT) contractor for pricing and include this pricing in their estimate and scope to include the installation of the Ethernet drops and corresponding network IP addresses in the quantity and location detailed and required by the controls contractor. The control systems shall be integrated into the base wide Energy Management and Control Systems (EMCS's) that are approved for Authority to Operate (ATO). These system vendors are Automated Building Systems, Inc., Honeywell and Paragon Robotics. Contractor shall contact and coordinate connections with the CE Information System Security Manager (ISSM), the CE Energy Management office and CE Operations.

3. **Control Protocol.** ASHRAE's BACnet® protocol is the required system for Tinker AFB facility monitoring and control systems. Facility HVAC control systems based on the BACnet® protocol must be designed and constructed in accordance with ANSI/ASHRAE Standard 135, UFGS 23 09 00, UFGS 23 09 23.02 and UFGS 23 09 13. For additional information refer to specific UFCs such as UFC 3-401-01 *Mechanical Engineering* and UFC 3-410-01 *Heating, Ventilating, and Air Conditioning Systems.*

4. Civil Engineer-owned, operated, or maintained control systems shall follow policy directives published in **Air Force Guidance Memorandum AFGM 2018-32-01** *Civil Engineer Control Systems Cybersecurity* (or latest edition), and AF CE CS *Cybersecurity Plan v 2.0* submitted 17-Sep-18. In addition, follow guidance published in UFC 4-010-06 Cybersecurity of Facility-Related Control Systems. Additional guidance is found in the Appendix section of this Standard, US DoD publication FACILITY-RELATED CONTROL SYSTEMS CYBERSECURITY GUIDELINE.

5. **System Design Requirements**

   Mechanical and electrical systems in facilities shall be provided with the necessary sensors, controls, and hardware points to implement the EMCS application programs per UFC 3-410-01 *Heating, Ventilating, and Air Conditioning Systems* (latest edition), following the guidance for ASHRAE BACnet® monitoring and control of the systems.

   a. The new and replacement network controllers shall be selected to be fully functional and seamlessly compatible with the equipment controllers such that the base operations control technicians utilize their systems training and system support tools to maintain, configure and program both the network controllers and the equipment controllers at the same time.

   b. Control system designers shall submit the proposed schedule of points to be monitored and/or controlled in the I/O summary table format as outlined UFC 3-410-01 *Heating, Ventilating, and Air Conditioning Systems* (latest edition). For additional requirements, consult other sections within the TAFB Facility Standards (such as the requirement for vibration isolation sensing and monitoring controls listed in Section IV herein).

   c. Site-specific schematics shall be provided showing all sensors, controls, and hardware points.

   d. Pneumatic HVAC controls are no longer allowed at Tinker AFB. All projects modifying, replacing, or installing HVAC controls shall utilize DDC.

   e. The new installation/replacement shall be coordinated in a way that does not interfere with existing performance contract(s) (ESPC/UESC) in place, where the majority of the specified areas are dictated by such contracts. In a building where the existing performance contract covers only a part of the area or systems, any controller may be selected as long as such installation does not interfere with the existing performance contract. Such controller shall be fully compatible with the existing EMCS's that are approved for ATO and serviceable by the base operations control technicians or local service crews.

6. **Installation Requirements**

   a. All abandoned-in-place temperature controls shall be demolished as part of the construction, renovation, repair or other improvement project.

   b. Where DDC controls are installed, the controls shall be fully compatible with the existing control system and the base wide EMCS system. Comply with specific code provisions regarding network controls, such as UFC 3-410-01, Chapter 4, Section 309, para. 309.3.

   c. **ALL** wiring from sensors, controls, and hardware points shall be in conduit. Conduit shall meet requirements outlined in the ***Base Electrical Standard***. Wiring shall be terminated at a Data Termination Cabinet (DTC) located in mechanical rooms. The conduit shall enter the side and bottom of the panel only.

d. Install conduits entering panels from side and bottom of panel to prevent water from entering the panels and destroying the electronics.

e. Provide adequate clear space around EMCS Data Gathering Panel (DGP) location of future FID and MUX and accessibility of maintenance personnel.

H. Solar Heating System Requirements

1. Any facility undergoing major renovation must be evaluated per life cycle costing to determine if 30% or more of required domestic hot water can be supplied by a cost effective solar heating system.

– End of Section –

II. Fire Protection Engineering

A. Safety Deficiencies in Existing Facilities

1. Existing facilities requiring correction of any fire safety deficiency shall comply with Air Force Instruction 32-10141 – *PLANNING AND PROGRAMMING FIRE SAFETY DEFICIENCY CORRECTION PROJECTS.*

B. System Design for Existing and New Facilities

1. All fire protection system designs shall be accomplished by a qualified Fire Protection Engineer. All fire protection systems shall be designed in accordance with the following:
    - UFC 3-600-01 Design: Fire Protection Engineering for Facilities,
    - UFC 3-601-02 Operations and Maintenance: Inspection, Testing, and Maintenance of Fire Protection Systems,
    - UFC 4-010-06 Cybersecurity of Facility-Related Control Systems,
    - NFPA 13,
    - *Life Safety Fire Protection System Analysis* (project specific, to be provided by the Engineer of Record).
2. Fire Protection designs shall reference the new **Air Force Corporate Facilities Standards** at the following web hyperlink:

    http://www.wbdg.org/ffc/af-afcec/corporate-facilities-standards-afcfs

3. Fire Protection designs shall incorporate cybersecurity requirements. Consult the Base Information System Security Manager (ISSM) regarding “Authority to Operate” (ATO) requirements for fire protection control communications systems.

C. Design Submittal

1. The designer shall provide a preliminary fire sprinkler design, including hydraulic calculations IAW UFC 3-600-01 requirements.

D. Piping System Design and Installation

1. Piping material for dedicated fire suppression systems shall be ductile iron or steel only and meet or exceed the material standards and requirements listed in NFPA 24 as amended by UFC 3-600-01. Minimum wall thickness for all sprinkler piping shall be schedule 40 steel.
2. COLOR IDENTIFICATION. In the absence of project-specific contract specifications, all fire suppression/sprinkler piping constructed of ferrous metal (non-galvanized) shall be painted red. New coatings shall be compatible with existing coatings. This requirement applies to all piping, whether concealed or exposed. Use of the following or equivalent paint system is required:
    a. Sherwin Williams Pro-Cryl Universal Acrylic Primer (One Coat)
    b. Sherwin Williams ProMar 200 Zero VOC Interior Latex (Two Coats if exposed)
3. LABELING. Piping shall be labeled IAW UFC 3-600-01 requirements. Painted labels shall be applied after piping has been painted and fully cured.

E. Firewalls and Fire Area Limitations

1. All construction, including fire walls, fire area limitations, emergency lighting systems, means of egress, and exit stairways, shall meet the more stringent requirement of both the NFPA 101 and the International Building Code.
2. All wall penetrations through existing firewalls shall be fire caulked and sealed.
3. All duct penetrations through fire walls on both new and repair projects shall have operational and code compliant dampers and seals as required by current code.

4. Identification (by painting) of Fire Rated Walls, Fire Pumps, Hydrants, Automatic Sprinkler Systems, Fire Alarm conduit, junction boxes and covers shall be provided and performed for all projects IAW UFC 3-600-01, *Fire Protection Engineering for Facilities.*

– End of Section –

III. Mechanical Engineering: *Plumbing Systems*

A. Plumbing Systems – General

1. Plumbing systems at Tinker AFB generally include the following facility systems:
    - Domestic water supply piping, booster pumps and related systems
    - Waste water piping and related components
    - Natural Gas piping and related components
    - Compressed air piping and related components (i.e. air-compressors)
    - Lavatory, toilet and related plumbing fixtures
    - Water heaters and boilers for domestic water heating
    - Storm drainage systems within and to 5 feet outside buildings
    - Water for landscaping
    - Water softening and treatment (small) systems for buildings
    - Corrosion control (cathodic) protection systems
2. Design and construction of plumbing systems shall be in accordance with the International Plumbing Code and the following, as applicable:
    - UFC 3-420-01 Plumbing Systems
    - UFC 3-420-02FA Compressed Air
    - UFC 3-230-01 Water Storage, Distribution and Transmission
    - UFC 3-430-09 Exterior Mechanical Utility Distribution
    - Air Force Instruction AFI 32-1066 *Backflow Prevention Program*
    - NFPA

B. Facility Domestic Water Supply

1. Base domestic water supply systems shall be from potable water lines. All water used for process purposes (heating, air conditioning) shall be isolated from domestic supply systems, or 'drinking water', by means of reduced-pressure backflow prevention devices.
2. Tie-ins to existing water lines shall be analyzed to document as part of the project design analysis that existing demands shall not be adversely affected by new demands.
3. Incorporate handicapped accessible design for all toilet areas, shower areas, and drinking fountains.
4. Provide access to piping, valves, and instrumentation for maintenance personnel. Access to through-wall piping shall be provided by means of wall access panels or, where space is available, from a walk-in plumbing chase. Where carriers are utilized to support fixtures, a walk-in plumbing chase is preferred.
5. Domestic hot and cold potable water piping shall be of Type L seamless copper tubing with dielectric insulators at point of contact with dissimilar metallic piping. Provide insulation for all domestic and comfort cooling supply and return lines.
6. Specify Type K copper pipe for underground domestic hot water supply applications and Type L copper pipe for above ground hot water applications.
7. Do not use dissimilar metals in contact with each other on piping in a common electrolyte such as water or soil.
8. Provide stop-valves at all plumbing fixtures.
9. Provide water hammer arrestors as required by code and for any location where quick-acting valves are installed. Utilize devices that comply with relevant standards such as ASSE 1010.
10. Design piping with the following velocity limitations to minimize erosion:

Pipe Dimension		Maximum Velocity	
inches	*mm*	*m/s*	*ft/s*
1	25	1	3.5
2	50	1.1	3.6
3	75	1.15	3.8
4	100	1.25	4
6	150	1.5	4.7
8	200	1.75	5.5
10	250	2	6.5
12	300	2.65	8.5

11. No asbestos-containing materials of any kind shall be used in construction.
12. Water meters shall be installed on all facilities. See TAFB Facility Standard Section 6: Utilities for full metering requirements.
13. For engineering design and system sizing determinations, it shall be anticipated by project designers that the highest demand for water shall be during normal duty hours.

C. Cross-Connection and Backflow Prevention

1. Cross-connection and backflow prevention policies of AFI 32-1066 *Backflow Prevention Program* shall be followed to protect the potable water system and facility occupants.
2. The proper backflow prevention device shall be specified as required in AFI 32-1066 for the hazard involved.
3. Backflow prevention devices shall be located and installed to ensure they shall function, not freeze, and are readily accessible for testing, service and repair.

D. Wastewater Systems Design

1. Comply with Air Force Instruction AFI 32-1066 *Backflow Prevention Program*, latest edition.
2. Where specific project requirements are determined more stringent by 72 ABW/CE, use the manual of practice Gravity Sanitary Sewer Design and Construction**,** as jointly published by the *Water Environment Federation* and the *American Society of Civil Engineers* as the MOP FD-5**.**

3. All projects on TAFB which include earthwork shall comply with Engineering Technical Letter ETL 03-1: Storm Water Construction Standards.

4. **General Requirements**

   a) Provide sanitary drain systems from lavatories, toilet areas, break areas, and non-industrial waste floor drains to sanitary lines. Piping shall be installed to provide a slope of ¼ inch per foot for a pipe diameter of 2 inches and below and 1/8 inch per foot for piping 2-1/2 inches and larger.

   b) All Restrooms projects involving under-floor plumbing work shall locate new floor drains under the partitions in the new or final floor layout.

   c) All projects involving a janitor closet and under-floor piping shall place a floor drain in the center of the janitor room with grading to ensure removal of all water from floor.

   d) Trap primers are required on all floor drains. Trap primers are preferred to be installed in the wall with access panels and with hammer arresters.

   e) Wall cleanouts shall be incorporated at appropriate points within plumbing system designs to serve all water closets, urinals, and lavatories. Wall cleanouts shall be located 26" A.F.F. Floor cleanouts are not acceptable in restrooms.

   f) Where piping is to be installed in exterior walls, the designer must show that the exterior wall design will prevent water or waste piping from experiencing freezing conditions.

   g) Do not provide water or waste piping in attic spaces where there is danger of freezing.

   h) The installation of an electric waste disposer/food waste grinder is prohibited except as provided in UFC 3-420-01 *Plumbing Systems*.

5. **Additional Requirements**

   a) Pre-Construction & Post-Construction Scoping. Prior to beginning construction, a contractor performing a renovation, repair or replacement project that involves sanitary waste lines shall snake existing sanitary pipes 100 feet to identify and clear any blockages in existing lines. Upon construction completion, following all clean-up activities, the contractor shall scope both new and existing sanitary pipe to clear any obstructions. Snake pipes that are smaller than 6". Provide video footage for sanitary pipes 6" and larger in diameter. Video footage shall be obtained pre-construction and again post-construction. Submit video evidence prior to new pipe being installed. Following construction, submit post-construction video evidence of all new and existing pipes. The Contractor shall perform the above work in the presence of the Construction Inspector. The above is a minimum standard requirement. Project specific requirements may differ and/or increase the line length.

E. Corrosion Prevention and Control

AFI 32-1054 Corrosion Control https://www.wbdg.org/ffc/af-afcec/instructions-afi/afi-32-1054

Cathodic protection for buried metallic structures shall be designed IAW UFC 3-570-02A Cathodic Protection, UFC 3-570-02N Electrical Engineering Cathodic Protection, and UFC 3-570-06 O&M Cathodic Protection System.

1. Protective coatings: Coating specifications for above and below ground high value metallic structures shall be prepared IAW the guide specifications as shown in UFC 3-190-06 *Paints & Protective Coatings.*

2. Underground piping systems shall conform to either FS-L-C-530, Type II except tape and primer

conform to AWWAC203, for epoxy or for continuously extruded polyethylene, FS-L-C-530, Type I.

3. On all metallic structures where the surface is blasted to white or near white finish, no blasted surface shall be left unprimed beyond the normal workday.
4. Coatings specified for underground or submerged use shall be those specifically designed for those types of environmental conditions.
5. Under no circumstances shall thin plastic film tapes, such as electrical tape, be used to coat underground structures or wiring.
6. Reference NACE Standard RP-01-69 for coating information.

F. Cathodic Protection

1. General soil conditions at Tinker AFB are very conducive to corrosion of underground metal structures.
   a) The soil varies from sandy silt to sandy clay with areas of stratification of the various types.
   b) Soil resistivity varies from a high of 26,100 ohm-cm to a low of 529 ohm-cm. There is no soil resistivity data available at the base.
2. Designer shall take readings at the locations of structures and paths of utilities having cathodic protection.
3. Design analysis shall contain a map showing the sites of such readings, type of instrument used and a table containing location designation and soil resistivity.
4. Cathodic protection design shall be a complete design and not a performance specification.
5. The cathodic protection system to be installed shall be designed by an engineer who has been accredited as a "Corrosion Specialist" by the National Association of Corrosion Engineers, which verifies that engineer has had experience in cathodic protection design, installation and testing as per UFC 3-570-02A *Cathodic Protection* and UFC 3-570-06 *O&M Cathodic Protection Systems*.
6. Guidance for the installation and/or use of corrosion mitigation equipment and procedures is provided by UFC 3-570-02A *Cathodic Protection* and UFC 3-570-06 *O&M Cathodic Protection Systems.*
7. All metals installed underground or in contact with the ground at Tinker AFB shall have cathodic protection for control of corrosion.

G. Water Treatment

1. Water treatment shall be provided for all transfer media in all heat transfer equipment.
2. Heat transfer equipment shall be taken to include cooling towers, chilled/hot water systems, and boilers.
3. Treatment shall contain no chromates and no heavy metals.
4. Water treatment design analysis shall contain base water analysis and step-by-step procedures used to arrive at suggested treatment.
5. This analysis shall include which constitute of water is the limiting parameter.
6. All new equipment, water treatment systems and methods installed shall be in compliance with support the descriptions, recommendations, and guidelines of UFC 3-240-13FN *Industrial Water Treatment Operation and Maintenance.*
7. Air Force Non-Chemical/Nontraditional Water Treatment Devices Policy: Most non-chemical water treatment devices or equipment are not currently authorized for use on military installations, as stated in paragraph 1-1.5. The Air Force will allow their use only under an Energy Saving Performance Contract (ESPC) in which the contractor assumes all performance-based risk. The performance standards for system component protection must meet or exceed those that are

achievable with chemical treatment. (See UFC 3-240-13FN Chapter 8 for details).

H. Water Softeners/Water Treatment Equipment:

1. Water softeners are required on all open loop makeup systems including but not limited to steam boilers, humidifiers, and commercial domestic hot water systems (kitchens).
2. Softeners shall be properly sized to allow soft water to be introduced into systems at all times, including emergency shutdown.
3. Provide adequate water/conditioned water for all boiler systems.
4. Side stream pot feeders and annual chemical treatment shall be provided on all "closed loop" systems including but not limited to heating water loops, chilled water loops, and fluid cooler applications.

I. Existing Energy Source

1. Natural gas is available for facility heating if steam is not available.
2. Natural gas pressure varies from 30 to 40 psig, seasonally.
3. Gas is on an uninterruptible contract.
4. Steam is no longer supplied from centralized locations on Tinker AFB (i.e. boiler plants). Most facilities previously served by a central boiler plant have been converted to heating water. A facility having a stand-alone steam boiler (except process boilers), will need to be evaluated for conversion to other mediums. Designers/contractors shall consult with Base Civil Engineering in order to confirm requirements for specific heating equipment.

J. Natural Gas Systems

1. Exterior Distribution Piping (Mains): Refer to TAFB Facility Standard, part 6.9 **Natural Gas Delivery Systems.**
2. Building Service:
   a) Install sufficient isolation valves to repair units without shutting off entire system
   b) Replace natural gas regulators over 15 years old.
   c) Distribution regulators: All distribution regulator sets shall be installed with:
      - Regulators that do not fail in the valve "open" position (e.g., do not use pilot loaded regulators since they fail to "open").
      - Valved, regulated bypasses to permit equipment repair or replacement.
      - Regulators that have valve stem indicators.
      - Sets that use one regulator for control of flow and a second regulator to monitor the flow.

K. Welding

1. All welding shall be performed by a welder certified IAW ANSI B31.1 or API 1104 codes. Welds shall be made and inspected IAW ANSI B31.8 requirements.

L. Plumbing Piping

1. Piping installed on new systems shall be corrosion resistant. Otherwise a cathodic protection system shall be provided. Provide necessary shutoff valves and identification.
2. Pipe Painting**:** All exposed plumbing piping shall be primed with paint suitable for metal surfaces and finish painted with color to match background. This requirement applies to repair and renovation projects as well as new construction or additions to existing building plumbing systems.

3. Pipe Labeling: All supply and return lines shall as a minimum be identified with markings denoting both flow direction and fluid transported.

M. Piping Thermal Insulation

1. Insulation of plumbing piping located outdoors. Where piping that serves domestic hot water, domestic cold water or similar fluid is installed outdoors or otherwise exposed to the elements, insulation shall exceed by 30% the requirements of ASHRAE 90.1, the International Mechanical Code, or the standard UFGS specification whichever is greater. This shall apply to all new construction, renovation, repair or replacement projects.
2. Insulation of plumbing piping located within a conditioned environment. Where piping is installed indoors or otherwise within a conditioned environment, thermal insulation shall meet requirements of ASHRAE 90.1, International Mechanical Code, or the standard UFGS specification, whichever is more stringent. This shall apply to all new construction, renovation, repair or replacement projects.

N. Compressed Air Systems

1. Compressed air, if required, shall be provided by base compressed air distribution system where available.
2. Where Base system is unavailable to the project site, provide stand-alone compressors and locate in facility mechanical room.
3. Provide necessary maintenance access for controls, refrigerated air dryers, and condensate handling equipment.
4. Ventilate mechanical rooms to prevent overheating of components and to maintain acceptable indoor air quality. Ventilation system designs shall comply with **ASHRAE Standard 62.1 – *Ventilation for Acceptable Indoor Air Quality,*** latest edition.
5. Install inlet air filtration with instrumentation.
6. Install vibration isolation pads (neoprene component material is preferred), including flexible connections between the compressor and its associated piping, to prevent vibration damage to compressors.
7. Noise suppression shall be provided to keep compressor noise within Occupational Safety and Health (OSHA) limitations.
8. Oil free compressors shall be required for breathing air applications.

O. Equipment & Fixtures

1. Electric Water Coolers/Drinking Fountains. Design electric water coolers (drinking fountains) to be dual use water coolers and bottle filling stations. Units shall be filter-less type. Provide accessible models where required.
2. Standard Restroom Fixture - Basis of Design.
   a) Faucet, hand washing. Sloan EAF-275 sensor activated, or equal.
   b) Service Faucet. T&S Brass & Bronze Works, Inc. model B-0665-BSTP wall mounted, or equal.
   c) Flush Valve (new/replacement). Sloan or equal, AC powered sensor-activated, single-flush or manual flush valve.
   d) Flush Valve (retrofit conversion). Sloan or equal AC-powered sensor activated, single-flush retrofit conversion kit for exposed closet or urinal applications.

– End of Section –

IV. Mechanical Engineering: *HVAC/R Systems*

A. General

1. Proper design of mechanical systems is required for the health and life safety of building occupants, operations and maintenance personnel and the general public.
2. Mechanical systems shall be designed, constructed, operated and maintained according to UFC requirements, Air Force Instructions, TAFB Instructions and other requirements. In the absence of specific criteria, follow recommendations from ASHRAE and/or the equipment manufacturer.
3. Mechanical systems, including all heating, ventilating, air-conditioning and refrigeration systems shall be designed and constructed, operated and maintained to meet applicable code requirements and Tinker AFB Standards.
4. All HVAC systems shall be tested and balanced following installation or replacement. Testing and balancing shall be performed in accordance with UFC requirements.
5. All mechanical equipment schedules shall incorporate the use of existing unit identification numbering (UID) for all real property equipment.

B. Submittal Requirements for All Mechanical Projects

The information herein applies to all construction and/or repair projects regardless of delivery method. Refer to contract documents for additional information on submittal requirements. In the absence of specific contract requirements, the following minimum requirements shall apply:

1. Design submittals shall be provided at one or more levels; schematic, preliminary, design development and final design phases (i.e. 15%, 35%, 65%, etc.) as per contract documents.
    a) Schematic phase: Preliminary design analysis to include manufacturer cut-sheets, sketches, preliminary load calculations.
    b) Design development phase: Preliminary design analysis, preliminary load calculations, mechanical equipment plan layout and air distribution design, preliminary hydraulic calculations, plumbing design, equipment selections, outline specifications, etc.
    c) Construction document phase: Final design analysis, final mechanical equipment plans, final air distribution design, final plumbing design, equipment selections, schedules, specifications, etc.
2. Shop drawing submittals shall consist of the following:
    a) Installing contractor or sub-contractor provided drawings to illustrate the dimensional requirements (including spatial constraints, maintenance requirements, etc.) for all systems, materials and equipment to be assembled or constructed in-place. Examples include isometric drawings for all plumbing and instrumentation (P&I), air distribution systems, buried piping, utility vaults, etc.
    b) Manufacturer's published data for all pre-manufactured items to be installed and/or otherwise provided on Tinker AFB. Data shall include, but not be limited to all of the following as applicable: certified performance data, capacities, dimensions, ratings, code approvals, the approval seal and/or published rating information for all listing agency standards, manufacturer's special requirements, general installation requirements, access requirements, electrical characteristics (voltage, frequency, phase, amperage, capacitance, resistance, inductance ratings, etc.).
3. Combine all related materials into one submittal, i.e. all plumbing fixtures, all air distribution devices, all related mechanical assemblies, etc. to be submitted using one form AF3000, with each item listed separately.
4. The following required deliverables shall be provided in electronic (PDF) format and hard copy:

a) Installation manuals

b) Operation & maintenance (O&M) manuals, including spare parts list

c) Wiring diagrams, including project specific wiring diagrams, control diagrams, etc.

d) Start-up test and check reports, Test and balance (TAB) reports, etc.

e) Commissioning plans, reports and manuals

5. As-built drawings shall be provided in both hard copy and electronic form. Electronic documents shall be in both AutoCAD and PDF formats.
6. Additional requirements are published in Tinker AFB Standard Specification Section 01 33 00 SUBMITTAL PROCEDURES. Specific drawing documentation details may be found in various code documents such as UFC-3-401-01 Mechanical Engineering, UFC 3-410-01 Heating, Ventilating, And Air Conditioning Systems, etc.

C. Mechanical Equipment

1. All abandoned-in-place mechanical equipment shall be demolished as part of the construction, renovation, repair or other improvement project.
2. All outdoor mechanical equipment shall be rated and installed for all weather conditions. These provisions shall include but not be limited to the following:
   a) Low voltage electrical connections to outdoor mechanical equipment.
   b) Heat tracing and insulation to prevent freezing.
   c) Aluminum protective covering for outdoor insulation.
   d) Protection for pipe insulation in high traffic areas.
   e) Rain tight NEMA rated enclosures and watertight EMT as applicable.
   f) Hail damage guards and high wind protection for refrigerant condenser coils.
   g) Low ambient capability (to at least 0 degrees F) for air-cooled refrigeration condensers, compressor-bearing condensing units and packaged outdoor HVAC units when required to operate in low ambient conditions.
   h) Hot gas reheat for packaged outdoor HVAC units for dehumidification.
3. All installed equipment utilizing refrigerants shall use a refrigerant which is approved for use on Tinker AFB as listed in the Base Refrigerant Management section of this Standard.
4. All HVAC installation, repair or replacement work shall be performed in accordance with ASHRAE and other industry-accepted standards.
5. The minimum thickness for pleated media shall be 4”.
6. Whenever possible, install bypasses or some other means to ensure regular maintenance items such as strainers may be cleaned without plant shutdown.
7. Provide disconnect switches for remote controlled equipment like air handlers and exhaust fans.
8. All equipment which could be damaged by inclement weather or accidental damage shall be installed with protective equipment options or provisions including, but not limited to, hail guards for all air-cooled condensers.
9. Floor mounted equipment shall be mounted on suitable concrete housekeeping pads extending 6 inches beyond the unit footprint.
10. Mechanical equipment having rotating or reciprocating components, such as compressors, fans, motors, etc. shall be mounted on spring isolators.
11. All equipment shall be located with sufficient clearance for maintenance and be provided with access by means of identified panels, catwalks, platforms, stairs or ladders as required.

12. Requirements for Boilers: Prior to construction, contractors shall contact Tinker AFB 72 ABW Civil Engineering Squadron, Environmental Management, Air Quality Division, regarding current environmental requirements for new boiler equipment. Additional requirements may be found in Tinker AFB General Specification Section 00 72 00 - *ENVIRONMENTAL REQUIREMENTS FOR CONSTRUCTION ON TINKER AIR FORCE BASE*. Tinker AFB Environmental shall also be contacted for current environmental metering, recording, and report requirements for new boilers.
13. Infrared Heating Systems, infrared heaters and system components installed on base, specifically in buildings located near the flight line such as aircraft hangers, shall be designed to prevent movement caused by vibration during aircraft take-off operations. Consider designing with seismic protection to accomplish this measure.

D. Mechanical Piping - General

1. All abandoned in place mechanical piping shall be demolished as part of the construction, renovation, repair or other improvement project.
2. Isolation valves shall be provided at each piece of connected equipment.
3. Isolation valves shall be provided at each branch line extending from a main line (tee fitting).
4. Thermometers, pressure gauges and PT plugs shall be provided at all coils.
5. All supply and return lines shall be identified with markings denoting flow direction and fluid transport.
6. Pipe Painting: All exposed mechanical piping shall be primed with paint suitable for metal surfaces then finished with a paint color to match the background. This requirement applies to repair and renovation projects as well as new construction or additions to existing building systems regardless of method of project delivery.
7. Pipes containing water or other fluids subject to freezing, when routed inside of an exterior wall cavity, ceiling cavity or other location exposed to an unconditioned space or to the outdoors, shall be protected from freezing.
8. All condensation shall be drained into sanitary sewer on all projects.
9. Piping installed on new systems shall either be manufactured as corrosion resistant, have protective coatings applied in the field or have a cathodic protection system.

E. Underground Piping

1. Steam utility piping systems shall be designed in accordance with UFC 3-430-01FA *Heating & Cooling Distribution Systems.*
2. All steam and hot water distribution systems shall have a cost analysis performed comparing aboveground, surface utility, and underground conduit systems to determine the most economical system. Comparison should include cost, maintainability, and system performance.
3. Install cathodic protection systems to protect all piping and appurtenances located underground.

F. Piping Thermal Insulation

1. Insulation of mechanical piping located outdoors. Where mechanical piping that serves steam, chilled water, hot water, domestic water or similar fluid is installed outdoors or otherwise exposed to the elements, insulation shall exceed by 30% the requirements of ASHRAE 90.1, the International Mechanical Code, or the standard UFGS specification, whichever is more stringent. This shall apply to all new construction, renovation, repair or replacement projects.
2. Insulation of mechanical piping located within a conditioned environment. Where mechanical piping is installed indoors or otherwise within a conditioned environment, thermal insulation shall

meet requirements of ASHRAE 90.1, International Mechanical Code, or the standard UFGS specification, whichever is greater. This shall apply to all new construction, renovation, repair or replacement projects.

G. Ductwork

1. All abandoned-in-place ductwork systems shall be demolished as part of the construction, renovation, repair or other improvement project.
2. All ductwork shall have a class A seal.
3. All HVAC ductwork shall be constructed and installed in accordance with industry-accepted standards including but not limited to ASHRAE and SMACNA standards.
4. Install sufficient insulation and vapor barrier on air conditioning ductwork and chilled water piping to prevent condensation. Duct liner shall be kept to a minimum for sound control only. The preferred thermal insulation shall be external wrap.
5. Balancing dampers in ductwork shall be installed so as to be inaccessible to the occupants of the space being served, i.e. in the take offs from the duct branches rather than in the diffusers.
6. Exposed Ductwork Painting: All exposed mechanical ducts shall be primed with paint suitable for metal surfaces and finish painted with color to match background. This requirement applies to repair and renovation projects as well as new construction or additions to existing building systems regardless of method of project delivery.

H. Natural Gas Systems

1. Refer to Plumbing Section for requirements.

I. Welding

1. All welding shall be performed by a welder certified IAW ANSI B31.1 or API 1104 codes. Welds shall be made and inspected IAW ANSI B31.8 requirements.

J. Temperature Controls / Energy Management / EMCS Systems

1. All abandoned-in-place temperature controls shall be demolished as part of the construction, renovation, repair or other improvement project.
2. Temperature controls for all renovation and new construction projects shall utilize direct digital control (DDC) systems as required by UFC 3-410-01.
3. Provide vibration sensors for all mechanical equipment having electric motor(s) equal to or exceeding 50 HP. Vibration sensing equipment shall include permanent mount sensors/transducers, collection boxes and cabling sourced via the same manufacturer – all devices shall be compatible. Preferred products are as manufactured by Connection Technology Center, Inc. Victor, NY.
4. Provide baseline measurements for all equipment in commissioning reports. Record results on the EMCS monitoring system.
5. For additional requirements, refer to **Section I – Energy Conservation Requirements** in this document.

K. Water Treatment

1. In order to protect boilers, cooling towers, chillers and other capital-intensive mechanical equipment, water treatment shall be provided as recommended by the specific equipment manufacturer. Site specific water quality testing shall be performed and written lab test results shall be provided by an independent third party test agency. Based on the lab test results, a formal water treatment plan shall be developed and a water treatment program implemented.

2. Annual chemical treatment shall be provided on all "closed loop" systems including but not limited to heating water loops, chilled water loops, and fluid cooler applications. Side stream pot feeders shall be provided for all mechanical systems requiring chemical treatment whether or not specified on plans, drawings or otherwise.
3. Water treatment shall be provided using traditional chemical-based methods. Non-chemical treatment methods are prohibited by USAF policy.
4. Ensure the output capacity (volume and pressure) from the water treatment equipment is adequate for the volume of makeup water required, according to the boiler manufacturer.
5. Water softeners are required on all open loop makeup systems including but not limited to steam boilers, humidifiers, cooling towers and commercial domestic hot water systems (kitchens).
    a) Softeners shall be properly sized to allow soft water to be introduced into systems at all times, including emergency shutdown.
    b) Provide soft water/conditioned water for all boiler systems.

L. Mechanical Room Design

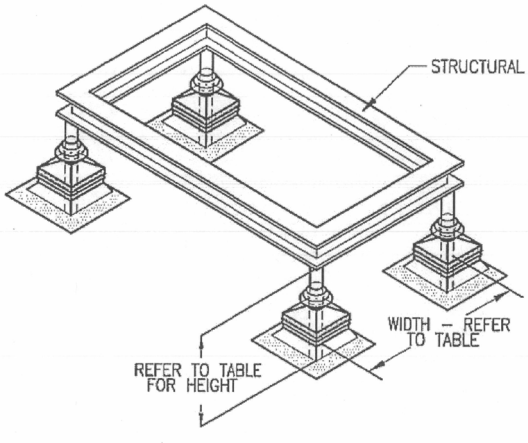
1. In order to protect boilers, cooling towers, chillers and other capital-intensive mechanical systems, dedicated mechanical room(s) shall be provided for all mechanical equipment and systems in accordance with the International Mechanical Code.
2. Mechanical rooms shall be provided with doorways suitable for passage of the mechanical equipment to be installed inside the space.
3. Mechanical rooms containing refrigeration equipment such as water chillers, refrigerant cooled equipment, coils, etc. shall comply with **ASHRAE Standard 15** ***Safety Standard for Refrigeration Systems***, latest edition. *This is a mandatory, Life Safety, Health and Welfare requirement.*
4. Ventilate mechanical rooms to prevent overheating of components and to maintain acceptable indoor air quality. Ventilation system designs shall comply with **ASHRAE Standard 62.1** ***Ventilation for Acceptable Indoor Air Quality****,* latest edition.
5. Concrete housekeeping pads shall be provided for all floor mounted mechanical equipment. Housekeeping pads shall be constructed of approved materials and shall be secured to the building foundation by means of mechanical, structural and/or chemical-bonding material. Construct pads to extend beyond supported mechanical equipment by six inches (6”) on each side. Pads shall be placed level, to a height of four inches (4”) above the floor, and all exposed edges shall have a one inch (1”) chamfer. Pads shall not be placed adjacent to a wall, column, or other building element unless suitable maintenance access is provided to the equipment to be mounted onto the pad.
6. For mechanical rooms housing chillers, boilers or heat exchangers, allow sufficient clearance to access the tube bundles for tube cleaning, eddy current testing or tube replacement. Typically, to meet the “sufficient space” requirement, allow clearances equal to the overall equipment length plus 20%, measured from the accessible end(s) of the equipment (i.e. end bell covers). Where possible, this type of equipment should be located at ground floor level and near an exterior, overhead door. In cases where space is at minimum, equipment could be positioned to allow for servicing through the open doorway.
7. Chillers, boilers, heat exchangers, fans, pumps motors or other large equipment exceeding 100 HP, 100 tons in refrigerating capacity, or having serviceable components exceeding 150 lbs. should be provided with permanently installed, overhead hoist or crane rails secured to and integrated with the building structure.

M. Mechanical Equipment Location

1. Locate equipment to allow access for maintenance IAW the International Building Code (IBC) and International Mechanical Code (IMC). Avoid locating equipment on roofs due to maintenance

problems. Provisions shall be made for removal of equipment for maintenance. Assure that proper distance between system components and walls is maintained to ensure ability to clean, repair, or replace system components.

2. Equipment such as Air Handling Units, large supply, return or exhaust fans, fan coil units and similar equipment shall not be located above spaces having ceilings constructed with acoustical tile (drop ceiling systems), gypsum board, or other material unless provided with dedicated code-compliant access stairways, ladders, maintenance walkways and other means of mechanical access IAW the International Building Code (IBC). This includes variable air volume (VAV) or other air terminals where the bottom of such units would be located more than 12'-0" above the finished floor space.
3. Curbed Applications. Where HVAC systems are to be installed on a roof using a roof curb assembly, the requirements of the roof assembly, including roof insulation material thickness, will need to be considered when selecting the height of the roof curb.
4. Non-Curbed Applications. Where HVAC systems must be installed above a roof in a non-curb application (no roof curb), provide an Elevated Mechanical Platform which will allow sufficient access for roof maintenance and repair without removal of the HVAC equipment. Elevated Mechanical Platform shall comply with the following requirements:
    a) Elevated Mechanical Platform shall be designed to support the HVAC equipment weight as well as the required maintenance walkway around the equipment including any stairs or ladders required for access, in addition to ductwork, piping and appurtenances.
    b) Minimum clear height from the roof surface to the elevated structure shall be as shown in Figure 1, below.
    c) Roof supports shall be secured to structure. Refer to Figure 2 (below) for typical requirements.
    d) Access to the roof below the Elevated Mechanical Platform supporting the HVAC system shall be provided on at least three sides, and the open sides shall not be obstructed with flashing, fencing, covering or other material.
    e) All penetrations, duct routing, conduit routing and equipment placement not on curbs shall be in general conformance to the representative set of details found in the Appendix section, ***Attachment of Rooftop Equipment in High-Wind Regions,*** **FEMA.**
    f) All pipe supports shall be structurally anchored to the deck.



WIDTH OF EQUIPMENT	HEIGHT OF LEGS
UP TO 24"	20"
25" – 36"	24"
37" – 48"	30"
49" – 60"	36"
61" AND WIDER	54"

FIGURE 1 – ELEVATED MECHANICAL PLATFORM SUPPORT STRUCTURE FOR INSTALLATIONS ABOVE ROOF

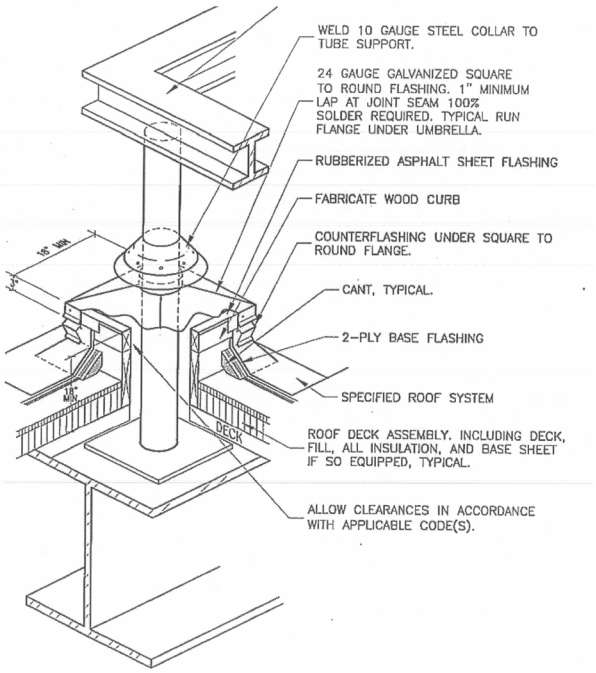


FIGURE 2 – TYPICAL ROOF SUPPORT DETAIL FOR ELEVATED PLATFORM

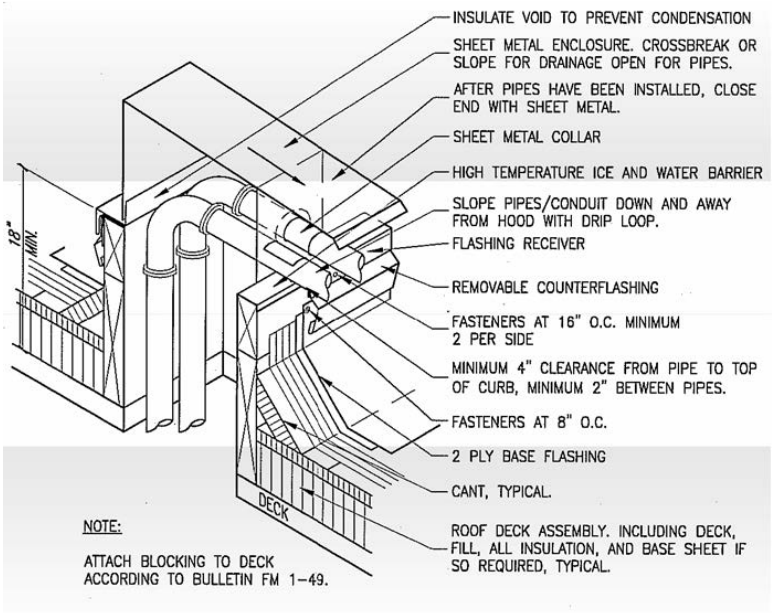


FIGURE 3 – TYPICAL PIPE AND CONDUIT ROUTING DETAIL FOR ROOF INSTALLATIONS

N. Base Refrigerant Management

1. The 72 ABW/CE is tasked to maintain a Refrigerant Management Program in accordance with the **Air Force Manual 32-7089 Refrigerant Management Program issued 4-Nov-2016.**
2. **ANSI/ASHRAE Standard 34, *Designation and Safety Classification of Refrigerants***, establishes a simple means of referring to common refrigerants and assigns safety classifications and refrigerant concentration limits based on toxicity and flammability data.
3. HQ AFMC Guidance (10 Jul 95 letter from HQ AFMC/CECS) strictly prohibits contractors from purchasing, providing or removing any refrigerants that contain either *chlorofluoromethane, chlorodifluoromethane or other "CFC" gases* (such as R-11, R-12, R-500, R-502 or R-503), to or from the government's inventory to perform contracts.
4. Contractors are prohibited from purchasing, providing, or removing any prohibited refrigerants to or from the government inventory. Refer to list of Prohibited Refrigerants below.
5. It is the obligation of 72 ABW/CE to account for use of all contractor-provided refrigerants on Tinker AFB which is to be installed to contracted equipment, and this obligation consists of the following:
   a) Track Environmental Protection Agency (EPA) certifications for refrigerant technicians and refrigerant recovery equipment.
   b) Track refrigerant inventory levels for each type of refrigerant.
   c) Report on refrigerant emissions.
6. REMOVAL OF REFRIGERANT (*Refrigerant Recovery*). Recovery of refrigerant (*as defined by 40 CFR 82*), from existing, government-owned "appliances" (*as defined by 40 CFR 82.152, i.e. HVAC, commercial refrigeration, industrial refrigeration or other refrigerant systems, except for small appliances*), will be performed by the Government upon written notice from the contractor. However, contractors may remove government refrigerants from contracted equipment into government-furnished containers, only when so directed in writing by the Contracting Officer.
7. NEW REFRIGERANT. All refrigerant provided or furnished for use on Tinker AFB shall be produced and sold as new, virgin refrigerant. Use of recovered, recycled, reclaimed or other category of refrigerants (i.e. used refrigerant) is strictly prohibited. Contractors shall only use refrigerant that is approved for use at Tinker AFB unless otherwise approved in writing by 72 ABW/CE.
8. REFRIGERANTS APPROVED FOR USE AT TINKER A.F.B.*
   Refrigerant 134a
   Refrigerant 410A
   * There are multiple refrigerants which are acceptable per current EPA regulations but current TAFB Refrigerant management policy is to simplify and standardize our refrigerant inventory to R134a and R410a refrigerant inventories for new equipment wherever possible. Therefore the refrigerants automatically approved for new equipment are only R134a and R410a unless approved in writing by TAFB Base Civil Engineering.
9. REFRIGERANTS PROHIBITED FROM USE AT TINKER A.F.B. Prohibited refrigerants include all refrigerants other than approved refrigerants.
10. EXCEPTIONS.

    Excluded from the list of prohibited refrigerants are "process" systems utilized in production and/or manufacturing, unless otherwise prohibited by USAF or TAFB policy.

    Any other exceptions to the Base Refrigerant Management policy requirements must be approved in writing by the Base Civil Engineer for the specific equipment, system or project for which the refrigerant is required. Exceptions will be made as needed on a case by case basis only.

O. Contractor Certifications and Recordkeeping for Refrigerant Management

1. When required to install, remove or recover refrigerants pursuant to provisions of part N above, Contractors shall furnish the following in conjunction with the performance of contracted work at TAFB:
   a) Prior to bringing technicians on base for installation or recovery of refrigerants to or from contracted equipment, the Contractor should submit to the Contracting Officer's Technical Representative (COTR): (1) A copy of the refrigerant technician's certification as required by 40 CFR (Code of Federal Regulations) part 82, subpart F; and (2) A copy of the certification to the EPA that the Contractor acquired refrigerant recovery equipment per 40 CFR 82.162.
   b) Prior to final acceptance of contract work, the Contractor should provide a record of the amount of refrigerant installed with the contracted equipment or recovered from equipment contracted for demolition into government furnished containers. In the case of commissioning new or retrofitted equipment, the Contractor shall provide the refrigerant amount determined to be the "Full Charge" as defined in 40 CFR 82.152.
   c) The Contractor shall provide information concerning refrigerant emissions.
   d) Prior to final acceptance of contract work, the Contractor shall provide to the COTR a record of any refrigerant losses to the atmosphere.
   e) Included with all warranty work, the Contractor shall provide to the Contracting Officer a record of all refrigerant losses to the atmosphere. The Contractor shall assume that the amount of refrigerant added to the equipment to bring it back to "Full Charge" is the amount of refrigerant that was emitted to the atmosphere.

P. Electrical and VFD Requirements:

1. Comply with the Tinker AFB Base Electrical Standards (Appendix B) for the following:
   a) All Variable Frequency Driven (VFD) electric drives and motors.
   b) All low-voltage control wiring.
   c) All wiring and conduit for mechanical systems.
2. Variable Frequency Driven (VFD) motor applications shall comply with all NEC rules for motor disconnect. In addition:
   a) VFD selection should include provisions for radio frequency (RF) shielding on incoming feeder side by either internal protection or cables.
   b) VFD selection should include provisions for radio frequency (RF) shielding on outgoing motor side by either internal protection or cables.
   c) VFD selection shall include an integral means of disconnect by manufacturer design.
   d) When necessary to utilize a brake function, it shall be provided with a separate power supply.
   e) VFD's shall be set to limit motor speed from exceeding 60 Hz.
3. Exhaust fan applications shall comply with all NEC rules for motor disconnect.
4. Exhaust fan applications serving restrooms.
   a) Ventilation exhaust fans for restroom shall not control fans by the light switch. Restroom exhaust fan(s) shall either operate continuously or interlocked with the HVAC system to operate when the HVAC supply fan operates.

Q. Anti-Terrorism Force Protection (ATFP) Requirements

1. UFC 4-010-01 *DoD Minimum Antiterrorism Standards for Buildings* applies to all facilities on Tinker AFB (*latest edition*).

2. ATFP provisions regarding Standard 18 – Emergency Air Distribution Shutoff: This provision is not applicable to small exhaust fans such as toilet exhaust fans, smoke purge (negative pressure) fans, or other fans where "*interior pressure and airflow control would more efficiently prevent the spread of airborne contaminants and/or ensure the safety of egress pathways.*"

– End of Section –

V. Appendix

This section includes the following: No. of Pages

- References 2
- Abbreviations and Acronyms 1
- Attachments
  - Table 1. Attachment of Rooftop Equipment in High-Wind Regions (FEMA) 4
  - FACILITY-RELATED CONTROL SYSTEMS CYBERSECURITY GUIDELINE 28

References

(Partial list - Not all inclusive)

UNITED FACILITIES CRITERIA

GENERAL

UFC 1-200-01 DoD Building Code (General Building Requirements)
UFC 1-200-02 High Performance and Sustainable Building Requirements

MECHANICAL

UFC 3-400-02 Design: Engineering Weather Data
UFC 3-401-01 Mechanical Engineering
UFC 3-410-01 Heating, Ventilating, and Air Conditioning Systems
UFC 3-410-02 Lonworks® Direct Digital Control for HVAC and Other Local Building Systems
UFC 3-410-04N Industrial Ventilation
UFC 3-420-01 Plumbing Systems
UFC 3-420-02FA Compressed Air
UFC 3-430-01FA Heating and Cooling Distribution Systems
UFC 3-430-02FA Central Steam Boiler Plants
UFC 3-430-07 Inspection and Certification of Boilers and Unfired Pressure Vessels
UFC 3-430-08N Central Heating Plants
UFC 3-430-09 Exterior Mechanical Utility Distribution
UFC 3-430-11 Boiler Control Systems
UFC 3-440-01 Facility-Scale Renewable Energy Systems
UFC 3-450-01 Noise and Vibration Control
UFC 3-460-01 Design: Petroleum Fuel Facilities
UFC 3-460-03 O&M: Maintenance of Petroleum Systems
UFC 3-470-01 Lonworks® Utility Monitoring and Control System (UMCS)

MULTI-DISCIPLINARY AND FACILITY SPECIFIC

UFC 3-190-06 Protective Coatings and Paints
UFC 3-230-01 Water Storage, Distribution and Transmission
UFC 3-240-13FN Industrial Water Treatment Operation and Maintenance
UFC 3-310-04 Seismic Design for Buildings
UFC 3-430-09 Exterior Mechanical Utility Distribution
UFC 3-520-05 Stationary Battery Areas
UFC 3-570-02A Cathodic Protection
UFC 3-570-06 O&M Cathodic Protection Systems
UFC 4-010-01 DoD Minimum Antiterrorism Standards for Buildings
UFC 4-010-05 Sensitive Compartmentalized Information Facilities Planning, Design, and Construction
UFC 4-010-06 Cybersecurity of Facility-Related Control Systems
UFC 4-024-01 Security Engineering: Procedures for Designing Airborne Chemical, Biological, and Radiological Protection for Buildings
UFC 4-211-01N Aircraft Maintenance Hangars: Type I, Type II and Type III, with Change 3; also see the Supplement ITG FY10-01
UFC 4-211-02 Aircraft Corrosion Control and Paint Facilities
UFC 4-390-01 O&M: Unmanned Pressure Test Facilities Safety Certification Manual
UFC 4-440-01 WAREHOUSE AND STORAGE FACILITIES
UFC 4-510-01 Design: Medical Military Facilities
UFC 4-610-01 Administrative Facilities
UFC 4-826-10 Design: Refrigeration Systems for Cold Storage
UFC 4-832-01N Design: Industrial and Oily Wastewater Control

FIRE PROTECTION

UFC 3-600-01 Fire Protection Engineering for Facilities

UFC 3-601-02 Operations and Maintenance: Inspection, Testing, and Maintenance of Fire Protection Systems

AIR FORCE PUBLICATIONS

AFI 32-1054, *Corrosion Control*

AFI 32-1066, *Backflow Prevention Program*

AFI 32-1068, *HEATING SYSTEMS AND UNFIRED PRESSURE VESSELS (14 MAY 2013)*

AFI 32-10141, (3 March 2011) – *PLANNING AND PROGRAMMING FIRE SAFETY DEFICIENCY CORRECTION PROJECTS*

AFI 23-204, *Organizational Fuel Tanks*

AFI 32-7044, *Storage Tank Environmental Compliance*

AFPD 90-17, Energy Management, and AFI 90-1701, Energy Management

AIR FORCE MANUAL 32-1084, Facility Requirements

ETL 03-1: *Storm Water Construction Standards*

ETL 11-25, *Implementation of Major and Area Source Rules as Applied to Boiler Tune-ups and Energy Assessments for the Boiler MACT Rule*

INDUSTRY STANDARDS AND CODES

ANSI/ASHRAE Standard 15 *Safety Standard for Refrigeration Systems*, latest edition

ANSI/ASHRAE Standard 34 *Designation and Safety Classification of Refrigerants*

ANSI/ASHRAE Standard 62.1 *Ventilation for Acceptable Indoor Air Quality,* latest edition

ANSI/ASHRAE/IES Standard 90.1 *Energy Standard for Buildings Except Low-Rise Residential Buildings* (latest edition)

ANSI/ASHRAE Standard 90.2 *Energy Efficient Design of Low-Rise Residential Buildings* (latest edition)

ASME *Boiler and Pressure Vessel Code*

ASME *Boiler and Pressure Vessel Code*, Section IX, “Welding and Brazing Qualifications,”

Gravity Sanitary Sewer Design and Construction**,** as jointly published by the *Water Environment Federation* and the *American Society of Civil Engineers* as the MOP FD-5

National Fire Protection Association

FEDERAL

40 CFR (Code of Federal Regulations) part 82

Executive Order 13423 - Strengthening Federal Environmental, Energy, and Transportation Management

Executive Order 13693 - Planning for Federal Sustainability in the Next Decade

Executive Order - FEDERAL LEADERSHIP IN ENVIRONMENTAL, ENERGY, AND ECONOMIC PERFORMANCE

Energy Policy Act of 2005 (EPAct 2005)

EPA 40 CFR Part 63, Subpart JJJJJJ, *National Emission Standards for Hazardous Air Pollutants for Industrial, Commercial, and Institutional Boilers Area Sources*

Building Life-Cycle Cost Program (BLCC) available at the Federal Energy Management Program website: http://www1.eere.energy.gov/femp/information/download_blcc.html**.**

Attachment of Rooftop Equipment in High-Wind Regions, FEMA, July 2006

Abbreviations and Acronyms

72 ABW – 72d Air Base Wing, Tinker Air Force Base, Oklahoma

AFCEE – Air Force Center for Engineering and the Environment
AFCESA – Air Force Civil Engineer Support Agency
AF – Air Force
AFB – Air Force Base
AFI – Air Force Instruction
AFGM – Air Force Guidance Memorandum
AFMAN – Air Force Manual
AFMC – Air Force Materiel Command
ANG – Air National Guard
AFPD – Air Force Policy Directive
AFRC – Air Force Reserve Command
ANSI – *American National Standards Institute*
ASHRAE – Official name of the international professional technical society formerly known as the *American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc.*
ATO – Authority to Operate

BCE – Base Civil Engineer
BCP – Base Comprehensive Plan

CATCODE – Category Code
CE – Base Civil Engineering
CECE – Base Civil Engineering Design & Construction
CECO – Base Civil Engineering Operations and Maintenance
CFR – Code of Federal Regulations
CS – Control Systems

DoD – Department of Defense

E.T.L. – Engineering Technical Letter

FOMA – Facilities Operation and Maintenance

IAW – in accordance with

MAJCOM – Major Command
MILCON – Military Construction
NFPA – National Fire Protection Association

NTE – Not to Exceed

O&M – Operation & Maintenance
OH&P – Overhead and Profit
OSD – Office of the Secretary of Defense

RPIE – Real Property Installed Equipment

SIOH – Supervision, Inspection and Overhead
SRM – Sustainment, Restoration and Modernization

TAFB – Tinker Air Force Base

ATTACHMENTS FOLLOW

DOCUMENT CONTROL RECORD

ISSUE	REV	DATE	BY
ORIGINAL DRAFT FOR QC REVIEW	-0-	10-FEB-2017	KDW
ISSUED FOR BASE WIDE REVIEW	1.1	14-FEB-2017	KDW
ISSUED FOR APPROVAL	-0-	01-MAR-2017	KDW
ISSUED FOR APPROVAL	2.0	20-MAR-2018	KDW
DRAFT ISSUED FOR REVIEW	2.1	20-FEB-2019	KDW
ISSUED FOR APPROVAL	2.2	15-MAR-2019	KDW
ISSUED FOR DISTRIBUTION / USE	2.2	15-MAR-2019	KDW
DRAFT ISSUED FOR REVIEW	2.3	31-JAN-2020	KDW
ISSUED FOR QC REVIEW	2.4	18-JUN-2020	KDW
ISSUED FOR APPROVAL	2.5	05-AUG-2020	KDW

Attachment of Rooftop Equipment in High-Wind Regions

FEMA

HURRICANE KATRINA RECOVERY ADVISORY

Purpose: To recommend practices for designing and installing rooftop equipment that will enhance wind resistance in high-wind regions.

> **Note:** For attachment of lightning protection systems, see Hurricane Katrina Recovery Advisory on Rooftop Attachment of Lightning Protection Systems in High-Wind Regions.

Key Issues

Rooftop equipment frequently becomes detached from rooftops during hurricanes. Water can enter the building at displaced equipment (see Figure 1); displaced equipment can puncture and tear roof coverings (thus allowing water to leak into the building). Equipment blown from a roof can damage buildings and injure people. Damaged equipment may no longer provide service to the building.

Figure 1. This gooseneck was attached with only two small screws. A substantial amount of water was able to enter the building during the hurricane.

Construction Guidance

Mechanical Penthouse: By placing equipment in mechanical penthouses rather than being exposed on the roof, equipment within penthouses is shielded from high-wind loads and windborne debris (see Figure 2). Therefore, use of mechanical penthouses designed and constructed in accordance with a current building code are recommended, particularly for critical and essential facilities.

Design Loads and Safety Factors: Loads on rooftop equipment should be determined in accordance with the 2005 edition of ASCE 7.

Note: For guidance on load calculations, see "Calculating Wind Loads and Anchorage Requirements for Rooftop Equipment," ASHRAE Journal, volume 48, number 3, March 2006.

A minimum safety factor of 3 is recommended for critical and essential facilities, and a minimum safety factor of 2 is recommended for other buildings. Loads and resistance should also be calculated for heavy pieces of equipment (see Figure 2).

Figure 2. This 30' x 10' x 8' 18,000-pound HVAC unit was attached to its curb with 16 straps (one screw per strap). Although the wind speeds were estimated to be only 85 to 95 miles per hour (3-second peak gust), it blew off the building.

Simplified Attachment Table: To anchor fans, small HVAC units, and relief air hoods, the following minimum attachment schedule is recommended (see Table 1) (note: the attachment of the curb to the roof deck also needs to be designed to resist the design loads):

Table 1. Number of #12 Screws for Base Case Attachment of Rooftop Equipment

Case No.	Curb Size and Equipment Type	Equipment Attachment	Fastener Factor for Each Side of Curb or Flange
1	12"x 12" Curb with Gooseneck Relief Air Hood	Hood Screwed to Curb	1.6
2	12"x 12" Gooseneck Relief Air Hood with Flange	Flange Screwed to 22 Gauge Steel Roof Deck	2.8
3	12"x 12" Gooseneck Relief Air Hood with Flange	Flange Screwed to 15/32" OSB Roof Deck	2.9
4	24"x 24" Curb with Gooseneck Relief Air Hood	Hood Screwed to Curb	4.6
5	24"x 24" Gooseneck Relief Air Hood with Flange	Flange Screwed to 22 Gauge Steel Roof Deck	8.1
6	24"x 24" Gooseneck Relief Air Hood with Flange	Flange Screwed to 15/32" OSB Roof Deck	8.2
7	24"x 24" Curb with Exhaust Fan	Fan Screwed to Curb	2.5
8	36"x 36" Curb with Exhaust Fan	Fan Screwed to Curb	3.3
9	5'-9"x 3'- 8" Curb with 2'- 8" high HVAC Unit	HVAC Unit Screwed to Curb	4.5*
10	5'-9"x 3'- 8" Curb with 2'- 8" high Relief Air Hood	Hood Screwed to Curb	35.6*

Notes to Table:

1. The loads are based on the 2005 edition of ASCE 7. The resistance includes equipment weight.

2. The Base Case of the tabulated numbers of #12 screws (or ¼ pan-head screws for flange-attachment) is a 90-mph basic wind speed, 1.15 importance factor, 30' building height, Exposure C, using a safety factor of 3.

3. For other basic wind speeds, or for an importance factor of 1, multiply the tabulated number of #12 screws by $\left(\frac{V_D^2 \times I}{90^2 \times 1.15}\right)$ to determine the required number of #12 screws or (¼ pan-head screws) required for the desired basic wind speed, V_D (mph) and importance factor, I.

4. For other roof heights up to 200', multiply the tabulated number of #12 screws by (1.00 + 0.003 [h - 30]) to determine the required number of #12 screws or ¼ pan-head screws for buildings between 30' and 200'.

Example A: 24" x 24" exhaust fan screwed to curb (table row 7), Base Case conditions (see Note 1): 2.5 screws per side; therefore, round up and specify 3 screws per side.

Example B: 24" x 24" exhaust fan screwed to curb (table row 7), Base Case conditions, except 120 mph and importance factor of 1: 120^2 x 1 ÷ 90^2 x 1.15 = 1.55 x 2.5 screws per side = 3.86 screws per side; therefore, round up and specify 4 screws per side.

Example C: 24" x 24" exhaust fan screwed to curb (table row 7), Base Case conditions, except 150' roof height: 1.00 + 0.003 (150' - 30') = 1.00 + 0.36 = 1.36 x 2.5 screws per side = 3.4 screws per side; therefore, round down and specify 3 screws per side.

* This factor only applies to the long sides. At the short sides, use the fastener spacing used at the long sides.

Fan Cowling Attachment: Fans are frequently blown off their curbs because they are poorly attached. When fans are well attached, the cowlings frequently blow off (see Figure 3). Unless the fan manufacturer specifically engineered the cowling attachment to resist the design wind load, cable tie-downs (see Figure 4) are recommended to avoid cowling blow-off. For fan cowlings less than 4 feet in diameter, 1/8-inch diameter stainless steel cables are recommended.

Figure 3. Cowlings blew off two of the three fans shown in this photo. Cowlings can tear roof membranes and break glazing.

Figure 4. To overcome blow-off of the fan cowling, this cowling was attached to the curb with cables.

For larger cowlings, use 3/16-inch diameter cables. When the basic wind speed is 120 mph or less, specify two cables. Where the basic wind speed is greater than 120 mph, specify four cables. To minimize leakage potential at the anchor point, it is recommended that the cables be adequately anchored to the equipment curb (rather than anchored to the roof deck). The attachment of the curb itself also needs to be designed and specified.

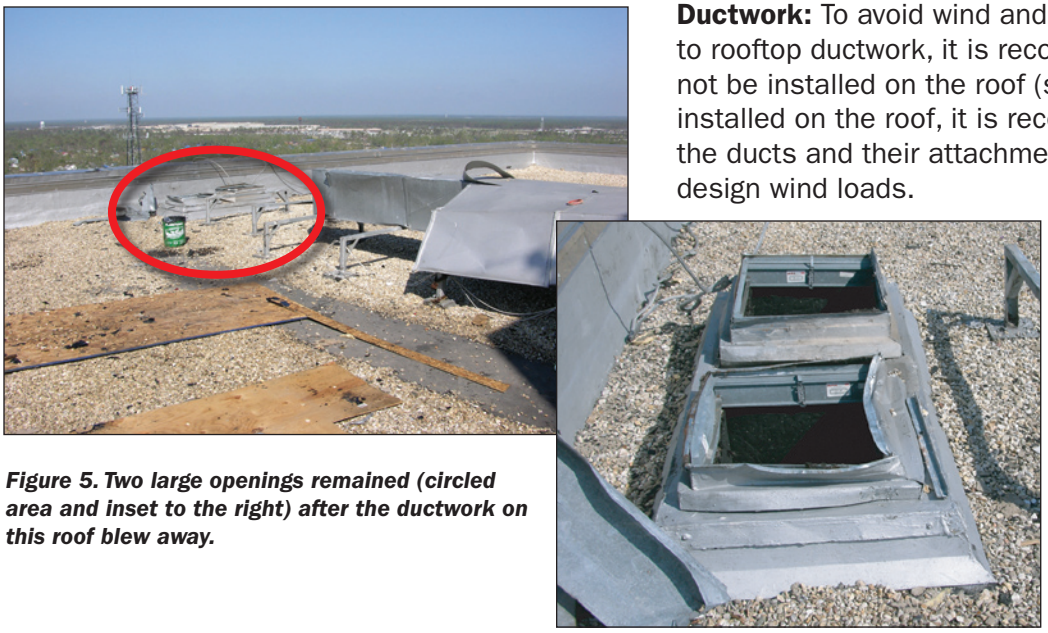


Figure 5. Two large openings remained (circled area and inset to the right) after the ductwork on this roof blew away.

Ductwork: To avoid wind and windborne debris damage to rooftop ductwork, it is recommended that ductwork not be installed on the roof (see Figure 5). If ductwork is installed on the roof, it is recommended that the gauge of the ducts and their attachment be sufficient to resist the design wind loads.

Condensers: In lieu of placing rooftop-mounted condensers on wood sleepers resting on the roof (see Figure 6), it is recommended that condensers be anchored to equipment stands. (Note: the attachment of the stand to the roof deck also needs to be designed to resist the design loads.) In addition to anchoring the base of the condenser to the stand, two metal straps with two side-by-side #14 screws or bolts at each strap end are recommended (see Figure 7).

Figure 6. Sleeper-mounted condensers displaced by high winds.

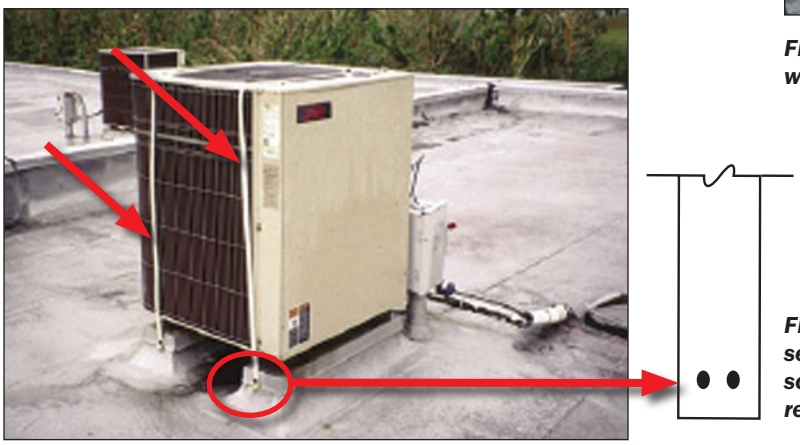


Figure 7. This condenser had supplemental securement straps (see arrows). Two side-by-side screws with the proper edge and end distances are recommended at the end of the strap.

Vibration Isolators: When equipment is mounted on vibration isolators, an isolator that has sufficient resistance to meet the design uplift loads should be specified and installed, or an alternative means to accommodate uplift resistance should be provided (see Figure 8).

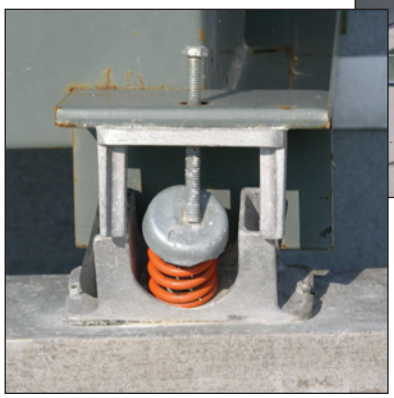


Figure 8. The equipment on this stand was resting on vibration isolators that provided lateral resistance but no uplift resistance (above). A damaged vibration isolator is shown in the inset (left).

Access Panel Attachment: Access panels frequently blow off. To minimize blow-off of access panels, job-site modification will typically be necessary (for example, the attachment of hasps and locking devices such as a carabiner). The modification details will need to be tailored for the equipment, which may necessitate detail design after the equipment has been delivered to the job site. Modification details should be approved by the equipment manufacturer.

Figure 9. Several of the equipment screen panels were blown away. Loose panels can break glazing and puncture roof membranes.

Equipment Screens: Equipment screens around rooftop equipment are frequently blown away (see Figure 9). Equipment screens should be designed to resist the wind loads derived from ASCE 7.

Note: The extent that screens may reduce or increase wind loads on equipment is unknown. Therefore, the equipment behind screens should be designed to resist the loads previously noted.

Other resources: Three publications pertaining to seismic restraint of equipment provide general information on fasteners and edge distances:

- Installing Seismic Restraints for Mechanical Equipment (FEMA 412)
- Installing Seismic Restraints for Electrical Equipment (FEMA 413)
- Installing Seismic Restraints for Duct and Pipe (FEMA 414)

FACILITY-RELATED CONTROL SYSTEMS

CYBERSECURITY GUIDELINE

DOCUMENT CONTROL	
VERSION	**DESCRIPTION**
Version 1.0 – 10/31/2016	Draft
Version 2.0 – 01/24/2017	Updated to use Facility-Related Control Systems (FRCS), incorporated External and Internal Networks definitions, updated Chapter 4
Version 3.0 – 05/16/2017	Updated to use Cybersecurity in lieu of Information Assurance, updated Design and Construction Sequence Table STIGs development time line

Contents

CHAPTER 1. INTRODUCTION 3
1.1 PURPOSE AND SCOPE 3
1.2 BACKGROUND 3
1.3 APPLICABLE POLICIES, STANDARDS AND PROCEDURES 4
1.4 ROLES AND RESPONSIBILITIES 5
1.5 REQUIRED SUBMITTALS 5
1.6 APPLICABLE ESTCP CS TEMPLATES 7
1.7 GLOSSARY (PER UFC 4-010-06) 7
1.8 REQUIREMENTS FOR SUBJECT MATTER EXPERTS 12
1.9 FRCS REFERENCE ARCHITECTURE 13
1.10 TEST AND DEVELOPMENT ENVIRONMENT 14
CHAPTER 2. FRCS CYBERSECURITY REQUIREMENTS 15
2.1 FRCS CYBERSECURITY REQUIREMENTS 15
2.2 FRCS CATEGORIZATION 16
2.3 FRCS CONFIGURATION MANAGEMENT 16
2.2 FRCS COMMISSIONING 16
2.2 FRCS CONTINUOUS MONITORING 16
CHAPTER 3. DESIGN AND CONSTRUCTION RESOURCES, DELIVERABLES AND CHECKLISTS 18
3.1 DESIGN AND CONSTRUCTION RESOURCES 18
3.2 TYPICAL SEQUENCE OF FRCS DESIGN AND CONSTRUCTION ACTIVITIES 20
CHAPTER 4. TYPICAL FACILITY-RELATED CONTROL SYSTEMS CONTRACT SUBMITTALS 24
4.1 FRCS IA SUBMITALL REQUIREMENTS 24
4.1 FRCS FRONT END INTEGRATION 27
4.2 FRCS CABLING 28
4.3 FRCS WIRELESS 28

CHAPTER 1. INTRODUCTION

1.1 PURPOSE AND SCOPE This document defines the Cybersecurity Procedures for ESTCP Facility-Related Control Systems projects. The intention of this document is to provide a general outline and more granular guide for the planning, design, construction, operations and commissioning of the FRCS following the Risk Management Framework (RMF) process outlined in UFC 04-010-06 Cybersecurity of Facility-Related Control Systems.

1.2 BACKGROUND Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, and DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), incorporate Platform IT (PIT) into the RMF process. PIT is a category of both IT hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. PIT is further categorized as PIT products, PIT subsystems, or PIT systems. PIT differs from "traditional" IT in that it is integral to – and dedicated to the operation of – a specific platform. Although the term PIT is used only by DoD, the concept of categorizing components and systems dedicated to the operation of a specific platform is not. For example, the term "Operational Technology" (OT) is also used to refer to these systems and components.

The most common forms of Facilities-Related PIT are Control Systems (CS), which are a combination of control components (e.g., electrical, mechanical, hydraulic, or pneumatic, etc.), special purpose controlling devices, and standard IT that act together upon underlying mechanical and/or electrical equipment to achieve an objective (e.g., transport of matter or energy, maintain a secure and comfortable work environment, etc.). All automated control systems are considered PIT. Industrial Control Systems (ICS) are automated control systems that act upon industrial systems and processes. ICS is used as a general term that encompasses several – but not all -- types of control systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other control systems, such as the Programmable Logic Controllers (PLCs) often found in the industrial sector and critical infrastructure.

To protect its facilities and infrastructure, DoD needs to know the type, quantity and purpose of PIT it owns and uses. For all PIT identified, including CS, the PIT owner, in coordination with an Authorizing Official (AO), must determine whether a collection of PIT products and/or subsystems "rises to the level of" a PIT System. In accordance with DODI 8510.01, PIT products and/or subsystems which do not rise to the level of a PIT System must undergo security assessment, but do not necessarily need to be authorized under the RMF. However, PIT Systems undergo both security assessment and authorization by an AO.

The enterprise system used to track DoD IT, including PIT, is the Enterprise Mission Assurance Support Service (eMASS). Both "Assess and Authorize" and "Assess-Only" CS will be entered into eMASS. In order to standardize how EI&E-owned and -operated CS information is entered into eMASS, the DoD CS Working Group (WG) is working to incorporate new data fields and PIT capabilities into eMASS. DoD has developed a list of common CS and a corresponding control overlay selection tool for selecting an appropriate combination of security controls in the EI&E PIT Control System Master List. The EI&E PIT Control System Master List is maintained along with this step-by-step guide on the DoD Chief Information Officer (CIO) RMF Knowledge Service portal, where it will remain a living document.

1.3 APPLICABLE POLICIES, STANDARDS AND PROCEDURES

- CNSSI 1253, Security Categorization And Control Selection For National Security Systems 2014
- Department of Defense Instruction 8500.01, Cybersecurity, March 2014 (available online at www.dtic.mil)
- Department of Defense Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 2014 (available online at www.dtic.mil)
- Department of Defense Instruction 8140 Cyberspace Workforce Management (available online at http://www.wbdg.org/pdfs/dod_cyberworkforce.pdf)
- Department of Defense Instruction 8530 Cybersecurity Activities Support to DoD Information Network Operations March 2016 (available online at http://www.wbdg.org/pdfs/DODI_853001_2016.pdf)
- Department of Defense Industrial Control Systems Advanced Tactics, Techniques and Procedures Jan 2016 (available online at http://www.wbdg.org/pdfs/jbasics_aci_ttp_2016.pdf)
- Department of Defense Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations (available online at http://www.wbdg.org/pdfs/ics_handbook.pdf)
- Federal Information Processing Standard 200 Minimum Security Requirements for Federal Information and Information Systems
- Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- National Institute of Standards and Technology Special Publication 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations 2013
- National Institute of Standards and Technology Special Publication 800-82 R2 Guide to Industrial Control Systems (ICS) Security 2015
- National Institute of Standards and Technology Special Publication SP 800-115 Technical Guide to Information Security Testing and Assessment 2008
- Department of Veterans Affairs Mental Health Facilities Design Guide 2010
- Department of Veterans Affairs Office of Information & Technology Design Guide 2011
- Department of Veterans Affairs Telecommunications and Special Telecommunication Design Manual (TDM) 01-2016
- Unified Facility Criteria Design 4-510-01 Military Medical Facilities 2014
- UFC 3-410-01 Utility Monitoring And Control System (CS) Front End And Integration 2016 (DRAFT)
- UFC 3-410-02 Direct Digital Control For HVAC And Other Building Control Systems 2016 (DRAFT)
- UFGS 23 09 00 Instrumentation and Control for HVAC (available online at www.wbdg.org)
- UFGS 23 09 23.01 LonWorks® Direct Digital Control for HVAC and Other Building Systems (available online at www.wbdg.org)
- UFGS 23 09 23.02 BACnet Direct Digital Control for HVAC and Other Building Systems (available online at www.wbdg.org)
- UFGS 25 10 10 Utility Monitoring And Control System (CS) Front End And Integration (available online at www.wbdg.org)

- Government Accounting Office Report 15-6 Federal Facility Cybersecurity 2014
- Building Industry Consulting Service International (BICSI) Telecommunications Distribution Methods Manual (TDMM)
- National Fire Protection Association (NFPA) 101 Life Safety Code 2015
- UL 639 Intrusion Detection Standard 2007
- UL 60950-1 Information Technology Equipment - Safety - Part 1: General Requirements 2013

1.4 ROLES AND RESPONSIBILITIES

Role: Government Stakeholders
Members: Service Design Manager, Facilities Engineering Acquisition Department (FEAD), Services Civil Engineering Representative (NAVFAC, AFCEC, USACE, DPW, etc.), Integrated Product Team (IPT).
Responsibilities: Review ESTCP CS Installation Contractor submittals, test reports, and Commissioning reports.

Role: ESTCP CS Installation Contractor
Members: Contractor responsible for the installation or modification of a CS network component. Includes the contractor's Control Systems Cybersecurity Specialist and Integration Specialist.
Responsibilities: Responsible for production and submittal of all project Configuration Items (CI's), project CI inventories, and design/construction/commissioning documentation associated with the installation or modification of CS systems.

Role: ESTCP CS Engineer of Record
Members: Project mechanical engineer of record, electrical engineer of record, and control system engineer of record (if applicable)
Responsibilities: Responsible for modifying the provided UFGS and ESTCP CS Engineering Manual design templates to meet the requirements of the specific project

Role: ESTCP CS Service Agreement Contractor
Members: Contractor(s) responsible for the operation and maintenance of the installation's CS network.
Responsibilities: Following configuration management procedures during required system modifications, security patches, and firmware upgrades.

Role: ESTCP Information Owner/Steward
Members: Installation Chief Information Officer (CIO)
Responsibilities: Responsible for maintaining the current baseline of Configuration Items, management of the CI repository, and managing and tracking the security state of information systems.

Role: Security Control Assessor (SCA)
Members: Installation Chief Information Officer (CIO)

1.5 REQUIRED SUBMITTALS

The Contractor(s) shall develop and upload into the DoD CIO eMASS tool, if required, for an Assess Only, Interim Authority To Operate (IATO), or Authority To Operate (ATO) package, all required artifacts and supporting documentation. The required artifacts are determined by the system security classification, system categorization, and cybersecurity controls.

For ETSCP projects, the intent is to only provide the **MINIMUM** documentation necessary to

demonstrate the R&D objective and capability to achieve an RMF approval. In general, for a Closed Restricted Network (CRN) or Stand-Alone, it will be an Assess Only project and **ONLY** the System Security Plan, the IT Contingency Plan and CONOPS Plans are required. For projects that will connect to the DoDIN, the full RMF Asses and Authorization will typically be required for the IATO or ATO packages. The RMF package information may include but is not limited to the list below:

a. System Security Plan (SSP)
b. Configuration Management Plan (CMP)
c. Disaster Recovery Plan (DRP)
d. Continuity of Operations (COP)
e. Information Technology Contingency Plan (ITCP)
f. Incidence Response Plan (IRP)
g. Security Assessment Report (SAR)
h. Plan of Action and Milestones (POAM)
i. System Architecture/Topology/Data Flow
j. Configuration Validation Checklist
k. Security Classification Guide
l. System Configuration Guide
m. Hardware Inventory List
n. Software Inventory List
o. Physical Security Plan
p. Personnel Security Plan
q. Cybersecurity Vulnerability Management (IAVM) Process
r. Patch Management Process, Connection Approval / System Approval documentation
s. Ports, Protocols, and Services (PPS) List
t. Active Directory (AD) Documentation, (if applicable)
u. TBD on project specific basis: Jump-Kit Rescue CD

For projects requiring an IATO or ATO, the data representing this information may either be uploaded directly, or cut and pasted from the CSET tool or the CIO Core Authorization excel file, into the eMASS tool for each applicable control. In addition, eMASS will provide a rollup of inherited controls for each system once it has been properly identified and classified. It is recommended that the current version of the Department of Homeland Security (DHS) Cyber Security Evaluation Tool (CSET) be used as a development tool for eMASS tool artifacts.

Completion of Scan/Fix/Scan Testing and Analysis: This work is performed before the Security Control Assessor (SCA) assesses the system(s) and provides a certification recommendation to the Authorizing Official (AO). The Contractor shall assess (scan and perform manual checks) its own system using

approved cybersecurity scanning tools. When issues are found (High, Medium, Low Impact Levels) the Contractor shall fix those issues and rescan the system to ensure all issues have been fixed and/or properly and acceptably mitigated. High impact level findings that cannot be fixed are to be reported to the Government immediately along with a valid reason the vulnerability cannot be fixed and a mitigation plan to fix the vulnerability in the future. The goal is for the system to have a proper cybersecurity posture before the SCA comes in to assess the system. The scan/fix/scan process should find and fix all issues before the SCA's assessment.

Completion of Documentation to Connect to the DoDIN: This shall be based on the services connection approval process (CAP). The ESTCP Project Team shall provide required assistance and documentation to the Government to satisfy the CAP. Normally this entails having an approved IATO or ATO, but it may vary depending on the site. When Penetration Vulnerability Testing (PVT) will be required to be performed on the sites network then completion of the CAP should be scheduled to occur before PVT. When PVT is not performed then the timeline for the CAP should be at least forty-five (45) days before connecting to the sites network.

1.6 APPLICABLE ESTCP FRCS TEMPLATES

- Factory Acceptance Testing Checklist
- Site Acceptance Testing Checklist
- DoD RMF Core Security Authorization Package
- ESTCP FRCS RMF ATO WBS Cost Template

1.7 GLOSSARY (PER UFC 4-010-06)

1.7.1 ACRONYMS

Acronym	Term
ACL	Access Control List
AO	Authorizing Official
BAS	Building Automation System
BCS	Building Control System
CCTV	Closed Circuit Television
CNSSI	Committee on National Security Systems Instruction
CCI	Control Correlation Identifier
COTS	Commercial Off The Shelf
CS	Control System
DoD	Department of Defense
ESS	Electronic Security System
EMCS	Energy Monitoring and Control System

FCN	Field Control Network
FISMA	Federal Information Security Management Act
FPOC	Field Point of Connection
GFE	Government Furnished Equipment
ICS	Industrial Control System
IDS	Intrusion Detection System
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IP	Internet Protocol
IT	Information Technology
MOA	Memorandum Of Agreement
MOU	Memorandum Of Understanding
NIST	National Institute of Standards and Technology
OS	Operating System
PIT	Platform Information Technology
PKI	Public Key Infrastructure
SCADA	Supervisory Control and Data Acquisition
SO	System Owner
UCS	Utility Control System
UFC	Unified Facilities Criteria
UFGS	Unified Facilities Guide Specification
CS	Utility Monitoring and Control System
USACE	U.S. Army Corps of Engineers

1.7.2 DEFINITION OF TERMS

Term Definition

Authorizing Official (CNSS Glossary) A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Building Automation System (BAS) The system consisting of a CS Front End, connected Building Control Systems which control building electrical and mechanical systems, and user interfaces for building control supervision. The BAS is a subsystem of the Utility Monitoring and Control System. This term is being phased out in favor of CS.

Building Control System (BCS) A system that controls building electrical and mechanical systems such as HVAC (including central plants), lighting, vertical transport systems, and irrigation systems. Building Control Systems generally do not have a full-featured user interface; they may have "local display panels" but typically rely on the CS front end for full user interface functionality. BCS is a subsystem of the Utility Monitoring and Control System, and is a class of Field Control System.

Closed Circuit Television System (CCTV) An ESS that allows video assessment of alarm conditions via remote monitoring and recording of video events. Video monitoring may also be incorporated into other systems which are not CCTV.

Control Correlation Identifier (CCI) The Control Correlation Identifier (CCI) provides a standard identifier and description for each of the singular, actionable statements that comprise a security control.

Control System (CS) A system of digital controllers, communication architecture, and user interfaces that monitor, or monitor and control, infrastructure and equipment.

Controller An electronic device – usually having internal programming logic and digital and analog input/output capability – which performs control functions. Two primary types of controller are equipment controller and supervisory controller.

Distributed Control System This term is being phased out in preference of BCS, UCS, and/or CS.

Electronic Security System (ESS) The integrated electronic system that encompasses interior and exterior (physical) intrusion detection systems (IDS), CCTV systems for assessment of alarm conditions, access control systems, data transmission media, and alarm reporting systems for monitoring, control, and display.

Energy Monitoring Control System (EMCS) Another name for a Utility Monitoring and Control System. See CS.

Equipment Controller (EC) A controller implementing control logic to control a piece of equipment. Note: a controller is defined by use, and many ECs also have the capability to act as supervisory controllers (SC). Some examples of equipment controllers are air handler controllers, protective relays, and pump controllers. Note that some devices, such as power meters or smart sensors, which only perform monitoring functions are still considered equipment controllers (despite not actually controlling anything).

Facility-Related Control System A control system which controls equipment and infrastructure that is part of a DoD building, structure, or linear structure.

Field Control System (FCS) A Building Control System, Utility Control System, Access Control System, etc. within the Facility and "downstream" of the FPOC.

Field Control Network (FCN) The network used by the Building Control System, Utility Control System, etc., within a facility "downstream" of the FPOC. This includes IP, Ethernet, RS-485, TP/FT-10 and other network infrastructure that support control system(s) in a given facility.

Field Point of Connection (FPOC) The FPOC is the point of connection between the ICS IP network and the field control network (an IP network, a non-IP network, or both). The hardware which provides the connection at this location is an IT device such as a switch, IP router, or firewall.

[CS, PCS, ESS, etc.] Front End The portion of the control system consisting primarily of IT equipment, such as computers and related equipment, intended to perform operational functions and run monitoring and control/engineering tool application software. The front end does not directly control physical systems; it interacts with them only through field control systems (FCS). The front end is a component of the [CS, ESS, etc.] infrastructure (see definition).

Impact The effect on organizational operations, organizational assets, or individuals due to a loss of Confidentiality, Integrity, or Availability in the control system. Impact is categorized as one of three levels:

- LOW: limited adverse effect
- MODERATE: serious adverse effect
- HIGH: severe or catastrophic adverse effect

The impact level of a system is generally written in ALL CAPS for clarity.

Incident (FIPS 200) An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

Industrial Control System (ICS) One type of control system. Most specifically a control system which controls an industrial (manufacturing) process. Sometimes also used to refer to other types of control systems, particularly utility control systems such as electrical, gas, or water distribution systems.

Information Technology (IT) Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

[CS, ESS, ...] Infrastructure The portion of a control system (such as a CS or ESS) which includes all components that are not part of a field control system. These components include the FPOC, the Platform Enclave, and the front end (i.e. it's architecture Levels 3, 4 and 5)

Intrusion Detection System (IDS) [Physical/ESS] A system consisting of interior and exterior sensors, surveillance devices, and associated communication subsystems that collectively detect an intrusion of a specified site, facility, or perimeter and annunciate an alarm.

Intrusion Detection System (IDS) [Cyber] A device or software application that monitors network or system activities for malicious activities or policy violations, and produces reports to management.

Mobile Code (NIST SP 800-53r4) Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Mobile Code Technology (NIST SP 800-53r4) Software technologies that provide the mechanisms for the production and use of mobile code (e.g. Java, JavaScript, ActiveX, VBScript)

Non-Local Maintenance (NIST SP 800-53r4) Maintenance activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

[CS, ESS, ...] Platform Enclave Those components of the control system that are standard IT components and can be secured in a standard manner independent of the type of control system. These components serve only the control system and include the IP network, network management and security devices (e.g., switches, routers), software, computers and/or other devices which provide management and security of the network.

Platform IT (PIT) IT, both hardware and software, which is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Remote Access (NIST SP 800-53r4) Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet).

Risk (NIST SP 800-53r4) A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Management (NIST SP 800-53r4) The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Security Content Automation Protocol (SCAP) A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP.

Supervisory Control and Data Acquisition (SCADA) This term is being phased out in preference of BCS, UCS, and/or CS.

Supervisory Controller A controller that implements a combination of supervisory logic (global control or optimization strategies), scheduling, alarming, event management, trending, web services or network management. A supervisory controller may be located between the Platform Enclave and the FCS

serving as the data aggregation conduit between the FCS and the front end. Note that this arrangement is defined by use; many supervisory controllers have the capability to also directly control equipment, and serve the role of both supervisory controller and equipment controller.

Utility Control System (UCS) A type of field control system used for control of utility systems such as electrical distribution and generation, sanitary sewer collection and treatment, water generation and pumping, etc. Building controls are excluded from a UCS, however it is possible to have a Utility Control System and a Building Control System in the same facility, and for those systems to share components such as the FPOC. A UCS is a subsystem of a Utility Monitoring and Control System (CS) and is a class of Field Control System (FCS).

Utility Monitoring and Control System (CS) The system consisting of one or more building control systems and/or utility control systems and the associated CS Infrastructure. In other words, it is the complete utility monitoring system – from the front end to equipment controllers. At the highest level the CS is composed of a CS Platform Enclave and CS Front End (jointly referred to as CS Infrastructure), and connected Field Control System(s).

CS IP Network The Level 4 IP network used by the CS.

Vulnerability (NIST SP 800-53r4) Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

1.8 REQUIREMENTS FOR SUBJECT MATTER EXPERTS

The CS shall be designed and engineered by qualified Control System Cybersecurity, Information and Communication Technology, and System Integration specialists complying with the requirements listed below.

1.8.1 Control Systems Cybersecurity Specialist:

The Control Systems Cybersecurity specialist shall have a minimum of five years' experience in control system network and security design and shall maintain current certification as a Global Industrial Cyber Security Professional (GISCP) or Certified Information Systems Security Professional (CISSP). The Control Systems Cybersecurity specialist must have demonstrated knowledge and experience applying IT and OT security strategies such as the application of the NIST security controls, exploitation techniques and methods, continuous monitoring, and utility/building control systems design. The résumé of the specialist must be submitted to the ESTCP Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

1.8.2 Information and Communication Technology Specialist:

The Information and Communication Technology specialist shall have a minimum of five years' experience in control system network and security design and shall maintain current certification as a Registered Communications Distribution Designer (RCDD®). The Information and Communication Technology specialist must have demonstrated knowledge and experience applying IT and OT security strategies such as the application of the NIST security controls, cable network design and installation, project management, and data center design. The résumé of the specialist must be submitted to the ESTCP Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

1.8.3 System Integration Specialist:

The System Integration specialist shall have a minimum of five years' experience in control system network and shall maintain current certification as a Certified System Integrator (CSI) for the products they are integrating (Tridium, Johnson Controls, Wonderware,

Schneider, Schweitzer Engineering Laboratories, Rockwell, etc.) and/or be Control System Integrators Association (CISA) Certified. The System Integrator specialist must have demonstrated knowledge and experience applying IT and OT security strategies such as the application of the NIST security controls, BAS design and installation, project management, quality assurance and commissioning. The résumé of the specialist must be submitted to the ESTCP Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

1.9 **FRCS REFERENCE ARCHITECTURE** The DoD FRCS Reference Architecture as defined in UFC 04-010-06 Cybersecurity of Facility-Related Control Systems is provided in Figure 1.

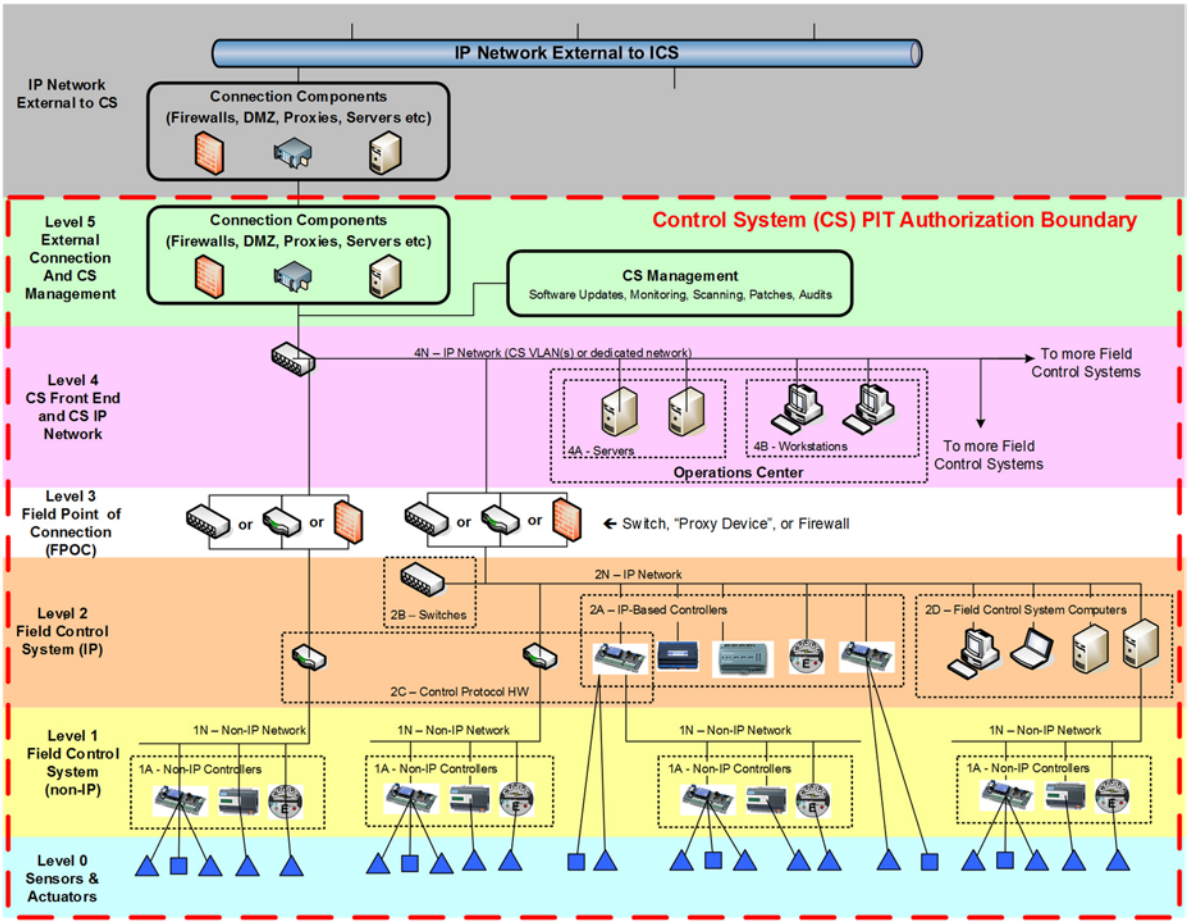


Figure 1 DoD FRCS Reference Architecture

UFC 04-010-06 Appendix E 5-Level Control System Architecture describes the 5-Level architecture for FRCS and presents cybersecurity considerations for each level. The FRCS level architecture is used to define the authorization boundary for FRCS systems and is a logical representation of the FRCS network. While many baseline security controls can be applied to a FRCS, how and where they are implemented varies, primarily because of technical and operational constraints. Interconnections between FRCS and organizational networks and business systems expose FRCS to exploits and vulnerabilities. Any attempts to address these exploits and vulnerabilities must consider the constraints and requirements of the FRCS.

Networked FRCS are those systems which have multiple controllers and can have both traditional IP traffic at the Level 3 and up, and Ethernet IP and serial traffic at the lower levels as defined by the UFC 04-010-06 Cybersecurity of Facility-Related Control Systems Reference Architecture Figure 5.1. Depending on the age and type of FRCS, these FRCS **MAY** have the capability for remote monitoring; almost all 2005 and newer CS are IP and web based and typically as part of the vendor service level agreement, most require remote access to the system for maintenance.

Non-networked FRCS are generally those that consist of a single controller, and do not have the capability for remote monitoring.

There are two types of networked FRCS; Internally Networked (IN), also designated as Closed Restricted Networks (CRN), which have multiple components networked together, but does not have a network connection to anything that is not part of the control system, and FRCS that are Externally Networked (EN), where the control system has multiple component networked together, and does connect to a network that is not part of the control system, most commonly the NIPR, Commercial Carrier/Internet, or separate government backbone network such as DHA Med COI, Navy PSNet or the Air Force CE VLAN.

If the FRCS is a EN (requires a connection to the DoDIN as defined by DoDI 8530.0), it will go through the full 6-step RMF process. If the FRCS is an IN and is a CRN, it can use the shorter Evaluate and Endorse process. Both IN and EN FRCS will follow the DoD Control Systems Reference Architecture levels as defined by UFC 04-010-06 Cybersecurity of Facility-Related Control Systems. Organizations will use a tailored set of security controls to evaluate automated control systems consistent with the RMF Assess & Authorize process through the implementation of the applicable controls in NIST SP 800-82R2.

The IA Guideline applies to all of the networks, components and devices within the Authorization Boundary.

1.10 TEST AND DEVELOPMENT ENVIRONMENT

For new or major modernization projects, the Systems Integrator will establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, software and with at least one of each of the Level 3-0 major components, devices, and actuators. At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the project to ensure the project has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides (STIGS), all patches (OS and CS) are installed and properly configured, and begin creating the artifacts for the draft System Security Plan.

At approximately 95-100% construction complete, the TDE will be used to conduct Site Acceptance Testing of the complete CS, and if required, Penetration testing. The SAT artifacts will be included in the final System Security Plan, FMC and Jump-Kit (if required).

The ESTCP Project Team/System Integrator will transfer the TDE to the ESTCP PM for inclusion into the Platform Enclave FRCS Operations Center.

CHAPTER 2. FRCS CYBERSECURITY REQUIREMENTS

2.1 FRCS CYBERSECURITY REQUIREMENTS

As long as DOD uses outside contractors to design, construct, and operate building control systems, it is vitally important that contractors and vendors become part of the cybersecurity solution, starting with the supply chain and ending with proper disposal of obsolete equipment. Cybersecurity of the FRCS begins in the planning and design phases, it is imperative that the FRCS design and construction teams understand the NIST RMF process and the various documents and artifacts associated with an Authorization package.

The Continuous Monitoring (CM) Strategy has been developed by the DOD using the DISA ESS tool suite for the Level 4 Operations Center servers and workstations. The ESTCP PI and support/system integrator contractors will be given guidance on the tools and applications to use for Level 3 and below components and devices. The PIT Control System Cybersecurity Lifecycle is shown in Figure 2.

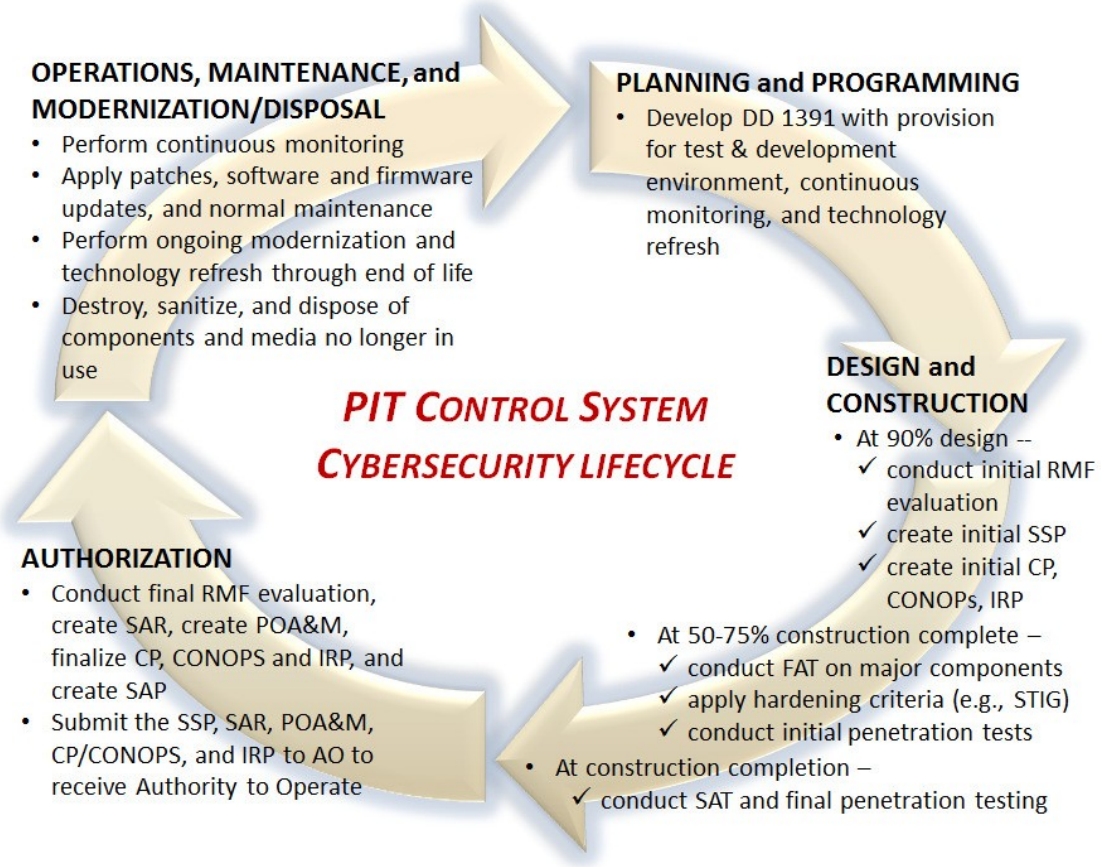


Figure 2 CS Cybersecurity Lifecycle

DoD has developed the facilities RMF Enclave Boundary approach that provides Defense In Depth and which is composed of two distinct authorizations:

- Platform Enclave (provided by hosting service/agency)
- Operational Architectures (the authorization that ESTCP projects will document)

The ESTCP office will assist Project Teams to obtain PE integration and documentation to coordinate their OA RMF authorization.

2.2 FRCS CATEGORIZATION

A key first Step 1 of the RMF is to categorize the FRCS for Confidentially, Integrity and Availability (C-I-A). The RMF KS portal EI&E webpage and the ESTCP website have the FRCS Master List and preliminary C-I-A values. The ESTCP office in conjunction with the PE owner and the Project Team will determine the final C-I-A values. In general, the majority of the ESTCP projects are expected to be L-L-M or M-M-H systems.

2.3 FRCS CONFIGURATION MANAGEMENT A FRCS configuration standard shall be established to support effective and efficient monitoring of the FRCS. Managing the configuration requires the following:

- Maintain baseline configurations in accordance with technical specifications for systems and security technology set forth by the PE.
- Establish and enforce security configurations for individual applications such as HVAC, Lighting, and IDS systems and products employed in FRCS.
- Monitor and control changes to the baseline configurations and to the constituent components of security systems (including hardware, software, firmware, and documentation) throughout the respective system lifecycle. Configuration management can be largely accomplished through updating FRCS documentation received during initial project installation.
- The PE and the CIO, is responsible for tracking and maintaining the baseline configuration of the FRCS.

2.2 FRCS COMMISSIONING FRCS systems, subsystems, and software programming shall undergo comprehensive Factory and Site Acceptance Testing. The acceptance test process shall be documented using a standard testing process that is implemented and assessed by a qualified independent third party. At a minimum, the process shall meet the following requirements:

- Demonstrate the functionality of each FRCS device or component.
- Demonstrate performance characteristics consistent with the manufacture's specifications.
- Demonstrate all functionality including software programming, integration of subsystems, and automation of system functions as specified for the particular project.
- Verify that network connections, IT integration, and IT security requirements meet FIPS, NIST, and all other applicable standards.
- Verify that all life-safety integration requirements and functions meet local and national codes and ordinances.
- Demonstrate startup, recovery from failure, and operator training requirements.

2.2 FRCS CONTINUOUS MONITORING For ESTCP projects that require connection to the DoDIN, the Project Team will be required to demonstrate the solution is compatible with the FRCS continuous monitoring Host-Based Scanning System (HBSS) and ACASS for Level 4, using active scanning and a FRCS passive network monitoring capability to provide end-to-end monitoring of both legacy systems and new systems that can support end-to-end active scanning. The monitoring capability will be based on a robust, multi-tier architecture that provides local, regional, and NSOC alarm monitoring, as well as

remote alarm assessment, dispatch, and response. The multi-tier structure provides multiple levels of FRCS event visibility that corresponds to the DoD Mission Assurance program and includes redundant primary and secondary monitoring capability within regions or in clusters.

For CRN projects, FRCS monitoring capability shall be analyzed on a case-by-case basis to determine suitability and cost effectiveness. The FRCS SSP and ITCP shall identify overall system framework and operational procedures.

CHAPTER 3. DESIGN AND CONSTRUCTION RESOURCES, DELIVERABLES AND CHECKLISTS

3.1 DESIGN AND CONSTRUCTION RESOURCES

The FRCS consultants shall comply with the FRCS UFC's, UFGS, and services/agencies latest construction specifications for FRCS, found on the Whole Building Design Guide, and augmented by other service/agency Policies and Directives. Additional sections shall be prepared by the designer as necessary to suit the project requirements.

The Whole Building Design Guide Cybersecurity Resource Page provides current best cybersecurity practices and references for all types of building control systems and links to several tools to support the development of the RMF IA package and documentation.

A FRCS **MAY** be a hybrid, or converged, system of traditional IT products and Operational Technologies (OT) products that must now be considered an exploit vector that can be used to penetrate into the larger DoDIN network. These hybrid systems contain or transmit Personally Identifiable Information (PII), Protected Critical Infrastructure Information (PCII), Health Insurance Portability and Accountability Act (HIPAA), or Payment Card Industry (PCI) information/data. Examples of systems that may be hybrid, or converged, systems include:

- Access control/alarm systems that use badges/PIV Cards and Active Directory for keyless entry (contain PII).
- Keyless entry/keypad systems that use Active Directory (contain PII).
- Meter data management systems that interconnect with a local utility with real time demand and response (if the meter data is determined to contain PCII).
- Patient Monitoring and Wandering Systems (contain PII, HIPAA).
- Patient Comfort Systems (contain PII, HIPPA)
- Vehicle fueling/charging stations/pumps with credit card swipe (contain PCI).
- Computerized maintenance management systems/work order systems that interconnect with control system back-end controllers and devices (if the system is determined to contain PCII or PII).

IF the FRCS is determined to be a Hybrid/Converged system, then the RMF package will consist of both the NIST SP 800-53R4 and NIST SP 800-82R2 Security Controls. Reference the CIO RMF KS EI&E web portal for more detailed guidance.

The following tools are available for the ESTCP Project Team, designer, construction and systems integrators to use in the creation of the Test and Development Environment (TDE) and Production FRCS.

3.1.1. Cyber Security Evaluation Tool (CSET) The DHS CSET is a useful tool that supports the FRCS design, construction and authorization phases of the CS lifecycle. CSET incorporates NIST, ISO, SANS, and other industry standard references. CSET includes the NIST SP 800-53 R4, NIST SP 800-82 R2, the NIST Cybersecurity Framework, and the Committee for National Security Systems Instruction (CNSSI) 1253 RMF standards and guidelines.

CSET has a plug-in (on initial install of CSET use the custom option) that connects to the National Security Agency-developed GrassMarlin (GM) passive network analysis tool. GM can be used to create

an initial network architecture diagram of existing FRCS. The CSET tool can be used during design and construction to develop baseline risk assessments and initial System Security Plans (SSPs). SSPs are published as Word documents that can be copied into the CIO eMASS Information Repository tool. CSET and the CIO eMASS Information Repository tool relationship is shown in Figure 3.

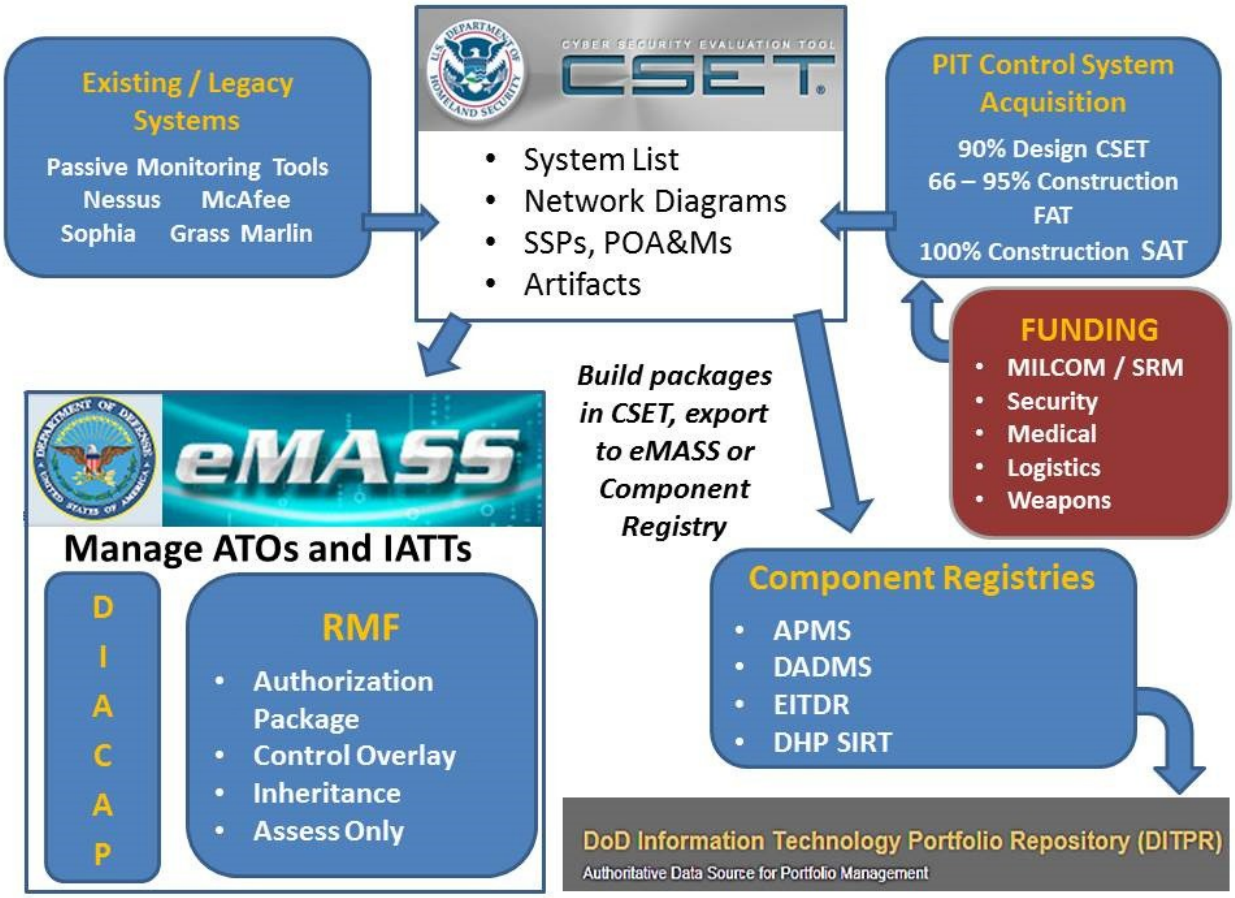


Figure 3 - Relationship of CSET, Component Registry, eMASS, and DITPR

3.1.2 GrassMarlin Passive Network Discovery Tool In support of a passive means to generate an Industrial Control System network and discover IP devices, NSA developed the GrassMarlin (GM) tool. GrassMarlin discovers and catalogs Control System on IP-based networks. GM uses a variety of sources to generate this data, including PCAP files, router and switch configuration files, CAM tables, and live network packet captures. The tool can automatically determine the available networks and generate the network topology as well as visualize the communication between hosts. The GrassMarlin file can be imported into the CSET tool to generate the network architecture and topology diagram and the preliminary inventory of devices and components and should be included on the Jump-Kit Rescue CD.

3.1.3 Security Content Automation Protocol (SCAP) Tool The SCAP tool is used to configure the FRCS BAS hardware and software to the proper DoD and Navy configurations using the Security Technical Implementation Guides (STIGS). The FRCS designer, construction and systems integrators will use the SCAP tool in the Test and Development Environment to create the artifacts required for the RMF

package documentation. The TDE SCAP configuration should be as close as possible to the HBSS ACAS configuration and should be included on the Jump-Kit Rescue CD (if required).

3.1.4 Samurai Software Testing For Utilities Tool The tool was developed by EPRI along with the Smart Grid and Advanced Meter Infrastructure Penetration Guides. The guides and the tool have electrical and utility analysis, penetration, exploit and RF communications procedures and processes and should be included on the Jump-Kit Rescue CD (if required).

3.1.5 Kali Linux Tool The tool is the state of the practice penetration and exploitation tool. The tool is used primarily for penetration testing of IT systems, but is beginning to get some OT capabilities to include Modbus and DNP3 protocols and should be included on the Jump-Kit Rescue CD (if required).

3.1.6 Glasswire Tool The tool is a combination network, firewall, usage and alert capability for IT systems. The tool can be used in the Test and Development Environment to establish the preliminary Functional-Mission Capability Baseline and should be included on the Jump-Kit Rescue CD (if required).

3.1.7 Belarc Advisor Tool The tool is a data gathering and analysis tool for IT systems. The tool can be used in the Test and Development Environment to establish the preliminary Functional-Mission Capability Baseline and should be included on the Jump-Kit Rescue CD (if required).

3.1.8 MalwareBytes Tool The tool is a malware and anti-virus scanner and cleaner for IT systems. The tool can be used in the Test and Development Environment to establish the preliminary Functional-Mission Capability Baseline and should be included on the Jump-Kit Rescue CD (if required).

3.1.9 OSForensics Tool The tool is a forensics data gathering and analysis tool for IT systems. The tool can be used in the Test and Development Environment to establish the preliminary Functional-Mission Capability Baseline and should be included on the Jump-Kit Rescue CD (if required).

3.1.10 Mandiant Redline Tool The tool is a data gathering and analysis tool for IT systems. The tool can be used in the Test and Development Environment to establish the preliminary Functional-Mission Capability Baseline and should be included on the Jump-Kit Rescue CD (if required).

3.1.11 Microsoft SysInternals Suite Tool This suite of tools includes data gathering and analysis tools for IT systems, applications and processes, CPU and memory usage, and Registry tools. The suite can be used in the Test and Development Environment to establish the preliminary Functional-Mission Capability Baseline and should be included on the Jump-Kit Rescue CD (if required).

3.1.12 Host-Based Scanning System (HBSS) and Assured Compliance Assessment Solution (ACAS) Tools HBSS and ACAS are components of the DISA Endpoint Security Solutions (ESS) suite which is an integrated set of capabilities that work together to detect, deter, protect, and report on cyber threats across all DOD networks. The FRCS designer, construction and systems integrators will not typically have access to HBSS ACAS; ESTCP CIO and DISA typically deploy the tools to the new systems being added to the DoD network.

3.2 TYPICAL SEQUENCE OF FRCS DESIGN AND CONSTRUCTION ACTIVITIES

An example sequence and duration of FRCS activities during design and construction is outlined in Table 1.

Table 1 Typical Sequence of FRCS Design and Construction Activities

Activity / Lead	New Project	Renovation Project	Typical Duration
Presolicitation RFP Considerations	Obtain the Regional and ESTCP Platform Enclaves catogorization and categorize the FRCS Use the EI&E FRCS Master Control List for C-I-A Values and Information/Data Types	Obtain the Regional and ESTCP Platform Enclaves catogorization and categorize the FRCS Use the EI&E FRCS Master Control List for C-I-A Values and Information/Data Types	NA
Design • Basis of Design • Concept Design (10-15%) • Design Development (35-50%) • Pre-Final (90%) • Final (100%) Lead: A/E Documents/Models/Tools: • Construction Design Documents / Building Information Model (BIM) / CAD • CSET • GrassMarlin • Draft Baseline System Security Plan (SSP) • IT Contingency Plan and CONOPS (ITCP)	FRCS front end or new susbsystem back end to connect to front end Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline security risk assessment.	FRCS front end upgrade or subsystem modernization Confirm/revise system categorization, define network architecture, system components, concept of operations, drawings, and specifications. At 90% design create initial SSP and baseline security risk assessment.	3-6 Months
Construction Test and Development (T&D) and Patch Management Environments (Virtual or Physical) Lead: Construction/System Integrator Documents/Models/Tools: • VM • Kali Linux • SamuraiSTFU	Conduct FRCS build and patch activities without impacting the organization's production systems (test and development environment typically provided by vendor).	Validate and verify the upgrade/modernization/ patch is ready to support the additional systems without impacting the organization's production systems (test and development environment typically provided by vendor).	4 – 6 weeks

Activity / Lead	New Project	Renovation Project	Typical Duration
Construction Build/Configure Servers	Build and/or configure servers to properly operate the FRCS solution.	Build and/or configure servers to properly operate the FRCS solution.	1 – 2 weeks
Construction Install Supporting Software Lead: Construction/System Integrator	Install supporting software on FRCS servers.	Install supporting software on FRCS servers.	1 – 2 weeks
Construction Configure Supporting Software Lead: Construction/System Integrator Documents/Models/Tools: • STIGS • SCAP • Continuous Monitoring • Kali Linux • SamuraiSTFU • FAT/SAT Checklist • Penetration Testing Scope and ROE (if required) • Jump-Kit Rescue CD	Configure FRCS software to meet unique needs. After the operating system is loaded, apply hardening criteria (STIGs), run Security Content Automated Protocol (SCAP)-validated tool, perform factory acceptance testing (FAT) on major system components and devices, perform initial penetration testing.	Configure FRCS software to meet unique needs. After the operating system is loaded, apply hardening criteria (STIGS), run Security Content Automated Protocol (SCAP)-validated tool, perform FAT on major system components and devices, perform initial penetration testing.	1 – 2 weeks NOTE: If a vendor will be creating a STIG for the UMCS Front-End or lower Level devices, this process can take several months to a year. Apply STIGS to the PE and isolate lower Levels until vendor STIGS are approved.
Construction Implement and assess security controls Lead: construction/system integrator Documents/Models/Tools: • CSET • SSP • Security Assessment Report (SAR) • Plan of Action & Milestones (POAM) • ITCP • Event/Incident Communications Procedures (EICP)	Conduct RMF Steps 3 and 4 by applying controls identified during the requirements and design phase, by assessing the adequacy and effectiveness of security controls, and by documenting findings in the security assessment report. Create draft approval package.	Conduct RMF Steps 3 and 4 by applying controls identified during the requirements and design phase, by assessing the adequacy and effectiveness of security controls, and by documenting findings in the security assessment report. Create draft approval package.	12 – 20 weeks

Activity / Lead	**New Project**	**Renovation Project**	**Typical Duration**
• Security Incident Response Procedures (SIRP) • Penetration Testing Scope, ROE, Checklist (if required) • Jump-Kit Rescue CD			
Conduct testing on initial build Lead: construction/system integrator Documents/Models/Tools: • Kali Linux • SamuraiSTFU	Test FRCS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	Test FRCS solution in a test and development environment to ensure system errors are found, corrected before solution is deployed on network.	2 – 4 weeks
Construction - conduct pilot implementation deployment Lead: construction/system integrator Documents/Models/Tools: • Kali Linux • SamuraiSTFU • OIT IT Repository • Penetration Testing Scope, ROE, Checklist (if required) • Jump-Kit Rescue CD	Pilot implementation of FRCS solution on a small subset of user base to evaluate solution against real-world requirements. Conduct site acceptance testing, and if required final penetration testing, and create final approval package.	Conduct site acceptance testing, and if required final penetration testing, and create final approval package.	Varies with size of deployment (number of facilities and interconnections)
Receive Authorization (ATO) and move to production Lead: construction/system integrator Documents/Models/Tools: • OIT IT Repository • Continuous Monitoring tools • Jump-Kit Rescue CD	Deploy the FRCS to full production and implement continuous monitoring.	Deploy the FRCS to full production and extend continuous monitoring to new systems.	NA

CHAPTER 4. TYPICAL FACILITY-RELATED CONTROL SYSTEMS CONTRACT SUBMITTALS

This chapter provides guidance and the engineering requirements to the designers, construction and systems integrators to cover the lifecycle of the FRCS Cybersecurity process.

At contract award, all FRCS contractors must complete or have current DOD Cybersecurity Awareness training and have a security background clearance or similar e.g. Facility Access Determination – FAD (SECNAV M-5510.30).

FRCS contractors cannot use non-approved laptops/ computer and external portable media storage devices on the DoD network; only FRCS/ UCS/ BCS/ DDC government-approved field laptop and portable media will be used for both the Test and Development Environment and the Production system.

All FRCS construction and building modifications must meet the requirements of the local Building Standards Code, National Fire Protection Association (NFPA) 101, and Life Safety Code such as DDC raceway penetrations of fire wall boundaries.

While no FRCS can be guaranteed to continue to function and operate when a determined advisory has targeted the FRCS, the ability to withstand cyberwar attacks, even if in a degraded state, is a key consideration, particularly for Mission Critical and Mission Essential facilities. Contractors should design, construct, and operate the FRCS in accordance with the USCYBERCOM Industrial Control Systems Advanced Techniques, Tactics, and Procedures 2016. Understanding how to Detect, Mitigate, and Recover from a cyberattack on the CS is vital; the Jump-Kit Rescue CD is a key deliverable that defines the Fully-Mission Capable (FMC) Baseline and is the living document that maintains the current FRCS configurations and operating parameters. USCYBERCOM, the Network Security Operations Center (NOSC), and the services Facilities-Related Control Systems Operations Center (FRCSOC) use the FMC to develop and manage the Continuous Monitoring strategy.

4.1 FRCS IA SUBMITALL REQUIREMENTS

Configure all installed hardware and software to comply with DOD cyber security requirements that will be needed for Risk Management Framework (RMF) certification in accordance with DoDI 8510.1 with all applicable DISA STIGs applied.

Provide all necessary documentation for system RMF certification and accreditation to include all relevant artifacts for installed equipment (hardware and software). Documentation should include the following.

- Hardware and Software (both OS and Applications) STIG
- Provide ACAS (Nessus) and/or Security Content Automation Protocol (SCAP) scans of installed and configured systems to demonstrate DOD cyber security compliance.
- Identify and close/mitigate category 1 & 2 findings
- System/Mission Description/CONOPS/COOP
- Actual or intended installation platform/location(s)
- Hardware and Software lists if selected, including list of IA managed or IA enabled devices, if any
- Topology/architecture/boundary diagram that identifies major component(s) and all interconnections.

- Current life cycle status (acquisition milestone or fielded).
- Identification of the Platform IT Infrastructure (PITI) on the boundary diagram with sufficient detail for Office of Designated Approving Authority (ODAA) to determine accreditation status of PITI.
- Include Ports/Protocols/Services in accordance with DoD PPS CAL.
- Identify interfaces that cross differing security domains.

Provide all technical documentation including as built drawings, software and hardware inventory, standard operating procedures as well as cabling diagrams.

Project reports including system status, problem resolution, unresolved system problems, patch and updates Cybersecurity Vulnerability Management (IAVM) compliance.

4.1.1 Security Controls Documents

The Security Controls Documents document the engineering requirements for the FRCS/ UCS/BCS/ DDC Hardware, Software/Firmware; the Platform Enclave and network topology; Operating System Software and multicast filtering, port configuration, status, statistics, mirroring, and security for reliability and redundancy; Field Control Systems software/firmware; and the various plans required as artifacts for the eMASS RMF ATO Package.

As part of the Design Development (35-50%) and Final (100%) design submittal, provide the following document deliverables:

System Authorization Documents

- Draft hardware list (Hardware list must include the following for each device):
  - Manufacturer,
  - Model,
  - Location,
  - Server and Workstation technical ratings (e.g. memory),
  - Serial number,
  - MAC addresses,
  - IP addresses.
- Software and Firmware List (list must include the following for each device):
  - Manufacturer
  - Version/subversion,
  - Location/device,
  - Used network ports/protocols/services.

(Both hardware and software/firmware lists should also include Common Criteria EAL status, eMASS entry number, and OS/IOS/Firmware version(s) as applicable).

- Network diagram
  - Network diagram must show equipment locations, names, models, and IP addresses on network communications schematic.
- Jump-Kit Rescue CD (if required)

- The Rescue CD is a bootable CD with tools, rootkit detection, master boot record check, and other capabilities. A Recovery Jump-Kit contains the tools the CS team and IT team will need to restore a system to its last FMC state during Mitigation and Recovery. The Jump-Kits must be maintained and be a part of configuration management. When configuration files or new versions ofoperating systems or applications are updated, the Jump-Kits need to be updated as well.

Access Controls Summary

- Information on software access controls, port control, and protection.
- System user roles implemented by application and access privileges assigned by default to each role. If privileges can be added to, or removed from, a role, so specify.
- Details on system logon, including denial after three (3) invalid attempts, how to delay subsequent logons.
- Details on privileged accounts - who should have them and when are they used.
- Details on kinds of accounts, their associated privileges, which roles should have access, and so on - servers, wireless, equipment, meters.
- User ID/Password requirements and/or PKI requirements including details on shadowing, enforcement of password strength, encryption of passwords.
- Details of system library structure and what roles should be allowed what access privileges to library components.
- Details on remote (wireless) access by laptops or servers to meter and/or radio data. Auditing Controls Summary
- Details on auditing controls and auditing (creation of system audit trail for user accountability).

COOP or Disaster Preparedness Plan

- Contractor will work with government personnel to develop COOP and Disaster Preparedness Plan for the updated system (applications and hardware)

Configuration Management Plan

- The Fully-Mission Capable (FMC) Baseline Configuration, to be included on the Jump-Kit Rescue CD.

Vendor Configuration Management Plan

- Information required to test all patches and upgrades prior to deployment, including coordination as required with any test procedures run at vendor labs.

Contingency Plan

- Restoration Procedures – Guidance on restoring vendor software & hardware including guidance to help determine priority for restoration.
- Startup & Shutdown Procedures – Details of system initialization, shutdown/aborts designed to ensure secure system state.

Security Features Guide List and discussion of all security features of Vendor hardware and software.

- Document use of mobile code (e.g. scripts, such as Java) and protections in place to prevent malicious content from using associated runtime systems.
- Documented FIPS 140-2 validated cryptography (or equivalent) compliance.

Vulnerability Management Plan

- Information required to test all patches and upgrades prior to deployment, including coordination as required with any test procedures run at vendor labs.
- Security issues associated with implementation and maintenance of the application.
- Cybersecurity POC for resolution of Cybersecurity issues post accreditation.

Maintenance Plan

- Names and other required information of personnel who will be authorized to perform maintenance in accordance with maintenance agreement

Documented Statements

- Declaration that public domain software (e.g., freeware, shareware) is not used in the system.
- Information on Common Criteria or National Cybersecurity Partnership (NIAP) or Federal Information Processing Standards (FIPS) evaluation status of hardware and software.

Include the following documents:

- As-built System Accreditation Documents (Security Controls documents, along with as-built drawings submittals). Follow requirements for as-built drawings submittal format, and additionally provide hardware and software lists in Microsoft Excel 2010 or .cvs format and the network diagram in editable AutoCAD 2010 format.
- Download the FAT and SAT Checklist from the ESTCP website, and annotate with information required by the checklist, as well as the date and name of the government representative who witnessed validation of each item. (Demonstrate to the satisfaction of the government that system components are in compliance with the FAT and SAT Checklist and Security Controls documentation prior to commissioning. Facilitate government testing of the system via network scans and Security Template Implementation Guide (STIG) testing, and provide support for interpreting scan and STIG test results as needed).

4.1 FRCS FRONT END INTEGRATION is the portion of the control system consisting primarily of IT equipment, such as computers and related equipment, intended to perform operational functions and run monitoring and control/engineering tool application software. The front end does not directly control physical systems; it interacts with them only through field control systems (FCS). The following UFC's and UFGS's provide detailed design guidance for the FRCS:

- UFC 3-410-01 Utility Monitoring And Control System (CS) Front End And Integration 2016 (DRAFT)
- UFC 3-410-02 Direct Digital Control For HVAC And Other Building Control Systems 2016 (DRAFT)
- UFGS 23 09 00 Instrumentation and Control for HVAC (available online at www.wbdg.org)
- UFGS 23 09 23.01 LonWorks® Direct Digital Control for HVAC and Other Building Systems (available online at www.wbdg.org)

- UFGS 23 09 23.02 BACnet Direct Digital Control for HVAC andOther Building Systems (available online at www.wbdg.org)
- UFGS 25 10 10 Utility Monitoring And Control System (CS) Front End And Integration (available online at www.wbdg.org)

NOTE: A major objective of the IA process is to obtain a Type Authorization for the FRCS and use Reciprocity to extend the ATO to other similar FRCS that will be added to the service/agency PE.

4.1.1 FRCS Front End System Elements and Features

- CS Compatibility: All components of the FRCS shall be fully compatible and shall not require the addition of interface equipment or software upgrades to ensure a fully operational system.
- CS System Integration: The FRCS shall be fully integrated with other FRCS subsystems and the Level 4 DMZ firewalls.

4.2 **FRCS CABLING** is the physical transport layer of the FRCS to include the IP, Ethernet and serial communication. Cabling can be legacy CAT-5, RS232, RS465 or can be next generation fiber Passive Optical Networks (PONs), or can be a combination of both. Refer to the Telecommunications and Network Engineering Requirements for more detailed guidance.

4.3 **FRCS WIRELESS** is currently a challenging area where ESTCP projects may provide insight into many aspects of best practices for wireless deployment and operation. Commercial wireless products are expanding rapidly to include 802.XX, HART, Bluetooth, and ZigBee and DoD will need to plan for and eventually incorporate these devices and protocols into the DoDIN or CS networks. If the ESTCP Project Team intends to use wireless products and devices, coordinate with the ESTCP PM ASAP to ensure the CIO, Spectrum Manager, and host PE will be prepared to support.