ERDC/CERL SR-22- 1

US Army Corps
of Engineers®
Engineer Research and
Development Center

Installation Utility Monitoring and Control System Technical Guide

Joseph Bush, Eileen Westervelt, Brian Clark, David Schwenk,
Stephen Briggs, Daniel Shepard, M. Cary Long, Tapan Patel,
Melanie Johnson, and Eric Lynch

August 2022

Construction Engineering
Research Laboratory

Building Energy System Team

ERDC/CERL SR-22- 1
August 2022

Installation Utility Monitoring and Control System Technical Guide

Joseph Bush, Eileen Westervelt, Brian Clark, Daniel Shepard, Tapan Patel, and Melanie Johnson

US Army Engineer Research and Development Center
Construction Engineering Research Laboratory
2902 Newmark Drive
Champaign, IL 61822

Stephen Briggs

Facility Dynamics Engineering
6760 Alexander Bell Drive, Suite 200
Columbia, MD 21046

David Schwenk

US Army Engineer Research and Development Center
Construction Engineering Research Laboratory
Oak Ridge Institute for Science and Education Research Participation Program at ERDC-CERL
2902 Newmark Drive
Champaign, IL 61821

M. Cary Long

US Army Corps of Engineers
Control System Cybersecurity Mandatory Center of Expertise
475 Quality Circle NW
Huntsville, Alabama 35806

Eric Lynch

US Army Corps of Engineers
UMCS Mandatory Center of Expertise
475 Quality Circle NW
Huntsville, Alabama 35806

Final Report

Prepared for Headquarters, US Army Corps of Engineers
Standards and Criteria Program
Washington, DC 20314-1000

Under Project 19A01

And

Prepared for Headquarters, Department of the Army, Deputy Chief of Staff Army, G-9
Army Installation Technology Transition Program (ITTP)
Washington, DC

Under FY18 ITTP Program, MIPR 11268080

Abstract

Army policy calls for each installation to install a building automation system (aka utility monitoring and control system [UMCS]) to provide for centralized monitoring of buildings and utilities to reduce energy and water commodity and maintenance costs.

Typically, the UMCS, including building control systems (BCS), is installed and expanded in piecemeal fashion resulting in intersystem incompatibilities. The integration of multivendor BCSs into a single basewide UMCS, and subsequent UMCS operation, can present technical and administrative challenges due to its complexity and cybersecurity requirements.

Open Control Systems technology and open communications protocols, including BACnet, LonWorks, and Niagara Framework, help overcome technical incompatibilities. Additional practical considerations include funding, control systems commissioning, staffing, training, and the need for a commitment to proper operation, use, and sustainment of the UMCS.

This document provides guidance to Army installations to help achieve a successful basewide UMCS through its full life cycle based on DoD criteria and technical requirements for Open Control Systems and cybersecurity. It includes institutional knowledge on technical solutions and business processes amassed from decades of collaboration with Army installations and learned from and with their staff. Detailed activities spanning both implementation and sustainment include planning, procurement, installation, integration, cybersecurity authorization, and ongoing management.

Contents

Figures and Tables

Figures

Tables

Preface

This guide was prepared under the Installation Technology Transition Program (ITTP) under MIPR 11268080 for Headquarters, Department of the Army, Deputy Chief of Staff Army, G-9 (HQDA-DSC-G-9) and under the Specification and Criteria Program under Project 19A01 for United States Army Corps of Engineers, Headquarters' (HQ-USACE). The technical proponents were the ITTP Technology Standards Group: Ms. Svetlana O'Malley, chair, Ms. Laura Vaglia, and Mr. Yamil Hernandez, HQDA-DSC-G-9; Mr. Eric Mucklow and Mr. Jansen Moon, HQ-USACE; and Mr. Steve Tallman, Mr. Ernesto Ortiz, and Mr. Ryan Hernandez, HQ-IMCOM.

The work was managed and executed by the Energy Branch of the Facilities Division, Construction Engineering Research Laboratory. At the time of publication, Jedediah Alvey was chief of the Energy Branch, and Timothy Shelton was chief of the Facilities Division. The US Army Corps of Engineers agencies involved in the execution of this work include the Engineer Research Development Center, Construction Engineering Research Laboratory (ERDC-CERL) and Huntsville Engineering and Support Center Mandatory Center of Expertise for Utility Monitoring Control Systems. Personnel from Fort Hood, TX; Fort Bragg, NC; Fort Leonard Wood, MO; Presidio of Monterey, CA; Ft. Knox, KY; Ft. Leavenworth, KS; and other Army installations provided valuable input. This research was supported, in part, by an appointment to the Research Participation Program at ERDC-CERL administered by the Oak Ridge Institute for Science and Education through an interagency agreement between the US Department of Energy and ERDC. The deputy director of ERDC-CERL is Ms. Michelle Hansen. The director of ERDC-CERL is Dr. Andrew Nelson.

The commander of ERDC is COL Christian Patterson, and the director of ERDC is Dr. David Pittman.

Portions of this guide modify and reprint portions of previous CERL technical reports (TRs),[1] the Tri-Services' Unified Facility Criteria (UFC), Unified Facilities Guide Specifications (UFGS),[2] Federal Information Pro-

[1] Available at the Engineer Research Development Center (ERDC) library at https://www.erdc.usace.army.mil/Library/ and the Defense Technical Information Center, https://discover.dtic.mil

[2] UFCs and UFGS are available at the Whole Building Design Guide, **https://wbdg.org**

cessing Standards (FIPS), Committee on National Security Systems Instructions (CNSSI), and DoD Instructions. All of these documents are in the public domain. Many of authors of this current work are also authors of these previous works.

Brian Clark, Matt M. Swanson, Sean M. Wallace, Eileen T. Westervelt, and Jay H. Tulley, 2018, *Army RCx Technical Guide: A Phased Approach for In-House or Contracted Existing Building Commissioning*, ERDC/CERL SR-18-1 (Champaign, IL: Engineer Research Development Center, Construction Engineering Research Laboratory).

Committee on National Security Systems (CNSS), 2009, *Security Categorization and Control Selection for National Security Systems*, CNSS Instruction 1253, (Washington, DC: National Security Agency).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2015a, *Instrumentation and Control Devices for HVAC*, UFGS 23 09 13 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2015c, *Sequences of Operation for HVAC Control*, UFGS 23 09 93 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)], 2017a, *Cybersecurity of Facility-Related Control Systems*, UFC 4-010-06, Change 1, effective 18 January 2017 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2017b, *Cybersecurity for Facility-Related Control Systems*, UFGS 25 05 11 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)], 2018a, *Direct Digital Control for HVAC and Other Building Control Systems*, UFC 3-410-02 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)], 2018b, *Utility Monitoring and Control System (UMCS) Front End and Integration*, UFC 3-470-01 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2019a, *BACnet Direct Digital Control for HVAC and Other Local Controls*, UFGS 23 09 23.02 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)], 2019b, *Engine-Driven Generator System for Prime and Standby Power Applications*, UFC 3-540-01, Change 2, effective 5 November 2019 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)], 2019c, *High Performance and Sustainable Building Requirements*, UFC 1-200-02, Change 04, effective 01 October 2019 (Washington, DC: Department of Defense).

Department of Defense (DoD), 2020, *Operation of the Adaptive Acquisition Framework*, DoD Instruction 5000.02 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2019d, *Instrumentation and Control for HVAC* UFGS 23 09 00, Change 1, effective November 2019 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2019e, *LonWorks Direct Digital Control for HVAC and Other Local Controls*, UFGS 23 09 23.01 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2019g, *Utility Monitoring* *and Control System (UMCS) Front End and Integration*, UFGS 25 10 10 (Washington, DC: Department of Defense).

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)], 2020a, *Risk Management Framework for Facility-Related Control Systems*, UFGS 25 08 11.00 20 (Washington, DC: Department of Defense).

Michael Cary Long, Joseph Bush, Steven Briggs, Tapan Patel, Eileen Westervelt, Daniel Shepard, Eric Lynch, and David Schwenk, 2019, A*rmy Guide to Navigating the Cybersecurity Process for Facility Related Control Systems: Cybersecurity and Risk Management Framework Explanations for the Real World*, ERDC-CERL SR 19-5 (Champaign, IL: Engineer Research Development Center, Construction Engineering Research Laboratory).

David M. Schwenk, Joseph Bush, and David M. Underwood. *Heating, Ventilating, and Air-Conditioning (HVAC) Control Systems Operations and Maintenance at Fort Bragg, NC: Training and Technical Assistance*, 2005, ERDC/CERL TR-05-14 (Champaign, IL: Engineer Research Development Center, Construction Engineering Research Laboratory).

David M. Schwenk, Joseph Bush, Lucie M. Hughes, Stephen Briggs, and Will White, 2008, *IMCOM LonWorks Building Automation Systems Implementation Strategy*, ERDC/CERL TR-08-12 (Champaign, IL: Engineer Research Development Center, Construction Engineering Research Laboratory).

David M. Schwenk, David Underwood, Joseph Bush, Brian Clark, Tapan Patel, Annette L. Stumpf, and Susan J. Bevelheimer, 2017, *Utility Monitoring and Control System (UMCS) and Utility Metering Plan and Specifications for Fort Leonard Wood, MO*, ERDC/CERL TR-17-15 (Champaign, IL: Engineer Research Development Center, Construction Engineering Research Laboratory).

Daniel A. Shepard, Joseph Bush, Eric Lynch, Alan Schuld, Andrew Spear, Fred Abbitt, Dahtzen Chu, 2018, *Facility Related Control Systems (FRCS) Architecture Report*, CEHNC-TR 18-01 (Champaign, IL: Engineer Research Development Center, Construction Engineering Research Laboratory).

1 Introduction

1.1 Background

1.1.1 Policy

A recent memorandum, *Army Policy on Building Automation Systems* (see Appendix B), issued 28 October 2020 by the Assistant Secretary of the Army (Installations, Energy and Environment) (ASA [IE&E]) calls for each Army installation to install a building automation system, referred to in the DoD criteria as a utility monitoring and control system (UMCS), to provide for centralized monitoring as a way to reduce energy and water commodity and maintenance costs in cost-effective applications.

In the summer of 2021, a new centralized Army Control System Governance Office was initiated with Deputy Chief of Staff (DCS), G-9, Installations as the lead. In the same timeframe, G-9 issued the *Department of the Army Guidance for Implementation of a Building Automation System (BAS)*, 25 August 2021, which provides technical direction for Army stakeholders at multiple organizational levels.

This new guidance sets out to fill many gaps in status quo facility-related control system (FRCS) utilization that have historically prevented optimal building operations. The implementation guidance establishes roles and responsibilities to effect widespread adoption of basewide networks of building controls in support of Army Installation Strategy objectives by engaging ASA (IE&E), DCS, G-9, Major Commands (MACOMS),[3] as well as individual Army installations with planning, budgeting, resourcing, execution, and ongoing evaluation. It calls for establishing roles (with associated training and funding) and regular reporting and accountability. It directs integration of building control systems (BCSs) into UMCS front ends in military construction (MILCON) as well as in applicable renovations of buildings (typically greater than 25K ft^2 or energy intensive facilities). It recommends the establishment of life-cycle cost estimates that include ongoing operations and maintenance and Risk Management Framework (RMF) accreditation and also calls for the inclusion of nonenergy benefits (such as productivity gains and maintenance reductions) in life-cycle cost

[3] Army Material Command (AMC) (including Installation Management Command [IMCOM]), Army Reserves (AR), Army National Guard (ANG)

analysis (LCCA). It mandates the use of the Unified Facilities Criteria (UFC) (unless waived) and encourages the use of the Unified Facilities Guide Specifications (UFGS) for all UMCS construction efforts, including new and existing building construction. Additionally, it provides guidance on network planning and architecture, control system design, and cybersecurity requirements necessary for project implementation. If the rigorous enforcement of these policies takes place, this will significantly change the composition of the UMCS landscape for the better.

1.1.2 Installation practices

Army installations make extensive use of BCS[4] ordinarily consisting of direct digital control (DDC) hardware. Most often this includes control of heating, ventilating, and air-conditioning (HVAC) systems and equipment, including central plants, but can include other mechanical and electrical building systems, notably lighting control systems and energy metering of utilities. These building control systems are then connected (often along with utility control systems) through the installation computer network to a central monitoring and control (M&C) front end to create a utility monitoring and control system (UMCS) (See Figure 1).

Army BCSs are usually installed, expanded, or replaced on a building-by-building or system-by-system basis under separate contracts by different contractors using multiple vendors’ hardware and software, which often results in incompatibilities between systems. To be successful, these systems must be installed with proper planning, preparation, training, and ground rules.

The implementation of multivendor BCSs presents both technical and administrative (primarily contracting) challenges. For example, each BCS, including expansions and replacements, needs to interoperate as part of a UMCS supervisory front-end server and workstations as illustrated in Figure 1.

While a BCS can function independently, or standalone, the UMCS front end provides important supervisory functionality, particularly when there are a multitude of BCSs that need to be monitored and managed. UMCS supervisory functionality typically consists of turning equipment on or off

[4] BCS and DDC are related terms. BCS refers to a control system that resides hierarchically at the building level, while DDC refers to a type of control hardware (microprocessor based) that performs control logic using directly sensed values and directly operating an output device.

according to a schedule, monitoring the systems for problems (e.g., receiving alarms), collection of historical data for analysis, remote viewing, and diagnosis of problems.

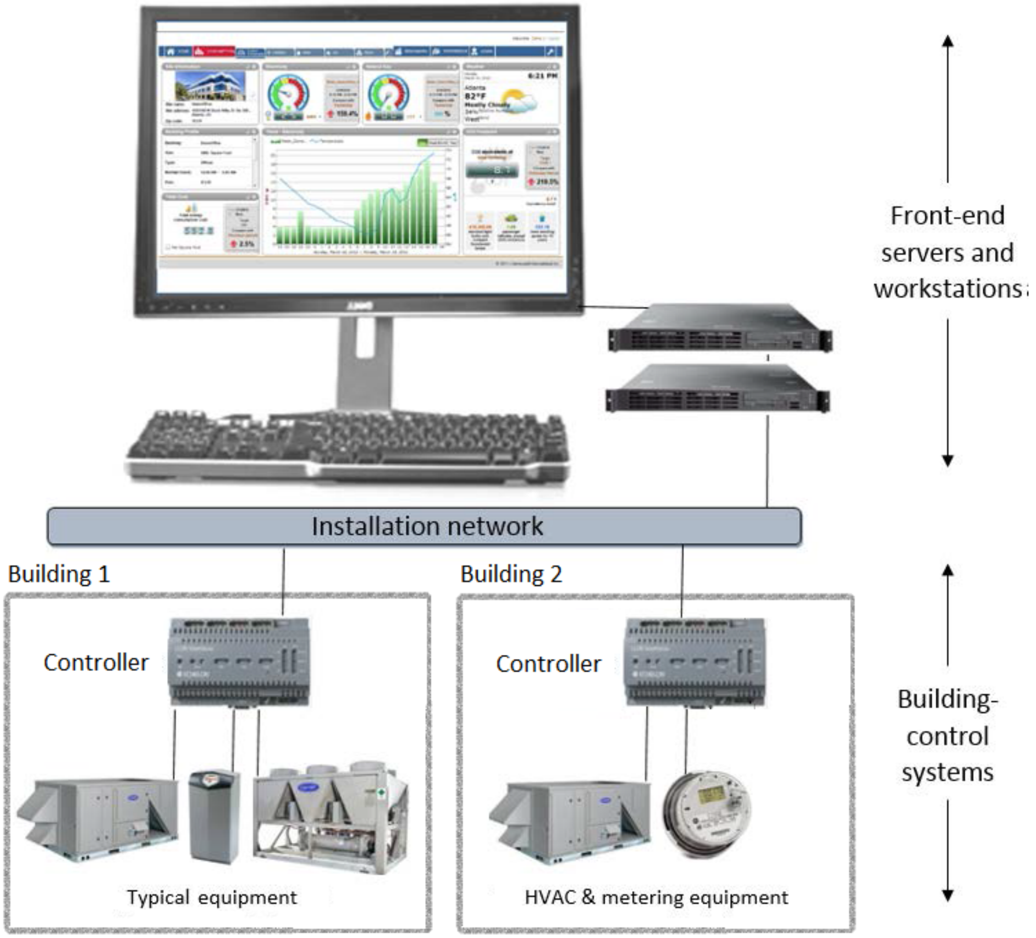
1.1.3 Open Control System protocols and technologies

A longstanding goal of most Army installations is to implement a ***single basewide*** UMCS with a single user interface as opposed to multiple separate and independent UMCSs. This goal supports the current Army Installations Strategy, December 2020, that envisions each installation employing a common operating picture of its operational environment to guide decision making and resource allocation (Department of Army 2020).

Congress recognized the challenge of interconnecting a multiplicity of facility-related control systems, and in H. R. 2647, the National Defense Authorization Act of 2010 (NDAA 2010) (see Appendix A) added 10 US Code § 2867, which requires the "adoption of an open protocol[5] energy monitoring and utility control system specification" throughout the DoD as part of military construction and related projects for installation-wide energy monitoring and utility control systems. The H.R. 2647 requirement included HVAC, lighting, utilities, metering, central plants, renewable energy, and power distribution systems. Current DoD design and specification criteria for UMCS, including BCSs, are a byproduct of this legislation. The full text of the H.R. 2647 legislation is in Appendix A.

[5] A (communications) protocol is a set of rules that defines how data are transmitted between pieces of equipment. *open* means it is published and available for any/all equipment manufacturers to use.

Figure 1. Example UMCS with front end and interconnected building control systems.



A single communications protocol that crossed all the industries and technologies listed in the H.R. 2647 was not available, and to this day, there still is not one. Therefore, it was impractical for the DoD to define a single protocol, so the DoD focused its specification development effort on the most accepted open protocols and technologies that were available, which has evolved over time to include Building Automation Control Network (BACnet), LonWorks, Modbus, Distributed Network Protocol (DNP), Niagara Framework, and Open Platform Communications (OPC).

Plus, the DoD interpreted the open protocol requirement in 10 US Code § 2867 to require Open Control Systems to help avoid the underlying issue of proprietary sole-source procurement. Sole source contracts are very difficult if not impossible to justify under Government procurement rules. This document uses Open Control Systems as a very specific technical term to safeguard the interest of the Government. To highlight this unique meaning, the name of the open system process is capitalized in this guide.

In short, for the Government, an Open Control Systems is one that does not require any future dependence on any original installing contractor for future system additions, upgrades, or modifications. Use of an industry-standard open protocol is necessary but not sufficient for implementation of an Open Control System; other details such as protocol options and extensions, and software licensing and submittals must be specified to achieve a truly open system. These particulars are addressed and included in the DoD published construction criteria and specifications (UFCs and UFGSs) and are also discussed, as applicable, in this technical guide.

Achieving a single, basewide, open UMCS, while challenging, has become more practical in recent years due to the maturing of Open Control Systems standards and technology, coupled with DoD design and specification criteria described in Section 3.3 of this technical guide.

Implementation of the DoD standards and criteria at Army installations is described in this guide with the intent to help plan, obtain, and sustain open but secure, nonproprietary, interoperable, multivendor BCSs that integrate with UMCS front-end servers or workstations. Even if the installation already has a UMCS, this guide can help with its sustainment.

1.2 Objectives

The objective of this work was to define and document an implementation approach that will serve as a detailed guide to help plan, procure, authorize, manage, and sustain UMCS hardware, software, and processes at Army installations based on current DoD Open Control Systems criteria, cybersecurity criteria, and technical requirements.

1.3 Approach

DoD specifications and criteria along with Army policies related to UMCS were reviewed. ERDC-CERL TR-08-12, *IMCOM LonWorks Building Automation Systems Implementation Strategy*, was also reviewed and used as a starting point of content for this technical guide (Schwenk et al. 2008). This 2008 technical report was then updated and expanded to incorporate current guidance, currently supported controls protocols, current roles and processes in the Army, and the RMF cybersecurity requirements. Additionally, institutional knowledge on technical solutions and business processes amassed from decades of collaboration with Army installations and learned from and with their staff was incorporated as insights and recommendations of best practice.

1.4 Scope

This document provides technical guidance for an installation-specific, basewide UMCS based on Open Control Systems technology adopted by the DoD. It addresses the full life cycle of the UMCS: definition, specification, procurement, installation, integration, use, and sustainment. The focus is on the UMCS, including the front end and commercial-grade building control systems connected to the front end. It does not address industrial-grade utility control systems. Limited guidance on the implementation of the connected building control systems is included. Building control system content focuses on those requirements and considerations that deal with system interoperability with the UMCS front end, overall system functionality, and maintainability. The scope of this document is based on DoD UFGS and UFCs containing the following Open Control Systems technologies: LonWorks , BACnet, and the Niagara Framework. While the content of this technical guide is Army specific, it may be generally applicable to a UMCS based on other technologies or protocols and be suitable for use by other DoD and non-DoD users.

This work complements the *Department of the Army Guidance for Implementation of a Building Automation System (BAS)* (see Section 1.1), which addresses multiple echelons of Army installation management and sets out *strategic level* requirements and methods for funding, planning, LCCA, cybersecurity, and sustainment (including Program Objective Memorandum [POM]). This document targets the Army installation energy manager at the *tactical level* and lays out the technical requirements and system implementation details.

1.5 Mode of technology transfer

This report will be made accessible through the Engineer Research Development Center (ERDC) library at https://www.erdc.usace.army.mil/Library/.

Content from this report has been incorporated into USACE Learning Center Proponent Sponsored Training (PROSPECT) courses including HVAC Control Systems: Design-Quality Verification (Course 340), HVAC Systems Commissioning (Course 327), and HVAC Testing and Balancing Quality Verification (Course 068) as well as IMCOM's Retrocommissioning (RCx) Academy training.

Much of the underlying technical content of this report is available as design and specification criteria in the form of DoD Unified Facilities Guide Specifications (UFGS) and Unified Facilities Criteria (UFCs) listed in Section 3.3, the bibliography, and available at the Whole Building Design Guide, https://wbdg.org.

“WAR STORY”

This technical guide contains “War Stories” that appear in a box like this one. The intent is to share learning experiences.

2 UMCS Overview

2.1 Basically . . . What is a UMCS?

A utility monitoring and control system, or UMCS, provides real-time monitoring and control of mechanical and electrical systems. A basic UMCS is illustrated in Figure 1.

UMCS is the DoD term (defined in DoD Unified Criteria and Guide Specifications) for both the supervisory front end (typically consisting of a server plus operator workstations) *and* the field control systems connected to the front end. In other words, the UMCS is a complete system from the front end down to the equipment controllers. It is important to note that industry (and sometimes those in Government) refer to UMCS technology by different names.[6]

The UMCS front end provides a user interface (with graphic displays) and typically includes both monitoring and control functions. The user interface provides for data-driven decisions by operators and management, notification of alarms when systems or equipment malfunction, remote operator response to system and equipment problems, energy and performance reports, and fine tuning of equipment settings to reap energy savings. Connected systems and equipment can include HVAC, lighting, chillers, boilers, solar heating, energy meters (for electric, gas, and water), electrical switchgear and substations, power generators, lift stations, etc. Note that some systems, such as a utility control system (described later) may have limited or no control capability from the front end.

While the UMCS is intended to be a basewide system (in the case of HVAC and other commercial control systems, such as lighting and metering) it may initially consist of very few, or even only one, control system in a single building. Using the Open Control Systems technology described in this technical guide, the UMCS can be expanded to include additional control systems from different contractors and with different vendors/brands of

[6] Some names that may be used to mean UMCS are building automation system (BAS), supervisory control and data acquisition (SCADA), building automation and control systems (BACS), building management system (BMS), building energy management system (BEMS), energy monitoring and control systems (EMCS), energy management and utility control system (EMUCS), smart building management systems (SBMS), facility management system (FMS), and distributed control system (DCS).

controls. A single basewide UMCS is expected to include many control systems from multiple vendors, where the control systems are procured separately and then integrated into the UMCS front end.

Note that while the UMCS does not technically include the connected equipment (pumps, fans, circuit breakers, etc.) the usefulness of the UMCS depends critically on the proper functioning of the underlying equipment. UMCS technology is further described in Section 3.

2.2 Why do installations need a UMCS?

UMCS technology is the norm in both commercial multibuilding settings and at Army installations because of its capability to remotely monitor a building's mechanical and electrical systems and to perform supervisory control of the associated building control systems. This capability is beneficial if not necessary. A large Army post can have thousands of building control systems to manage, and they cannot be managed well without a common front end. The UMCS ties buildings together to provide coordinated supervisory functionality for day-to-day operations.

A UMCS front end can be used to monitor and help control the underlying HVAC mechanical systems[7] to

- Better maintain and troubleshoot systems. The UMCS front end can alert the first responder to system anomalies and thereby reduce site visit legwork. Using the UMCS as a window into an underlying mechanical system, a UMCS operator can assist O&M staff to troubleshoot and, in many cases, correct system issues without requiring intervention by a mechanic or technician. Consequently, UMCS operators and O&M staff have better-quality interactions, which allow each staff member to manage and maintain more buildings.
- Monitor operational parameters, like space temperatures, CO2 levels, static pressures, relative humidity levels, chilled water and airside supply and return temperatures, to fine tune system operation and optimize control sequences and setpoints to improve building and system performance.

[7] A UMCS can include other building control systems, such as electrical, metering, lighting and others. It may also include (at a more supervisory level) utility control systems. However, the typical UMCS tends to be in support of HVAC.

- Operate building systems in a cost-effective and efficient manner. This can include use of the UMCS front end to perform centralized scheduling of equipment to turn equipment and systems on or off, use energy optimization strategies, monitor the connected control systems for problems (e.g., transmit an alarm when there is an abnormal condition), and remote viewing and diagnosis of problems using graphic display screens and access to stored performance or trend data.
- Collect performance data and provide performance and energy reports to decision makers. A UMCS can provide valuable facility performance trend data to O&M and energy management staff for system discrepancy and optimization purposes. This can support installation resilience, reduce energy consumption and energy costs, and improve O&M processes and procedures.

Recognizing these multifold benefits, the Army has made UMCS a requirement through the previously mentioned policy, see Section 1.1.1.

2.3 What is success?

A vision for a successful UMCS is one that is established, fully functioning (i.e., *useful* and *used)*, and maintained and sustained:

- ***Established:*** An *established* UMCS consists of a front end with a sufficient number of BCSs connected to it to provide a significant O&M and energy management benefit.
- ***Fully Functioning:*** A fully functioning system is set up and working correctly—graphics accurately reflect the equipment and sequences of operation, alarms are appropriately set, trends and schedules are established, demand limiting is configured, the connected building control systems are functional, etc. Consulting the UMCS is the first step in troubleshooting controls or mechanical problems. The system is accessible and *useful* to the O&M staff and energy manager. The system is used to support all connected buildings, not just a small subset of them.
- ***Maintained and Sustained:*** The system is designed, installed, staffed, and supported such that it is sustained long term. This includes
    - Programming of maintenance, sustainment, and recapitalization cost for system components and network in addition to all cybersecurity requirements and should include those costs in the overall FRCS POM build,

  - Staffing for systems integration, maintenance, and use of the system (Be advised that the needed staffing levels are likely greater than what the installation might anticipate),
  - Coordinating specifications for the procurement of new BCS with in-house and Corps of Engineers designers,
  - Procuring and integrating new BCS into the UMCS,
  - Obtaining all necessary system certifications (e.g., cybersecurity) required to operate, and
  - Establishing IMCOM-level sustainment funding and support.

2.4 Challenges

UMCS implementation is not easy. The expansive technical, multidisciplinary, and sustainment aspects of a UMCS present multiple challenges with potential pitfalls and roadblocks. Many Army installations, DoD agencies, manufacturers, contractors, and technical experts have grappled with the challenges and helped pave the way to dealing with them. Still, each installation is likely to encounter its own unique set of challenges, so there is no single, easy clear-cut path to success, and the degree of difficulty of each challenge can vary from installation to installation.

The DoD design and specification guidance (primarily the UFCs and UFGSs) was crafted to address not only the technical challenges and pitfalls, but also the administrative and procurement aspects of UMCS technology. Still, it is important to realize that, while design is critical, implementation challenges extend beyond the designer's ordinary realm of responsibility and are, therefore, largely left to the individual installations. This guide is intended to help identify and address these challenges.

Some of the key challenges of UMCS implementation are

- ***Management and leadership.*** The installation needs someone (e.g., a UMCS manager, discussed later in Section 7.2) to lead and manage the UMCS effort. This responsibility is expected to lie at the installation's Directorate of Public Works (DPW) level and should include the creation of a UMCS workgroup.
- ***Master planning.*** The installation should develop and document (at least) a baseline UMCS master plan to map out a strategy to achieve success as described in Section 2.3 "What is success?" The plan should

be coordinated with all stake holders, notably the DPW and O&M staff as well as the designers and specifiers.

- ***Complex decisions.*** There are many technical questions that need to be answered for the overall system: What buildings and systems should be part of the UMCS initially and in the future? Which of the four Open Control Systems technology and protocol options (as outlined later in this guide and in the UFCs and UFGS) should the installation pursue? What functions do the DPW (and others) want the UMCS to perform? Who will be the UMCS front-end users and operators? What resources are available to help make technical selections and decisions? While DoD specifications and criteria exist to ensure an open and maintainable UMCS is delivered, implementing these criteria can be a challenge for Army designers, project office staff, and contractors unfamiliar with DoD requirements.
- ***Funding and staffing.*** Consideration needs to be given to how the UMCS will be staffed and paid for. A UMCS requires specialized staffing/roles and sustainment dollars as well as up-front costs to own and operate. Personnel constraints may require contract support to execute UMCS roles that are not inherently Governmental (e.g., Technicians, Programmers, and Integrator).
- ***Training and utilization.*** The UMCS must be actively used to troubleshoot, maintain, and improve facility operations. Generally, vendor-specific training, well-defined UMCS operator processes, and a regular program of maintenance are necessary to make the most of a UMCS and protect investments in UMCS infrastructure.
- ***Technology selection and support.*** Careful selection of manufacturer or brand of front-end M&C software needs to take place. This is an important consideration because (except for the Niagara Framework) the UMCS front-end software (e.g., the user interface software) will be procured from a single vendor, and the installation will use (and in the worst case “be stuck with”) this front end indefinitely. It must be decided if the installation should pursue the services of a UMCS front-end contractor to service the front end, including performing activities such as integration or connection of BCSs into the UMCS front end. Also important is determining who will manage day-to-day operation of the UMCS computer and servers, such as back-ups, security updates, etc.
- ***Cybersecurity.*** UMCS cybersecurity requirements must be addressed and will create additional burdens on the design and DPW staff in part because cybersecurity is often outside the working discipline of

UMCS implementers and owners. Resources are available for understanding and dealing with the Risk Management Framework (RMF) such as ERDC-CERL's SR19-5 *An Army Guide to Navigating the Cyber Security Process for Facility Related Control Systems* (Long et al, 2019), and Army staff at the Mandatory Center of Expertise (MCX) for cybersecurity at the U.S. Army Engineering and Support Center who specialize in RMF.

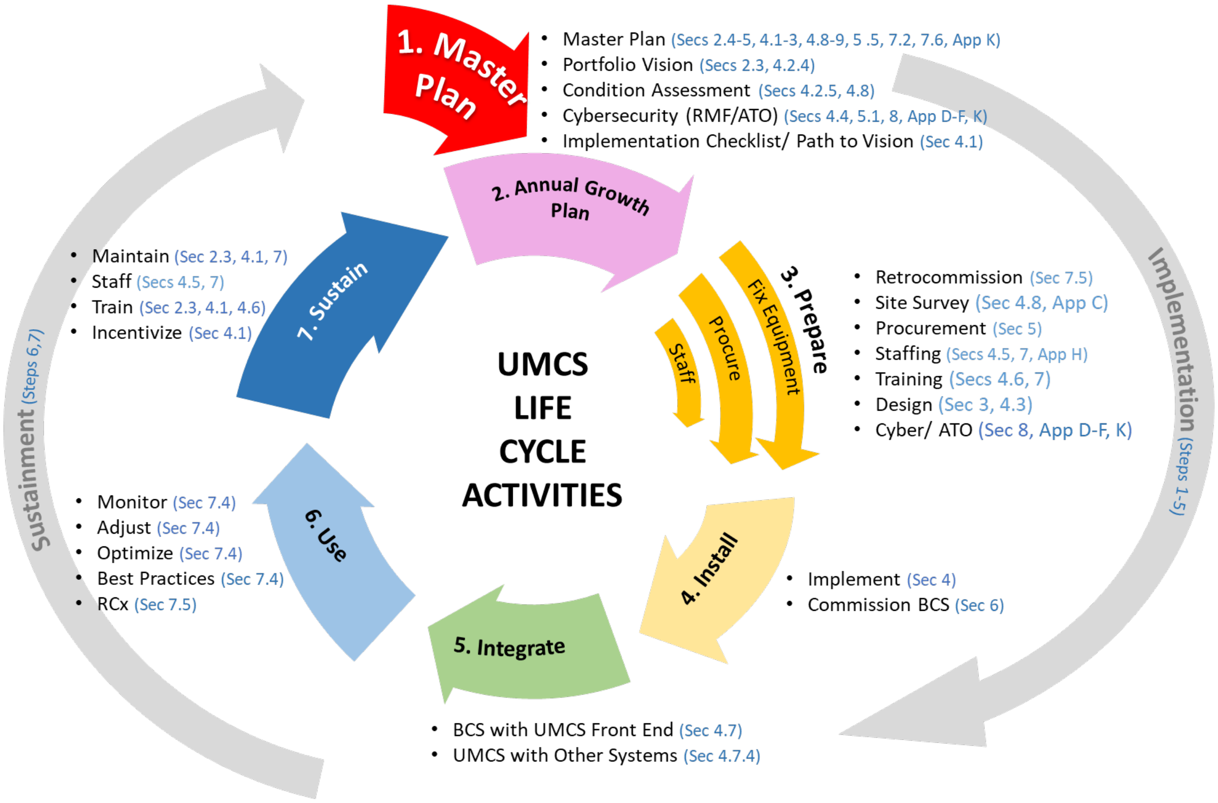
- ***Commissioning and O&M***. Government acceptance of systems and equipment that function properly and do not become a maintenance burden from day one is an ongoing challenge in the Army. Proper commissioning is intended to help alleviate this challenge. Inspections, testing, and acceptance of each BCS and the UMCS front end should be a routine part of the USACE's (in new construction) and the DPW's (in retrofit and local DPW construction) commissioning process. This is discussed in Section 6.
- ***Coordination and buy-in.*** The implementation of any impactful technology, especially UMCS based on DoD Open Control Systems technology, should be coordinated with affected stakeholders to gain buy-in. The stakeholders can include anyone involved in the UMCS life cycle, including designers, installers, administrators, managers, maintenance staff, and building occupants. Various aspects and phases of UMCS implementation are addressed to some degree in this guide, such as funding, staffing, training, best practices for UMCS related roles, design specifications and criteria, and commissioning[8].

2.5 UMCS life cycle

The life cycle of the UMCS can be divided into an implementation phase followed by a sustainment phase. Each phase can further be divided into steps. The implementation phase, covering steps 1–5, starts with a master plan, then proceeds to an annual plan, followed by necessary preparation, then installation and integration. The sustainment phase, covering steps 6 and 7, includes the ongoing use and maintenance activities. The sections of this guide that mention each step are tagged in the figure. (See Figure 2 below.)

[8] Additional insights on the human aspects of facility energy management are discussed in Westervelt et al., 2020, *Enhancing Army Energy Culture with Behavioral Approaches* (ERDC-CERL TR20-5)

Figure 2. UMCS life-cycle activities.


1. Master Plan
- Master Plan (Secs 2.4-5, 4.1-3, 4.8-9, 5 .5, 7.2, 7.6, App K)
- Portfolio Vision (Secs 2.3, 4.2.4)
- Condition Assessment (Secs 4.2.5, 4.8)
- Cybersecurity (RMF/ATO) (Secs 4.4, 5.1, 8, App D-F, K)
- Implementation Checklist/ Path to Vision (Sec 4.1)
2. Annual Growth Plan
3. Prepare
Fix Equipment
Procure
Staff
- Retrocommission (Sec 7.5)
- Site Survey (Sec 4.8, App C)
- Procurement (Sec 5)
- Staffing (Secs 4.5, 7, App H)
- Training (Secs 4.6, 7)
- Design (Sec 3, 4.3)
- Cyber/ ATO (Sec 8, App D-F, K)
4. Install
- Implement (Sec 4)
- Commission BCS (Sec 6)
5. Integrate
- BCS with UMCS Front End (Sec 4.7)
- UMCS with Other Systems (Sec 4.7.4)
6. Use
- Monitor (Sec 7.4)
- Adjust (Sec 7.4)
- Optimize (Sec 7.4)
- Best Practices (Sec 7.4)
- RCx (Sec 7.5)
7. Sustain
- Maintain (Sec 2.3, 4.1, 7)
- Staff (Secs 4.5, 7)
- Train (Sec 2.3, 4.1, 4.6)
- Incentivize (Sec 4.1)
UMCS LIFE CYCLE ACTIVITIES
Implementation (Steps 1-5)
Sustainment (Steps 6,7)

3 UMCS Technology Background

3.1 UMCS components

This section describes the parts and pieces of a UMCS and their basic functions and features.

A utility monitoring and control system, or **UMCS**, as first described in Section 2, is the DoD term for a supervisory front end *and* the field control systems connected to the front end. In other words, it is the complete utility monitoring system from the front end down to the equipment controllers. The connected systems and equipment can include HVAC, lighting, chillers, boilers, solar heating, energy meters (for electric, gas, water), electrical switchgear and substations, power generators, lift stations, etc.

Note that fire, life safety, and electronic security systems (ESS), due to their sensitive nature (e.g., life safety requirements), are generally not part of a UMCS (but likely have their own independent basewide system). Some life safety devices may provide a hardware-only interface (e.g., contact closure) between the UMCS and these systems, but despite that connection, these remain separate and distinct systems.

3.1.1 UMCS parts and pieces

Front End. The portion of the UMCS consisting primarily of computer-based servers that host the monitoring and control software (described below) to provide a full-featured user interface with the field control systems (e.g., BCSs). Ideally, the UMCS front-end server will reside in a Network Enterprise Center (NEC)-managed data center. Note that some vendors cannot implement all of the desired functionality in their standard front end or server-based software; therefore, some functionality—specifically point calculations and demand limiting—may be performed by controller hardware. The front end does not directly control physical systems; it interacts with them only through field control systems. A front end “workstation” is a desktop or laptop used to provide and support user interface functions. UFGS 25 10 10 contains specifications for front-end server hardware and client workstations.

M&C Software. The UMCS will have monitoring and control (M&C) software, which resides in the front end described above. The UMCS software must be programmed or configured to connect to field control systems (e.g., BCSs) in order to perform supervisory functions, such as alarm handling, scheduling, trending (data logging), electrical demand limiting, report generating; and to provide a user interface for monitoring the system and configuring these functions. M&C software is generally proprietary, although open access licensing is available with some technologies such as Niagara Framework (see Section 3.2.5he goal is to have a single front-end M&C software for the entire installation.

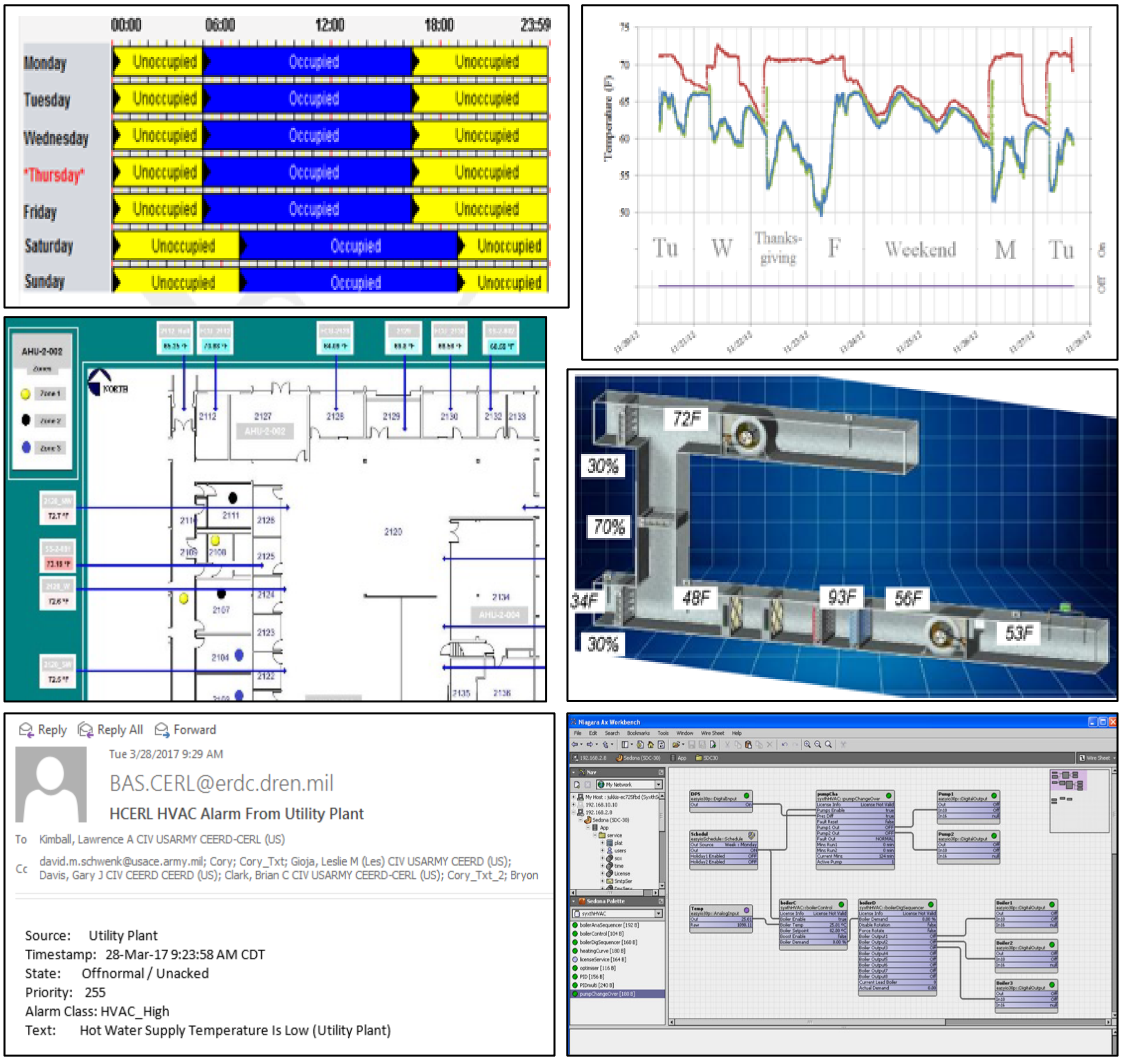
M&C software typically uses a client-server arrangement with web-browser-based clients and, therefore, functions as a multiuser interface. The M&C software, as defined and specified in UFGS 25 10 10, can provide user, operator, and management staff with supervisory monitoring and control functionality, such as

- A graphical user interface (GUI), as illustrated in Figure 3, provides for graphical navigation between systems (e.g., via floor plans), graphical representation of systems, access to real-time data for systems, ability to override points (e.g., setpoints, on and off of equipment, etc.) in a system, and access to all supervisory monitoring and control functions. For example, it can display BCS functions and processes, such as the on or off status of equipment, actual room temperatures, room temperature setpoints, etc. Note that the look and feel of the GUI will vary depending on both the manufacturer and developer of the M&C software and the contractor who installs and configures it.
- Remote access and diagnosis of problems, including analysis and improvement of systems performance for both occupant comfort and energy savings. A goal is to be proactive to optimize performance, with a secondary goal of using the GUI for forensic analysis.
- Systems/equipment scheduling to turn individual pieces of equipment or entire systems on or off. This is sometimes referred to as occupancy scheduling, and staff can configure scheduling to be performed on a 24-hour, 7-day-a-week (24/7), user-defined schedule. Special user-defined events and holidays can also be scheduled.
- Alarm transmission to staff, for example via email or text message, to provide notification of a BCS's problems, such as equipment not running when it should be, room temperatures out of range, etc. The M&C software allows staff to define, generate, handle, and route the alarms

and the ability to configure critical and informational alarm conditions and categories.

- Trending functionality to access and view data (such as room temperatures, equipment status, etc.), which is stored by the UMCS as trend data. Trend data can be displayed in a graph with multiple points or exported for use in another program, such as a spreadsheet. Staff can define which points to trend, how often, and the duration. Trending allows for the collection and storage of performance data (temperatures, equipment status, etc.) for viewing, diagnosis of problems, and analysis of performance, such as energy performance.
- Demand limiting functionality, where the UMCS can change the occupancy control mode (e.g., transition from occupied mode to unoccupied mode) of a system or adjust the setpoint of control system devices based on a projected limit to maintain electrical demand (kW) below a configured target. The UMCS can also help identify peak demand, real power, and other electrical performance parameters necessary for rightsizing generation assets and to help optimize design of microgrids supporting mission-critical building operations.
- Report generation, such as reports for energy, power usage, water usage, equipment usage and runtimes, alarms, etc.

Figure 3. UMCS M&C software GUI.



Reply Reply All Forward

Tue 3/28/2017 9:29 AM

BAS.CERL@erdc.dren.mil

HCERL HVAC Alarm From Utility Plant

To Kimball, Lawrence A CIV USARMY CEERD-CERL (US)

Cc david.m.schwenk@usace.army.mil; Cory; Cory_Txt; Gioja, Leslie M (Les) CIV USARMY CEERD (US); Davis, Gary J CIV CEERD CEERD (US); Clark, Brian C CIV USARMY CEERD-CERL (US); Cory_Txt_2; Bryon

Source: Utility Plant
Timestamp: 28-Mar-17 9:23:58 AM CDT
State: Offnormal / Unacked
Priority: 255
Alarm Class: HVAC_High
Text: Hot Water Supply Temperature Is Low (Utility Plant)

FCS. Field control system. FCSs may be located throughout an installation in various buildings and/or as part of remote pieces of equipment exterior to buildings. An FCS might operate the system or subsystem independent of the UMCS front end (i.e., standalone, as described later). There are two categories of FCS:

- **BCS.** Building control system. Generally considered commercial grade and is used for applications such as HVAC, central plants, lighting control, and energy metering. BCSs are emphasized and discussed in this guide more so than UCSs. BCS refers to a control system that resides hierarchically at the building-level where HVAC building control systems typically include **DDC** hardware (a term used widely in industry and also as part of the UFGS). DDC refers to a type of control hardware (microprocessor based) that performs control logic using directly sensed values and direct operation of an output device, such as an actuator or a solenoid or relay. DDC hardware automatically runs or controls the BCS-connected equipment based on a sequence of operation, which is either a written or logical description of the control functions to be performed by the DDC hardware. For example, this might include temperatures to be sensed, setpoints to be maintained, and devices to be actuated. The BCS generally uses controllers designed to perform real-time sensing and control functions without relying on a UMCS front end. These systems, in the Army environment, generally do not include (nor require) a dedicated local (i.e., at the building) front end. However, often BCSs include local displays with limited functionality at specific equipment (e.g., a local touch screen at a chiller).

- **UCS.** Utility control system. Generally considered industrial grade and is used for applications where a higher level of reliability and performance can justify a higher cost, such as for process control or power distribution systems. One example, often used in DoD applications, is a supervisory control and data acquisition (SCADA) system. A UCS might vary in composition from “smart relays” to programmable logic controllers (PLC). A UCS is used for systems such as electrical distribution and generation (that might include a microgrid), central steam distribution, sanitary sewer collection and treatment, sewer lift stations, water generation and pumping, etc. Note that these systems, unlike BCS, often include their own dedicated local front end, and in some cases, the front end will have limited or no control capability (i.e., it may perform monitoring-only functions).

FCN. Field control network. There are two categories of FCN:

- **BCN**. Building control network. The communication network used by the BCS
- **UCN**. Utility control network. The communication network used by the UCS

FPOC. Field point of connection. The connection point between the portion of the network (e.g., FCN) that is physically dedicated to the control system and the portion of the network (e.g., UMCS IP network) that is shared with other applications. Typically, in a BCN the FPOC is a NEC-owned-and-managed switch, as illustrated in Figure 4–Figure 6, and resides in each facility’s IT room. The NEC will refer to it as the end use building switch (EUB). UFC 4-010-06 further describes the FPOC (DoD 2017a).

UMCS IP Network. A basewide IP network, typically part of the installation campus area network (ICAN) provided and supported by the installation's NEC, that supports interbuilding communication and serves as the communications link between the field control system(s) and the UMCS computer(s). While the UMCS IP network could be contractor installed, it will generally be Government furnished. Note that coordination with the NEC is critical to ensure that the IP network usage is approved and that cybersecurity for the UMCS has been addressed.

3.1.2 UMCS technology: BCS vs UCS

This technical guide focuses almost exclusively on UMCS technology consisting of a front end integrated with (or connected to) multiple BCSs (typically performing commercial-grade HVAC control, lighting control, and energy metering functions) as opposed to utility control systems (UCS), such as microgrids, gas or electrical distribution systems, or other industrial-grade process control applications.

As the Army pursues improved energy resiliency and expands smart infrastructure at installations, and as technologies mature, installations will experience increasing interconnection between different types of control systems (e.g., BCS and UCS).

As an example, a microgrid control system as a potential part of a basewide UMCS offers capabilities and efficiency to improve how the installation uses electrical energy. In DoD applications, a microgrid can provide power resiliency to serve critical electric loads with high reliability, where the microgrid uses advanced control systems to island a distribution system when utility service is not available. Microgrids might also operate in a grid-connected mode to manage renewable energy production and energy storage units. Microgrids are further discussed in Appendix J.

3.2 Open Control Systems technology

“WAR STORY”

Installation X was an early innovator with DDC. Not satisfied with the pace of the Corps of Engineers’ DDC evolution, they went beyond the original DDC adopted by the Corps, referred to as Single-Loop Digital Control, and implemented by themselves, with some Louisville District help and a bit of CERL advice, an early version of Niagara Framework, a technology later adopted and currently used by the Corps. With a staff of two or three dedicated DPW staffers, they developed an early version of a building operations center (BOC) with multiple “open”-systems-technology control systems (of the time) in about 100 buildings. Their BOC, crammed into the back of the electrical shop, had several over-sized monitors displaying the status of Installation X’s building control systems sprawled across the installation.

A UMCS, as discussed in this guide, consists of a front end and at least one but usually many (dozens to several hundred) BCSs. BCSs are usually installed, expanded, or replaced across the installation on a building-by-building or system-by-system basis under separate contracts and, due to Government competitive procurement rules, often by different contractors. Unfortunately, these systems can be incompatible with each other in a variety of ways, from differences in the sensor input signals to differences in the communication protocols employed by the vendors. Even when vendors use the same protocols, differences in *implementation* of the protocol can cause systems to be incompatible.

One example is when a failed controller cannot be replaced by a different brand of controller because the sensor inputs from one might be voltage signals, while the sensor inputs from the other controller are resistance.

Another very common area of incompatibility is in how a controller communicates and interoperates (over a network) with other controllers or a front-end computer. Most manufacturers’ controllers use a communications technique that is unique to their line of controllers. At the same time, most manufacturers are also adopting industry standard communications and Open Control Systems technology to help alleviate communications incompatibilities.

Open systems technology, as further described below, is beneficial because it allows for the procurement of interoperable BCSs from multiple vendors by establishing requirements for an implementation of a shared (open) protocol that is common across the various building control systems as well as the UMCS front end. This helps ensure that the BCSs are not only compatible with each other but can be integrated into the single basewide UMCS.

3.2.1 What is an Open Control System?

Generally, an Open Control System is one where there is no future dependence on any one contractor or controls vendor:

It is one system—multiple field systems with controls installed by multiple vendors are integrated into one system.

There is one common front end that provides users with the capability to interface with all field systems (monitoring, supervisory control, etc.).

There are a minimum number of vendor-proprietary (software) tools (ideally zero, in practice, a small number) required to operate, maintain, and modify the system.

There is no future need for the installing contractor or any particular device manufacturer to perform work on the system.

There is no need for coordination between the installer of the field system and the installer of (or integrator to) the front end. As long as each contractor follows the appropriate specification, the systems will interoperate.

It is important to be aware that openness is not black and white. There is no such thing as a 100% open system, but the DoD criteria and specifications are intended to procure the most Open Control System practical. Further, an Open Control System can contain some proprietary components and can have fees, provided the components are a small part of the system and the fees are reasonable.

3.2.2 Open Control Systems technology options

A communications protocol is a set of rules that defines how data are transmitted between pieces of equipment. For example, a protocol might define that all temperatures be transmitted in units of Celsius and not

Fahrenheit. Different vendors often use a communications protocol unique to their line of products, which can lead to an inability to communicate with devices from other vendors and prevents the establishment of a single multivendor system.

An open protocol is one that is published, ideally by a standards organization. An Open protocol, to be useful, must be supported, meaning it is widely used and is maintained.

UFGS 25 10 10 describes multiple technologies with several available industry standard open protocols available to support these technologies. These technologies include

- BACnet and ANSI 709.1, primarily as BCS protocols where they are also available as BACnet-over-IP (BACnet/IP) and CEA-852 (Lon/IP),
- The Niagara Framework (further described below), which is the de facto nonproprietary standard and is IP based,
- Modbus and DNP, primarily as UCS protocols, and
- OPC is used for integration of UCS or BCS systems but is not generally considered a field protocol.

There are four different Open Control Systems technology options defined by DoD criteria for BCS applications (e.g., HVAC, lighting, etc.). They are based on LonWorks, BACnet, and Niagara Framework. In summary, the four options as presented in UFGS 23 09 00 *Instrumentation and Control for HVAC* are

1. BACNET: A building control system with components based on BACnet and using the BACnet communication protocol and interoperable with a UMCS front end using BACnet advanced workstation (B-AWS)
2. LNS LonWorks: A building control system with LonWorks components, using CEA 709.1 (commonly known as LonTalk) as the communication protocol, LNS as the network database standard, and interoperable with a UMCS front end using LNS
3. NIAGARA BACNET: A building control system using the Niagara Framework and BACnet controllers. This system is interoperable with a UMCS front end using the Niagara Framework.
4. NIAGARA LonWorks: A building control system using the Niagara Framework and LonWorks controllers. This system is interoperable with a UMCS front end using the Niagara Framework.

3.2.3 BACnet

The first part of this subsection describes basic BACnet terms and technology. The second part describes DoD implementation.

BACnet (Building Automation Control Network) is a communications protocol for building automation and control system networking defined by ANSI/ASHRAE standard 135 that supports the integration of control system products made by different manufacturers into a single system. BACnet loosely describes a collection of technologies, including hardware, software, vendors, and installers related to or based on the ASHRAE Standard 135 communications protocol. BACnet is supported by BACnet International, an industry association that facilitates the use of the BACnet protocol in building automation and control systems through interoperability testing, educational programs, and promotional activities. BACnet International oversees operation of the BACnet Testing Labs (BTL) and maintains a global listing of tested products.

A BACnet network browser provides the capability to read values from and write values to a BACnet network. While the M&C software will also have this functionality, the BACnet network browser can be installed on a laptop and used by maintenance staff in the field even when the building control system is not connected to the UMCS IP network or when a local interface is beneficial.

In addition to HVAC, the BACnet standard is designed to support other building control functions, such as life safety, security, lighting, energy metering, and power analysis. The latest industry information on BACnet is available at http://www.bacnet.org/.

BACnet—DoD Implementation

DoD BACnet design guidance is described in UFC 3-410-02, *Direct Digital Control for HVAC and Other Building Control Systems*. UFGS 23 09 23.02 specifies BACnet BCS requirements, and UFGS 25 10 10 specifies BACnet UMCS requirements.

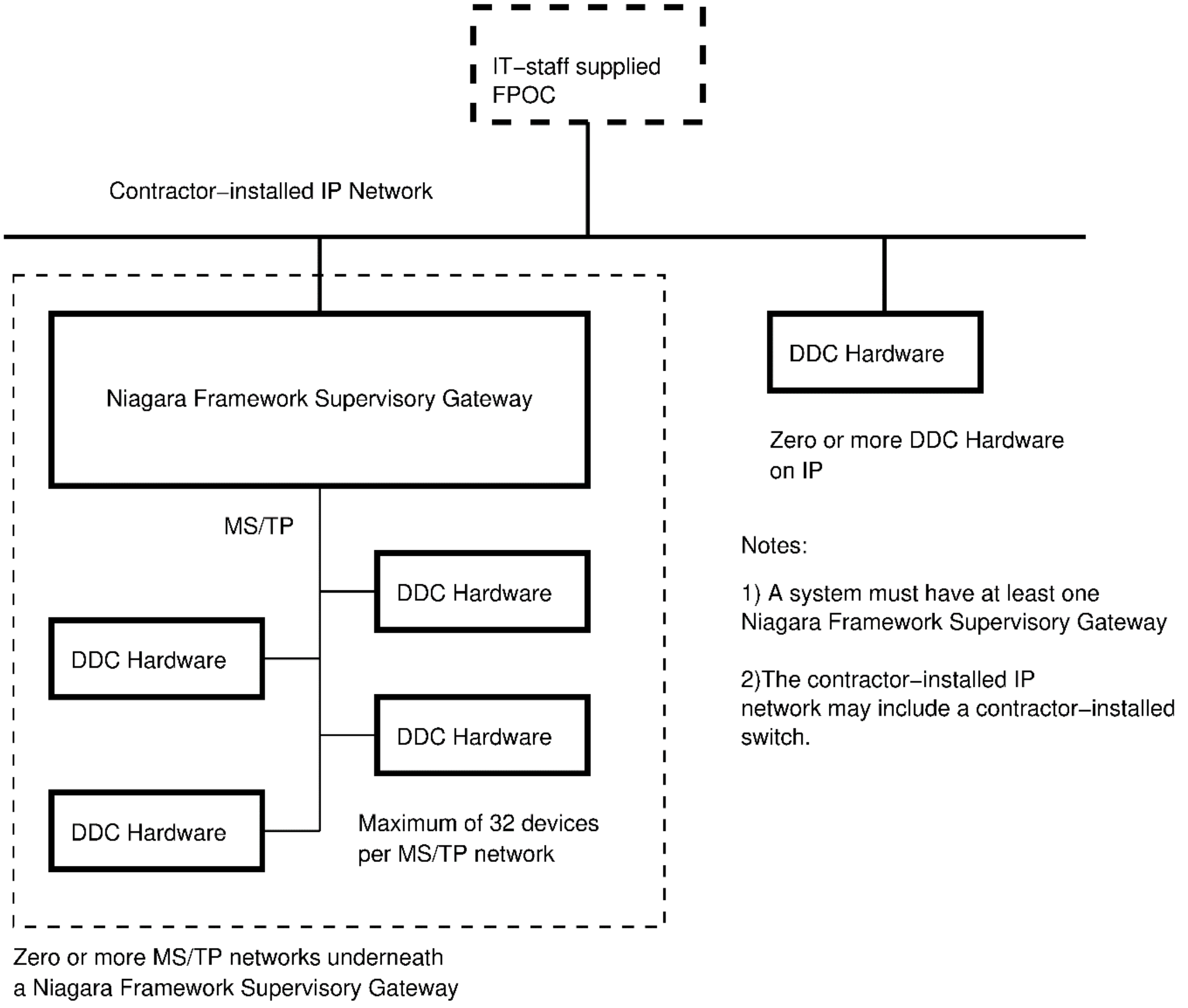
There are two BACnet approaches described by the DoD criteria: with and without Niagara Framework.

Figure 4 and Figure 5 illustrate BACnet building network architecture with and without Niagara Framework, respectively, in accordance with (IAW) DoD criteria. Each consists of an IP network with a mixture of DDC hardware (including, in the case of the Niagara Framework, Niagara Framework Supervisory Gateways) and BACnet MS/TP-to-BACnet IP[9] routers (which may be furnished as part of the DDC hardware). At the contractor's discretion, each MS/TP-to-IP router or Niagara Framework Supervisory Gateway may have MS/TP networks beneath it, with DDC hardware on the individual MS/TP networks. Each project will have a single FPOC, which provides an interface between the basewide IP network and the BCN installed by that project.

UFC 3-410-02 describes BACnet media selection and BACnet device and network addressing.

[9] BACnet MS/TP is a BACnet device using master slave token passing protocol. BACnet IP is a BACnet device using internet protocol

Figure 4. BACnet (with Niagara Framework) building network architecture (IAW DoD criteria).

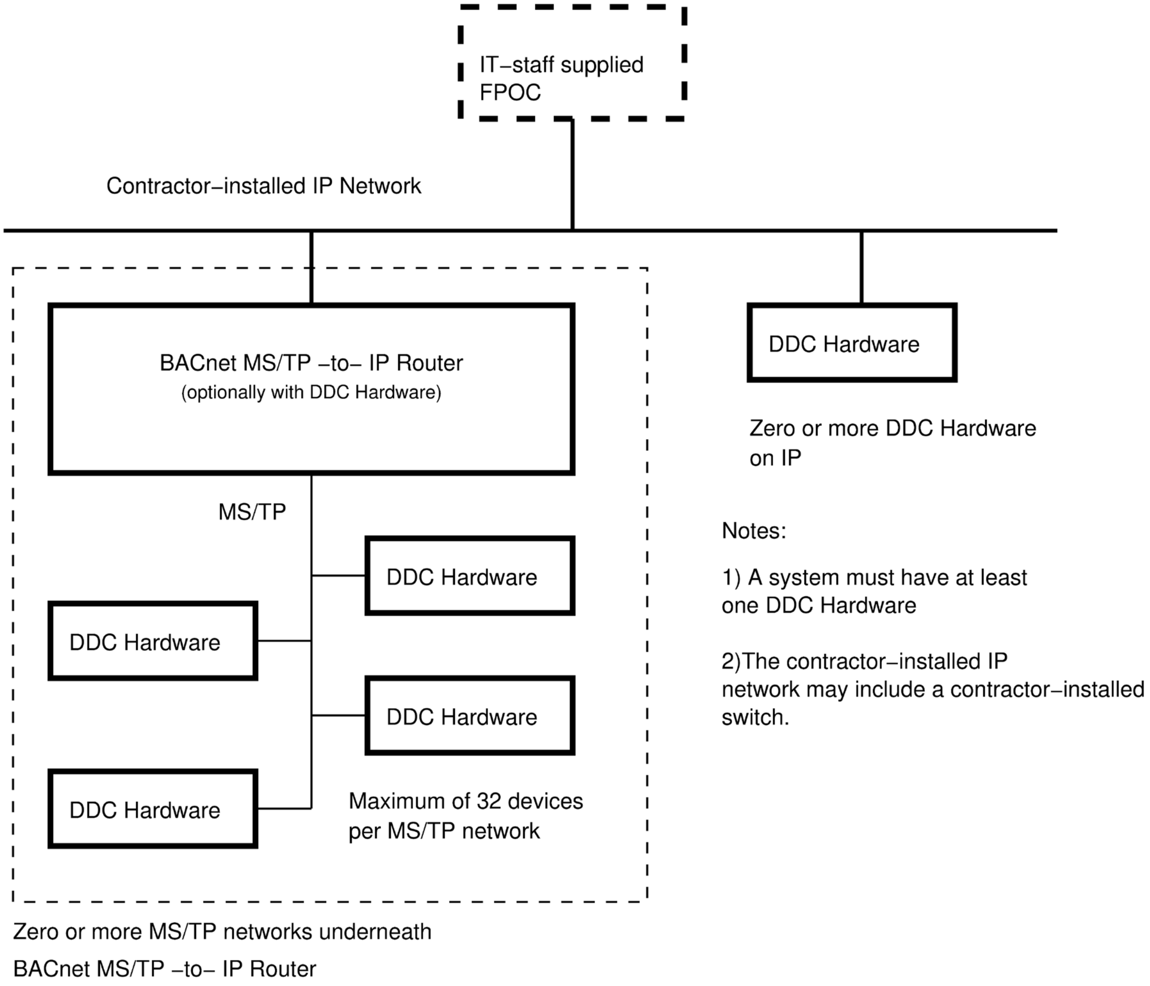

IT–staff supplied
FPOC
Contractor–installed IP Network
Niagara Framework Supervisory Gateway
MS/TP
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
Maximum of 32 devices
per MS/TP network
Zero or more MS/TP networks underneath
a Niagara Framework Supervisory Gateway
DDC Hardware
Zero or more DDC Hardware
on IP

Notes:

1) A system must have at least one Niagara Framework Supervisory Gateway

2)The contractor–installed IP network may include a contractor–installed switch.

Figure 5. BACnet (without Niagara Framework) building network architecture (IAW DoD criteria).


IT–staff supplied
FPOC
Contractor–installed IP Network
BACnet MS/TP –to– IP Router
(optionally with DDC Hardware)
MS/TP
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
Maximum of 32 devices per MS/TP network
Zero or more MS/TP networks underneath BACnet MS/TP –to– IP Router
DDC Hardware
Zero or more DDC Hardware on IP
Notes:
1) A system must have at least one DDC Hardware
2)The contractor–installed IP network may include a contractor–installed switch.

Specifying BACnet to connect to legacy buildings (buildings containing preexisting systems not installed in accordance with DoD criteria) is a challenge because the existing systems may not have the ability to pass information on a BACnet. The designer will need to work closely with the existing hardware supplier to determine what degree of BACnet capability (if any) is possible with the existing system. These legacy systems will likely require a gateway to connect the BACnet and the legacy system. In specifying the gateway, the specifier needs to list the alarms, trends, schedules, variables, and point data that must be transferred. UFGS 25 10 10 specifies how to do this (DoD 2019g). Simply stating in the specification that the existing system has to be made BACnet compatible is not enough.

3.2.4 LonWorks

LonWorks refers to the overall technology related to the CEA-709.1-D standard protocol (sometimes called “LonTalk”), including the protocol itself, network management, interoperability guidelines, and products. It is supported by LonMark International, a global membership organization consisting of numerous independent product developers, system integrators, and end-users dedicated to determining and maintaining guidelines for the interoperability of CEA-709.1-D devices and issuing the LonMark Certification for CEA-709.1-D devices. Common terms include the following:

- **LonWorks** is the technology.
- **LonTalk** is the name of the CEA 709.1-D standard communications protocol given to it by its original developer (Echelon Corporation, now part of Adesto Technologies).
- **LONMARK** is a certification issued by **LONMARK International** that certifies a device as LONMARK compliant and bears the LONMARK logo.
- **LON** is the local operating network (similar to a LAN but larger). **Lon** is also a shorthand term sometimes used instead of the term LonWorks.
- **LNS** (LonWorks Network Services) is a network management and database standard for CEA-709.1-D devices.

LonWorks—DoD Implementation

DoD LonWorks design criteria are described in UFC 3-410-02, *Direct Digital Control for HVAC and Other Building Control Systems* (DoD 2018a). UFGS 23 09 23.01 specifies LonWorks BCS requirements, and UFGS 25 10 10 (DoD 2019g) provides LonWorks UMCS requirements.

There are two LonWorks approaches described by the DoD criteria: with and without Niagara Framework.

Figure 6 and Figure 7 illustrate LonWorks building network architecture with and without Niagara Framework, respectively, in accordance with DoD criteria. Building networks consist of an IP network with one or more routers to connect the non-IP controller network with the IP-based controller network: CEA 852 routers (for LonWorks with LNS) or Niagara Framework Supervisory Gateways (in the case of LonWorks with Niagara). At the contractor’s discretion, beneath each CEA 852 router or Niagara

Framework Supervisory Gateway is either TP/XF-1250 media or TP/FT-10 media (not all Niagara Framework Supervisory Gateways will necessarily have a network beneath them). TP/XF-1250 media functions as a non-IP network backbone and will only have Lon-to-Lon routers connected to it.

Figure 6. LonWorks (with Niagara Framework) building network architecture (IAW DoD criteria).

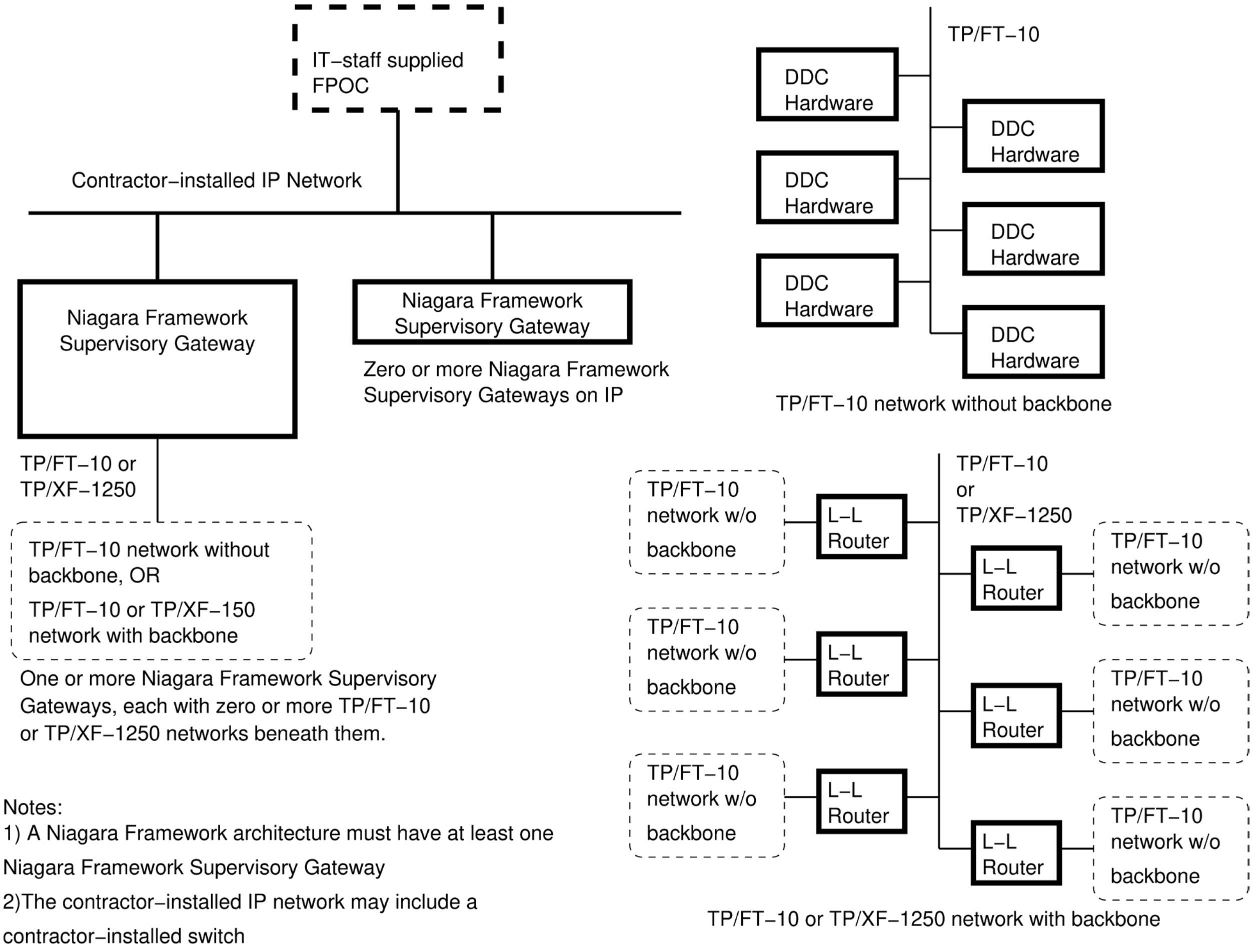
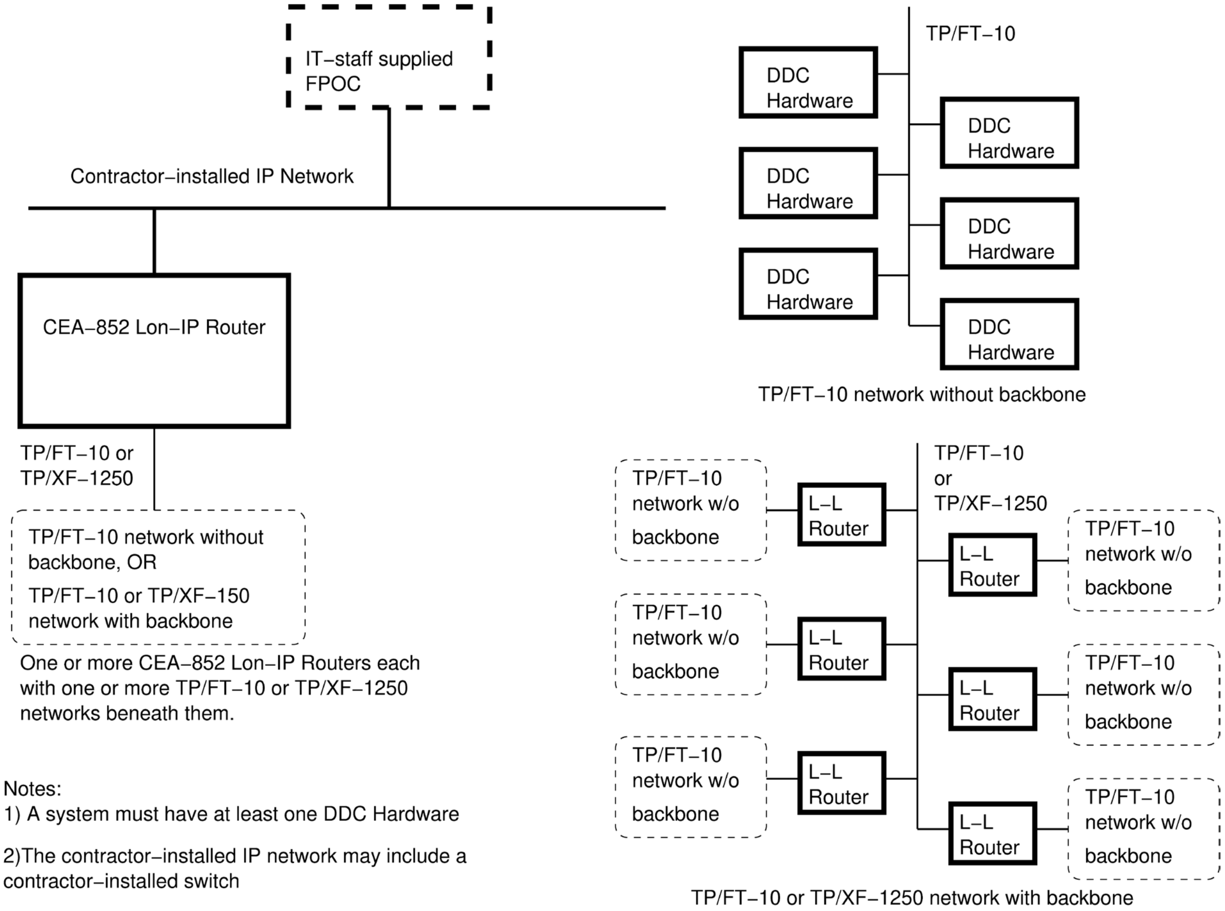

IT−staff supplied FPOC
Contractor−installed IP Network
Niagara Framework Supervisory Gateway
Niagara Framework Supervisory Gateway
Zero or more Niagara Framework Supervisory Gateways on IP
TP/FT−10 or TP/XF−1250
TP/FT−10 network without backbone, OR
TP/FT−10 or TP/XF−150 network with backbone
One or more Niagara Framework Supervisory Gateways, each with zero or more TP/FT−10 or TP/XF−1250 networks beneath them.
TP/FT−10
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
TP/FT−10 network without backbone
TP/FT−10 or TP/XF−1250
TP/FT−10 network w/o backbone
L−L Router
TP/FT−10 network w/o backbone
L−L Router
TP/FT−10 network w/o backbone
L−L Router
L−L Router
TP/FT−10 network w/o backbone
L−L Router
TP/FT−10 network w/o backbone
L−L Router
TP/FT−10 network w/o backbone
TP/FT−10 or TP/XF−1250 network with backbone
Notes:
1) A Niagara Framework architecture must have at least one Niagara Framework Supervisory Gateway
2)The contractor−installed IP network may include a contractor−installed switch

Figure 7. LonWorks (without Niagara Framework) building network architecture (IAW DoD criteria).


IT–staff supplied FPOC
Contractor–installed IP Network
CEA–852 Lon–IP Router
TP/FT–10 or TP/XF–1250
TP/FT–10 network without backbone, OR
TP/FT–10 or TP/XF–150 network with backbone
One or more CEA–852 Lon–IP Routers each with one or more TP/FT–10 or TP/XF–1250 networks beneath them.
Notes:
1) A system must have at least one DDC Hardware
2)The contractor–installed IP network may include a contractor–installed switch
TP/FT–10
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
DDC Hardware
TP/FT–10 network without backbone
TP/FT–10 or TP/XF–1250
TP/FT–10 network w/o backbone
L–L Router
TP/FT–10 network w/o backbone
L–L Router
TP/FT–10 network w/o backbone
L–L Router
TP/FT–10 network w/o backbone
L–L Router
TP/FT–10 network w/o backbone
L–L Router
TP/FT–10 network w/o backbone
L–L Router
TP/FT–10 or TP/XF–1250 network with backbone

3.2.5 Niagara Framework

The Niagara Framework is a protocol and set of technologies developed and owned by Tridium Inc. (who, in turn, is owned by Honeywell) and is licensed to multiple vendors using an open access licensing procedure as described later.

Different vendors provide this system under different product names, but the overall term used by Tridium is “Niagara.” While the Niagara Framework is focused at the UMCS front end, it also provides support for field devices and field protocols within BCSs and UCSs using a variety of protocols, most notably including BACnet and LonWorks.

Niagara Framework does not provide a flat system since the Niagara Framework Supervisory Gateways[10] used in the field control systems (primarily BCSs but also for UCSs) functions as a gateway, but it can provide a single multivendor system. To integrate with a UMCS front end based on the Niagara Framework, a building control system must be installed using the Niagara Framework components, such as the Supervisory Gateway, while the remaining FCS/BCS components can be from any vendor meeting UFGS requirements. All Niagara components must use an open license, which allows multiple vendors to interoperate freely with Niagara components from other vendors.

The Niagara Framework provides an overlay system. At the bottom level of the architecture, there are non-Niagara Framework controllers based on either LonWorks or BACnet. Above those controllers are Niagara Framework Supervisory Gateways, which connect the individual building to a Niagara Framework UMCS front end.

The Niagara Framework engineering tool is software used to program and configure all aspects of the Niagara Framework, including both Niagara Framework Supervisory Gateways and the Niagara Framework M&C software. It also provides network management and device configuration capabilities for Niagara Framework devices. In general, the Lon or BACnet devices underneath the Niagara Framework Supervisory Gateways may require additional software tools to support those devices. However, some vendors have devices and software tools, which are compatible with the Niagara Framework engineering tool.

Niagara Framework—DoD implementation

The Niagara Framework may be used in conjunction with either the BACnet or LonWorks UFGS option to design a system that can interoperate with a Niagara Framework front end when installed in accordance with UFGS 25 10 10 (DoD 2019g) and UFC 3-401-01 (DoD 2015b). UFGS 25 10 10 (re: UMCS), UFGS 23 09 23.01 (re: LonWorks) (DoD 2019e), and UFGS 23 09 23.02 (re: BACnet) (DoD 2019a) contain requirements and options for use of the Niagara Framework. With any protocol (e.g., LonWorks or BACnet) the Niagara Framework Supervisory Gateway converts

[10] This device is more commonly known as a “JACE,” which is the name for a specific version of this device. The term “Niagara Framework Supervisory Gateway” is used to remain vendor neutral. The JACE might be referred to by vendor-specific names: EC-BOS, FX-40, or UNC.

between the building protocol and the UMCS front-end protocol and is ordinarily installed as part of the BCS. Note that the use and selection of Niagara Framework will override some design options that would normally be used in a purely BACnet or LonWorks system.

Niagara Framework is the only UMCS Open Control Systems technology that provides for all-inclusive open access at the UMCS front end. (The downside is that each BCS has a Niagara Framework Supervisory Gateway in it, so the BCS is less open than a purely BACnet or purely LonWorks BCS). The licensing procedure ensures that any systems integrator has access to the system and its components. To this end, it is important that the licensing be accomplished (and specified) in accordance with the Niagara Compatibility Statement (NiCS) as described below.

The two ways DoD criteria implements the Niagara Framework are

- Niagara Framework and **LonWorks**. Figure 6 shows that a Niagara Framework Supervisory Gateway provides a connection to the IP network. The Niagara Framework Supervisory Gateway is a gateway and (unlike a CEA 852 router) does not route CEA 709.1 to the IP network. The Niagara Framework Supervisory Gateway is DDC hardware and may be connected directly to the IP network. The Niagara Framework engineering tool is used for network management instead of an LNS-based tool. For many requirements, an LNS-based requirement is replaced with a similar requirement based on the Niagara Framework engineering tool. The communication between the building control system and the front end is via the Niagara Framework and not CEA 709.1.
- Niagara Framework and **BACnet**. Figure 4 shows the Niagara Framework Supervisory Gateway functions as the BACnet MS/TP-to-IP router. The Niagara Framework Supervisory Gateway does route BACnet, and all MS/TP networks must be connected to a Niagara Framework Supervisory Gateway. The communication between the building control system and the front end is via the Niagara Framework and not BACnet. Non-Niagara BACnet devices on the IP network must use the Niagara Framework Supervisory Gateway to communicate with the Niagara Framework front end.

Regardless of whether Niagara Framework is used with LonWorks or BACnet, a key aspect of the DoD implementation of Niagara Framework is the requirement for open licensing. The licensing must be in in accordance with the NiCS, where the requirements for the NiCS unrestricted license are spelled out in UFGS 23 09 00 (DoD 2019d) and UFGS 25 10 10 (DoD 2019g), including the appropriate entries in the license.dat file. This licensing is essential so that any vendor or system integrator can work on the system. Note, both the front end and BCS UFGS specifications are mentioned because the NiCS is needed for UMCS front-end open access and is also needed at the BCS (building level) for each NFSG.

3.2.6 System licensing

All UMCS have licensing requirements. Licensing must be considered for certain UMCS software and even some hardware. The UMCS workgroup should take into account licensing for the size and scale of the UMCS front end (i.e., the M&C software). Regardless of the vendor, licenses must be managed, but this seems to especially be the case with Niagara Framework due to the sheer number of potential licensed components.

With regard to the front-end M&C software, licensing for *any* UMCS can involve at least two parameters: the number of system users and the number of system points that the front end will handle. This information should be obtained by the UMCS workgroup, possibly as part of a site survey as described elsewhere in this technical guide.

3.2.7 Choosing an Open Control Systems technology option

The primary goal of choosing one of the four Open Control Systems technology and protocol options (described previously) is to ensure that the UMCS front end and the connected BCSs are interoperable. The selection of Niagara Framework, LonWorks, or BACnet should be done carefully. Information is widely available to help with this decision—unfortunately, while some of it is good, much of it is not good, and a surprising amount of it is wrong. For Army projects, installations are advised to coordinate with the UMCS MCX at Huntsville Engineering and Support Center. Note that this decision should only be made once—at the procurement of a new UMCS. All subsequent work must use the same protocol to ensure proper interoperability.

UFC 3-470-01 discusses protocol advantages and disadvantages (DoD 2018b).

Open Control Systems technology and protocol selection considerations include

1. Availability of local contractor support. This is the number one concern; the best protocol and software in the world will not make up for poorly trained installers and contractors. To some extent, this also depends on level of complexity in the specification and level of enforcement—both the LonWorks and BACnet specifications (IAW DoD requirements) tend to push contractors out of their comfort zone with the need to meet requirements largely unique to the DoD. Where it is well supported locally, selecting the Niagara Framework option will allow for a somewhat more "normal" installation.
2. Expected future support. Most vendors are reducing or eliminating their support for LonWorks-based controllers. Consequently, in the future an LNS-based UMCS front end (one of the three main DoD specification options) may have limited vendor options for new BCS work. An installation with an LNS-based UMCS front end may find itself in a situation where continued growth of that system is prohibitively expensive, and an installation should carefully consider this before installing a new LNS-based UMCS front end.
3. BCS compatibility. The primary driver behind protocol selection must be the needs of the BCSs. Only if there are a large number of UCSs to be integrated and they use a common protocol should the UCS requirements impact the overall choice of protocol. Even then, BCS protocol compatibility should not be sacrificed for UCS protocol compatibility. Most BCS vendors make hardware gateways that support Modbus (for UCS connection), some BCS vendors' front ends support Modbus or OPC. (Note: UCS and BCS characteristics were described earlier).
4. Open systems protocol options. In order to support the procurement of open BCSs, the UMCS must support either BACnet, LonWorks, or the Niagara Framework. In general, the UMCS front end should not support more than one. The only possible exception would be an installation with a large established base of both Niagara Framework and BACnet buildings that wishes to continue to add both Niagara and BACnet buildings and to have a single UMCS (an installation wishing to support multiple protocols could simply have multiple UMCSs). Since many BACnet vendors' front ends do not support Modbus or OPC, if BACnet is selected, Modbus or OPC should NOT be selected (this might otherwise severely limit competition).

5. Existing front end protocol. If a UMCS front end preexists, selecting the BCS protocol supported by the UMCS front end is recommended. UFGS tailoring options supported by the UMCS front end should be used.
6. Front end options. If no UMCS front end exists or one has not been selected as the basewide UMCS, all four options are on the table.
7. Niagara BCS options. If the Niagara Framework is selected, it is strongly recommended to standardize on either LonWorks or BACnet for the BCSs. This will help provide a more maintainable system for operation and maintenance staff as they will not have to understand both protocols and can reduce the number of software tools that must be maintained.
8. Staff experience. The local staffs' (DPW, HVAC shop, energy manager, civil engineering group, resident engineer, etc.) prior experience with and knowledge of local vendor capability and competence should be considered.
9. Predominant systems. The extent and type of existing legacy systems should be considered. This is important, but for most installations, no single legacy system has a clear majority of buildings when compared to the eventual size of a site-wide UMCS. However, the existence of a large quantity of specific legacy systems is generally an indicator of local vendor support. As part of this, it is helpful to consider the compatibility of the legacy systems with an open-protocol UMCS. In other words, how well do the legacy systems meet the Open Control Systems requirements of the DoD criteria? For example, older Niagara Framework Supervisory Gateways may not be compatible with the newer Niagara Framework architecture. To help assess legacy system support, the installation might seek assistance from the UMCS MCX at Huntsville Engineering and Support Center.
10. Technology capabilities. The particular strengths and weaknesses of each option should be considered where there is no clear preference based on local support or existing legacy buildings between LonWorks, BACnet, or Niagara Framework.
11. Vendor capabilities. The need to support large numbers of Modbus or OPC UCS systems might eliminate some BACnet vendors from consideration since many BACnet vendors' front ends do not support Modbus and/or OPC.
12. Existing accreditation. Any existing valid accreditation or Authority to Operate (ATO) and its supported vendors or protocols should be considered.

3.3 Specifications and criteria related to UMCS

The DoD has established Tri-Service-vetted Unified Facility Guide Specifications and criteria to guide military facility design and construction.

These documents are available at the Whole Building Design Guide, https://www.wbdg.org. There is an extensive set of UFGS and UFC for use in procurement of BCSs—specifically HVAC, but also applicable to other systems—and in procurement and integration of a UMCS front end. There is also a UFGS and UFC for cybersecurity of these systems. These documents are continually updated and interested individuals may submit criteria change requests online. The Whole Building Design Guide should be consulted when using these criteria and specifications to determine the latest version and changes or amendments.

UFCs constitute the DoD building code, and compliance with this code is mandatory for all DoD construction, regardless of executing agency or funding type. Deviation from the code requires an exemption or waiver requests approved by the Engineer Senior Executive Panel (ESEP) member as defined in MIL STD 3007G (DoD 2019f). For the Army, the ESEP member and signature authority for UFCs is the Chief of Engineering and Construction of the Army Corps of Engineers.

UFGSs provide construction requirements in support of UFC criteria. In general, guide specifications use is not required, but it is strongly encouraged. Note that in the case of HVAC controls, the UFCs require the use of the UFGS, and that use of UFGS 25 10 10 (DoD 2019g) is also required by 10 USC 2867.[11]

Table 1 lists and describes the pertinent sections of the UFGS and UFCs. The UFGS covers a broad scope at currently 23K pages with 48 divisions and a table of contents that is 20 pages long. UFGS divisions and sections of interest for UMCS include Division 01—General Requirements; Division 23—Heating, Ventilating, and Air Conditioning (HVAC) Section 09 (Controls); and Division 25—Integrated Automation. The UFC is broken up into four series. UFC series of interest include Series 1—Policy, Procedures, and Guidance; Series 3—Discipline Specific Criteria, and Series 4—Multi-disciplinary and Facility Specification. Many UFGSs and UFCs have attached related documents.

The specifications have been carefully tailored to work together: UFGS 25 10 10 (front end spec) is designed to procure a front end that can integrate

[11] *Energy Monitoring and Utility Control System Specification for Military Construction and Military Family Housing Activities, 10 USC § 2867 (2009). https://www.govinfo.gov/app/details/USCODE-2011-title10/USCODE-2011-title10-subtitleA-partIV-chap169-subchapIII-sec2867.*

a BCS procured under UFGS 23 09 *xx* series (BCS specs);[12] UFGS 23 09 *xx* series (BCS specs) are designed to procure a BCS that can be integrated into a UMCS front end procured under UFGS 25 10 10 (DoD 2019g) (front end spec). Neither the building-level (23 09 *xx*) sections nor the front end (25 10 10) are sufficient in and of themselves, both sections are absolutely required to obtain a complete integrated system.

There are three UFCs that provide planning, design, and related criteria for either the BCS, UMCS, or cybersecurity. There is also a related cybersecurity UFGS (UFGS 25 05 11) (DoD 2017b).

The specifications and criteria were developed to help obtain open, nonproprietary, and interoperable multivendor BCSs that integrate with a UMCS front end server or workstations using one of the four Open Control Systems technology options described previously.

Ultimately, the UMCS, as defined by UFGS 25 10 10 (DoD 2019g), is intended to be a single system that serves as a basewide interface to the multivendor BCSs. The intent of UFGS and UFC criteria along with this guidance document is to help specify and procure an open and cyber-secure UMCS.

[12] Either 23 09 23.01 for LonWorks or 23 09 23.02 for BACnet

Table 1. UMCS design and specification criteria.

Document	Title	Description
UFGS 01 91 00.15 10	*Total Building Commissioning*	Detailed commissioning requirements, including building control system(s)
UFGS 23 09 00	*Instrumentation and Control for HVAC*	“Top level” spec with overall requirements
UFGS 23 09 13	*Instrumentation and Control Devices for HVAC*	Sensors, actuators, and instrumentation
UFGS 23 09 93	*Sequences of Operation for HVAC Control*	Control logic requirements for various HVAC systems
UFGS 23 09 23 .01	*LonWorks DDC for HVAC and Other Local Controls*	Specs based on LonWorks and ANSI/CEA 709.1 communications protocol
UFGS 23 09 23 .02	*BACnet DDC for HVAC and Other Local Controls*	Specs based on ASHRAE 135 BACnet communications protocol
UFGS 25 10 10	*UMCS Front End and Integration*	For procuring a new UMCS or integrating into an existing UMCS
UFGS 25 08 10	*Utility Monitoring and Control System Testing*	Factory and performance test requirements for UMCS and HVAC controls
UFGS 25 05 11	*Cybersecurity for Facility-Related Control Systems*	Cybersecurity requirements for facility control system projects
UFGS 25 08 11.00 20 (Navy)	*Risk Management Framework for Facility-Related Control Systems*	Navy requirements to support the Risk Management Framework (RMF) Authority to Operate (ATO) Process for facility-related control systems
UFC 1-200-02	*High Performance and Sustainable Building Requirements*	Building full life cycle guidance for sustainability. Calls for commissioning of building projects.
UFC 3-410-02	*DDC for HVAC and Other Building Control Systems*	Criteria for building control systems based on Open Control Systems technologies: LonWorks, BACnet, or Niagara Framework.
UFC 3-470-01	*UMCS Front End and Integration*	Criteria for an UMCS front end and connection to building control systems using Open Control Systems technologies
UFC 4-010-06	*Cybersecurity of Facility-Related Control Systems*	Criteria for application of RMF to UMCS and steps for cybersecurity design

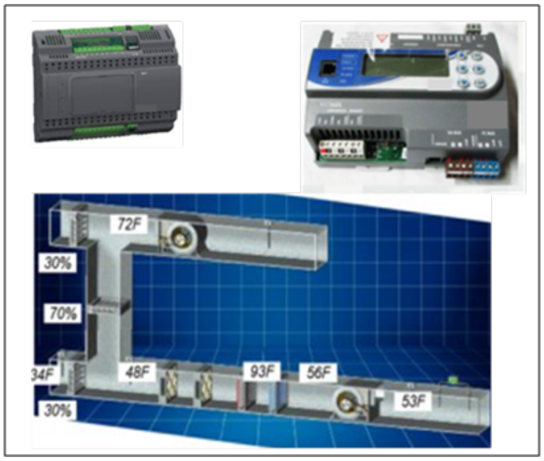
The following subsections summarize key features of UMCS-related specifications. They provide a summary description nickname for the document(s), followed by a more detailed description of the contents along with an indication of extent or nature of tailoring options that allow designers to develop a procurement specification that applies to their particular situation (such as choice of protocol and their applicable military service branch, etc.), and a list of key construction submittals required to demonstrate compliance with the specifications. The citation for the source document of each summary is given in the title of that subsection.

3.3.1 UFGS 23 09 00—*Instrumentation and Control for HVAC* (DoD 2019d)

Nickname: *Top level BCS spec (with general requirements and references to other Division 23 specs).*

Description: This specification defines the "top level" (general, starting point) requirements for a building control system (BCS) necessary for completely functional automatic control. It includes control hardware installation and startup, submittals, shop drawings, testing, and training requirements. See Figure 8.

Figure 8. Typical UFGS 23 09 00 hardware.



Tailoring Options:[13] Protocol Tailoring: LonWorks/BACnet/Niagara; Service Tailoring: Air Force/ Army/Navy/Navy with Acceptance Engineer/Service Generic, approximately 100 bracketed designer options

Key Requirements and Decisions:

1. All submittal, project sequencing, testing, and training requirements related to Division 23 HVAC controls requirements reside in this spec.
2. Control sequences must reside in the DDC hardware in the building. The building control network (BCN) must not be dependent upon connection to a UMCS front end or to any other system for performance of control sequences. To the greatest extent practical, the hardware performs control sequences without reliance on the building network.
3. A complete controls Points Schedule[14] must be part of the contract drawings. Points Schedules are key submittals that represent critical point naming, sequence of operation, and system interface requirements and must be coordinated between building-level and UMCS contractors.

[13] UFGS are developed using Government software called *SpecsIntact*. This software has a feature called *Tailoring*, where the user can select from some multiple-choice options; selection of these options automatically makes insertions and deletions in the specification to meet the selected options.

[14] A controls Points Schedule is the name of a specific drawing sheet that must follow a format detailed in DoD 2018a, (UFC 3-410-02)

4. A determination whether control logic diagrams (CLDs) must be included in the contract drawings must be made. The arguments for CLDs include specific and standardized HVAC logic and utilization of a common controls vendor language. The arguments against CLDs include the length of time to develop drawings and an increased risk of potential Government error. CLDs may limit the ability to leverage controls vendor expertise.
5. It is essential to ensure that performance verification testing (PVT) fully demonstrates compliance of controls work and complete required O&M training as part of PVT.

Part Descriptions:

1. General: This section details the goals and overarching guidelines of the specification and includes related specifications and references. It provides explicit definitions of all components referenced throughout the document and other UFGS 23 09 *xx* series documents. It includes a project sequencing table and submittal requirements. It describes the required software related to the programming and configuration of DDC hardware and Gateways. It notes that the quality control (QC) checklists are in Appendix A of the UFGS.
2. Products: This section details general requirements that the products must meet including operation environment, enclosures, and wire and cable. Product data sheets are also required.
3. Execution: This section details the execution process for developing a building control system, including existing conditions, installation, drawings and calculations (see Points Schedule), controller tuning, startup, PVT, if tailored for LNS—final LNS database, operation and maintenance (O&M) instructions, maintenance and service, and training.

Appendix A (of the UFGS): Quality Control (QC) Checklists.

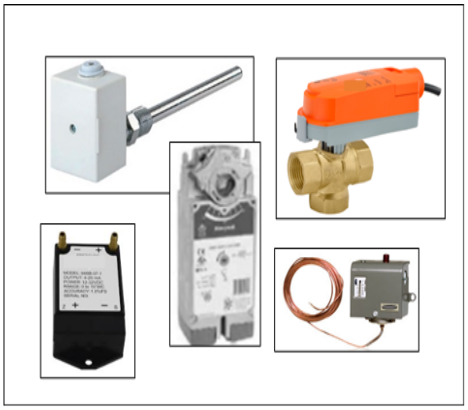
Key Submittals: SD-02 Shop Drawings, SD-03 Product Data, SD-06 Test Reports, SD-10 Operation and Maintenance Data, SD-11 Closeout Submittals

3.3.2 UFGS 23 09 13—*Instrumentation and Control Devices for HVAC* (DoD 2015a)

Nickname: *The Sensors and Actuators Spec*

Description: This specification defines requirements for all of the input and output control hardware (e.g., sensors and actuators) necessary for a completely functional automatic control system. These devices are typically home-run wired as low voltage (e.g., 0–10 V, 4–20 mA, dry-contact) devices and thus protocol agnostic, but the spec allows and defines requirements for networked sensors and actuators. See Figure 9.

Figure 9. Typical UFGS 23 09 13 hardware



Tailoring Options: Approximately 50 Designer Options (no protocol tailoring)

Key Requirements and Decisions:

1. Sensor ranges and accuracies
2. Space sensor module functions (room temperature display, setpoint adjustment, override pushbutton, occupancy sensor, etc.)
3. Electric or pneumatic actuation (of valves and dampers). Pneumatic actuation may require significant tailoring and associated decisions. An air compressor will need to be specified (requirements are in the spec).

Part Descriptions:

1. General: This section details the goals and overarching guidelines of the specification document and includes related specifications and references.
2. Products: This section details the hardware requirements, including accuracy, operating range, and materials for the following: weather shields, tubing, wire and cable, automatic control valves and dampers, actuators, sensors and instrumentation (temperature, pressure, flow, CO2, etc.), gauges, user input devices (e.g., switches, buttons), multifunction devices, and compressed air stations.
3. Execution: This section details the installation requirements for all equipment, including weather shields, room instrument mounting, indication devices installed in piping and liquid systems, occupancy sensors,

switches, temperature sensors, air flow measurement arrays, duct static pressure sensors, relative humidity sensors, meters, dampers, valves, thermometers and gauges, wire and cable, copper tubing, plastic tubing, pneumatic lines and compressed air stations.

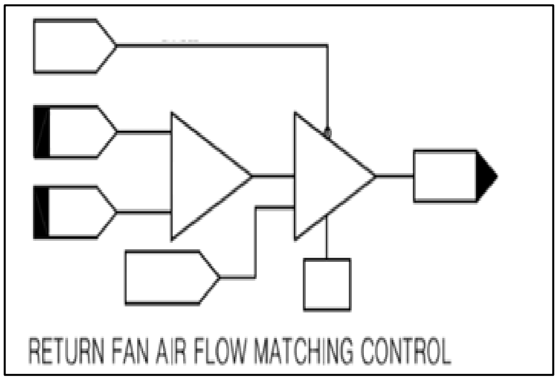
Key Submittals: In accordance with UFGS 23 09 00 "Manufacturer's Product Data," ensure temperature control modules are shown on Thermostat Schedule selected per the controls equipment schedule requirements

3.3.3 UFGS 23 09 93—*Sequences of Operation for HVAC Control* (DoD 2015c)

Nickname: *The Sequences Spec*

Description: This specification describes the sequence of operation for a variety of HVAC systems (e.g., an air handler). The sequence is a (written) narrative description of how the control is required to function. The sequences detailed in this specification are draft sequences; thus, when working with this specification, the sequences should be edited, and the final versions put onto the drawings described in UFGS 23 09 00. See Figure 10.

Figure 10. Example of a UFGS 23 09 93 sequence illustrated in control logic diagram format.



Tailoring Options: Approximately 60 Designer Options; (no protocol tailoring)

Key Requirements and Decisions:

1. Designer must decide whether CLDs will be part of the design package or shop drawings requirements; however, narrative sequences of operation must also be included.
2. It is important to make sure that Points Schedule requirements (point types, names, setpoints, resets, interface requirements, etc.) reflect the sequences of operations selected.
3. If considering the sequences of operation for air-side systems, it is important to note that most of the sequences assume the use of a system scheduler, occupied and unoccupied modes (as shown on the Points Schedule), and space occupancy inputs (occupancy sensor or local push

buttons) and require designer input on whether things like economizers, preheat coils, return fans, and zone temp setpoint adjustment will be in use.

4. A review of the need for and importance of alarms should be made so that nuisance alarms are minimized.
5. If considering the sequences of operation for hydronic systems, it is important to select steam or high-temperature hot water as appropriate. For systems based on an enabling condition, such as demand, the sequence and condition(s) that enable the system should be carefully considered.

Part Descriptions:

1. General: This section notes that information regarding definitions and submittals for this specification can be found in UFGS 23 09 00.
2. Products: None as part of this spec
3. Execution: This section details the requirements for sequences of operation for occupancy scheduling, including system mode, system scheduler requirements, system scheduler output determination, air handler system scheduling, and standalone terminal unit scheduling. This section also details the requirements for sequences of operation for specific systems, including air handling units, terminal units, and hydronic systems. For each unit or system, a controls narrative is provided that describes hand-off-auto (HOA) switches, equipment options, occupancy modes, proofs, safeties, system enables, and control loop details such as temperature, pressure, flow, fans, and pumps.

Key Submittals: In accordance with UFGS 23 09 00

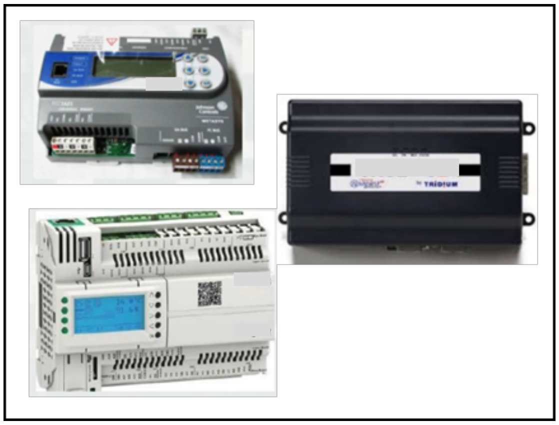
3.3.4 UFGS 25 09 23.01 and .02—*LonWorks/BACnet Direct Digital Control for HVAC and Other Local Controls* (DoD 2019e)

Nickname: *The LonWorks and BACnet specs.*

Description: These two specifications describe the requirements for a building control system including DDC hardware and LonWorks or BACnet communication protocol requirements necessary for a completely functional automatic control system at the building level. See Figure 11.

Tailoring: Protocol Tailoring (.01): LonWorks/Niagara; Protocol Tailoring (.02): BACnet/Niagara; Service Tailoring (.01/.02): Air Force/Army/Navy/Service Generic; ~20 Designer Options (.01); ~30 Designer Options (.02)

Figure 11. Typical 23 09 23.01/.02 hardware



Key Requirements and Decisions:

1. The control system must be an Open Control Systems installation such that individual control equipment can be replaced by similar control equipment from other equipment manufacturers with no loss of system functionality.
2. For an LNS-based LonWorks system, the contractor must submit the LNS database.
3. Hardware and software must be installed and configured such that the Government or their agents are able to perform repair, replacement, and upgrades of individual hardware and software without further interaction with the installing contractor.
4. It is important to ensure for the integration of a single piece of equipment that Gateways are used appropriately to prohibit the installation of new networks not meeting the requirements as stated in this specification.
5. A determination is needed as to whether Ethernet switches must be managed and if HOA switches should be included at DDC hardware outputs. These should only be required when there is a specific project requirement for them, otherwise they add extra cost to the system.

Part Descriptions:

1. General: These sections detail the goals and overarching guidelines of the specification and include system requirements for an Open Control Systems and use of the Niagara Framework. They also include related references.
2. Products: These sections detail the requirements that the components of the control system must meet, including network hardware, control network wiring, DDC hardware, and the Niagara Framework engineering tool.
3. Execution: These sections detail the control system installation requirements for all equipment, including the Niagara Framework engineering

tool, BCN, DDC hardware, scheduling, alarming, trending overrides, and Gateways.

Key Submittals: In accordance with UFGS 23 09 00. This also includes the submittal of source code.

3.3.5 UFGS 25 10 10 — *Utility Monitoring and Control System (UMCS) Front End and Integration* (DoD 2019g)

Nickname: *UMCS front end spec*

Description: This specification defines the requirements for a new utility monitoring and control system (UMCS) front end or the integration (to a BCS) using an existing UMCS front end. This specification deals with hardware, including standard IT components, computer hardware, IP networks, and UMCS software. See Figure 12.

Figure 12. Typical UFGS 25 10 10 hardware.

Tailoring Options: Protocol Tailoring: LonWorks/BACnet/Niagara/Modbus/OPC; Service Tailoring: Air Force/Army/Navy/Service Generic ~240 Options

Top Requirements and Decisions (when used to procure a new front end):

1. Ensure that the monitoring and controls software can execute the appropriate operational tasks, including viewing alarms, making overrides, viewing trends, and changing setpoints; and engineering tasks, including setting up alarms and trends, and creating new reports and graphics.
2. Many decisions reside in the server hardware and workstation hardware (desktop and laptop) sections. Ensure that these decisions are made with care.
3. The system must include a graphical user interface, which allows for access to all supervisory monitoring and control functions.

Key Requirements and Decisions (when used to integrate a new system to an existing new front end):

1. How will integration be funded and executed?

2. Was the front end installed IAW UFGS 25 10 10?
3. Was the BCS installed IAW UFGS 23 09 23?
4. Is the BCS protocol compatible with the UMCS front end?
5. Are graphics and point naming standards available?

Part Descriptions:

1. General: This section details the goals and overarching guidelines of the specification document with specific requirements for each of the specific protocols. It includes related references and explicit definitions of all components referenced throughout the document. It provides an outline for project sequencing. It also notes operation and maintenance instructions and quality control checklists in Appendix A of the UFGS.
2. Products: This section details general equipment requirements, including product certifications, product sourcing, nameplates, and product data sheets. It then goes on to specify control hardware, computer hardware, computer software (monitoring and control [M&C] software), uninterruptable power supplies (UPSs), and racks and enclosures.
3. Execution: This section details the execution process for installing and integrating a UMCS front end, including factory testing, an existing conditions survey, drawings and calculations, installation requirements, installation of equipment, three step integration of field control systems, startup and startup testing, PVT, maintenance and service, and training.

Appendix A (of the UFGS): QC Checklists

Key Submittals: SD-02 Show Drawings, SD-03 Product Data, SD-05 Design Data, SD-06 Test Reports, SD-10 Operation and Maintenance Data, SD-11 Closeout Submittals

3.4 Design and construction process overview

Overall, there are six basic design and construction scenarios depending on the project scope:

1. Front end only. Procure a new UMCS front end. Conduct no BCS work with this purchase.
2. BCS only. Procure one or more new BCSs. Do not integrate to a UMCS front end (standalone BCS).
3. Integration only. Integrate one or more BCSs to a UMCS front end.

4. Front end with integration. Procure a new UMCS front end. Integrate one or more BCSs into it (combination of 1 and 2).
5. BCS with integration. Procure one or more new BCSs and integrate into a UMCS front end (combination of 2 and 3).
6. Front end and BCS with integration. Procure a new UMCS front end. Procure one or more new BCSs and integrate into the UMCS front end (combination of 1, 2, and 3).

The first decision is whether the project involves UMCS front-end-related work only, or if the project includes the procurement of at least one building control system. Note that "UMCS front-end-related work only" can include the integration of a BCS that is not procured as part of the project, where the BCS could preexist or be procured separately.

3.4.1 BCS paths

1. Choose protocol and technology. Consider which protocol will be used—LON or BACnet—and whether or not to use Niagara Framework. How to make this decision is described in Section 3.2.6. Ideally, this decision will have already been made.
2. Design control system. Create new or edit existing control schematics, ladder diagrams, logic diagrams, sequence of operations, instrument schedules, and Points Schedules.
3. Taylor and edit specs. The specifications for protocol and other project-specific requirements and needs.
4. Develop Request for Proposal (RFP).
5. Award a contract.
6. Review submittals. Once the contract is awarded, there may be several iterations of submittal review.
7. Conduct inspections and acceptance procedures. As applicable and as specified, participate in inspections; startup; testing, adjusting, and balancing (TAB); performance tests; RMF assessment; endurance tests; and training and prepare closeout documents before final acceptance or turnover.

3.4.2 UMCS front end paths

1. Assess RMF posture.[15]

    a. New front end: If the project is a new UMCS front-end procurement, Determine or identify the system owner (SO) and authorizing official (AO). Assign system cybersecurity impact levels (related to confidentiality, integrity, and availability (CIA) of information and select applicable cybersecurity controls.

    b. Existing front end: If a UMCS front end exists, determine if it has a valid accreditation. If yes, then the next step is to select the protocol (if not already done during the BCS process).

2. Design control system. Develop UMCS front end schedules and drawings, including Points Schedule requirements.

3. Tailor and edit the specifications.

4. Develop the RFP.

5. Award the contract.

6. Review submittals.

7. Conduct acceptance procedures. As applicable and as specified, participate in inspections, startup, performance tests, RMF assessment, and training, and prepare closeout documents before final acceptance or turnover.

3.4.3 UMCS front end and BCS inspections, testing, and acceptance paths

UMCS front end and BCS technology (and contracting) can be very complicated. Careful and deliberate system(s) inspections and testing are necessary prior to system acceptance. This is discussed as part of commissioning in Section 6.

[15] See Section 8.

4 UMCS Implementation

4.1 Implementation planning checklist

This chapter describes UMCS implementation planning, scoping, and coordination activities that should be considered in advance of system use and are applicable to both new and existing systems. Table 2 contains a basic big picture checklist of activities. The checklist items are further discussed in this guide; section references are provided. Most of these implementation activities are included in this chapter; however, procurement, RCx, and cybersecurity are elaborated in other chapters due to the extensive guidance provided and their applicability throughout the UMCS lifecycle beyond implementation.

Table 2. UMCS implementation planning, scoping, and coordination activity checklist.

	Item	Description
1	UMCS workgroup (Sec. 4.2)	Select someone to be the UMCS manager (they may need to grow into this role). Create a workgroup to review UMCS technology, this guide, the four Open Control Systems technology options, etc., and ultimately, create a UMCS master plan. Engage with Design Branch, DPW, O&M shops and services, etc.
2	UMCS master plan (Sec. 4.9)	Create a plan. Start with an outline (that is later fleshed out) to identify and briefly describe important chapters, elements, issues, and content. Refer to "UMCS master plan" Section 4.9.
3	Design guidance (Sec. 4.3)	In coordination with the DPW and others, identify design and specification guidance sources and considerations for the UMCS (and BCSs). Develop an installation design guide (IDG) to help ensure new systems meet the installation's requirements. Develop design coordination checklists that identify specification needs and preferences (see Section 4.3).
4	Site survey of existing conditions (Sec 4.8)	Identify and assess existing UMCS front end and BCS infrastructure. Identify HVAC systems in need of repair or replacement and prioritize. Include as an appendix to the UMCS master plan.
5	Maintenance, PM, and RCx needs (Sec. 7.5)	Institute a regular program of scheduled maintenance, preventative maintenance (PM), and retrocommissioning (RCx) of systems.
6	DPW training (Sec. 4.6)	Identify training needs. Provide training and incentives for personnel to acquire needed skills and allow for advancement.
7	Cybersecurity & NEC coordination (Sec. 4.4; Chapter 8; Appendices D, E, and F; Long et al. 2019.)	Identify a NEC partner. Share this document's cybersecurity sections and the RMF how-to guide (Long et al. 2019) with NEC to facilitate RMF and help categorize the UMCS. Investigate the authorization strategy for the UMCS under the RMF.

	Item	Description
8	Staffing and assistance from others (Secs. 4.2.2 and 4.5)	Identify roles and positions. Many probably do not preexist and can be a significant challenge. Create a staffing strategy. Discuss needs and resources for staffing with management. Consider external support (contracted) elements to meet needs. Coordinate with Huntsville Engineering and Support Center (HNC) UMCS Mandatory Center of Expertise (MCX).
9	System integration approach (Sec. 4.7)	Consider the system integration approach and strategy along with funding and procurement mechanisms.
10	Budgets and costs (Sec 5)	Identify costs, funding sources, strategy.

4.2 UMCS workgroup

It is highly recommended that a UMCS workgroup be formed to help facilitate the various stages of UMCS implementation. A UMCS is most effective when all stakeholders (or their representatives) are involved. Stakeholders are those who have a vested interest in making the UMCS successful. All workgroup members should help identify and involve stakeholders.

The planning process requires a degree of familiarity with UMCS technology, which can vary considerably among individuals. The planning process is an education and workforce development opportunity for stakeholders regarding the benefits and challenges of UMCS.

The workgroup should be led by a UMCS manager, a Government employee who has both the responsibility and authority to successfully manage the UMCS. This is a position that generally does not exist (at a sufficient GS level) at most installations to be effective. This position will be covered in more detail in Section 7.

4.2.1 Members

The UMCS workgroup should include the following individuals or office representatives:

- *UMCS Manager*. This person leads the planning effort and, as described in Section 7.2, is the individual with responsibility over the UMCS's day-to-day use and growth and is the principal champion of the UMCS. Presently, this will generally be a role taken on by another member of the DPW team listed here.
- *DPW Energy Manager and/or Utilities Division Chief*

- *DPW Mechanical Engineer*
- *DPW O&M Chief*
- *DPW Shop and/or Work Leader(s)*
- *DPW Technicians and Mechanics*
- *DPW Plans and Programs, Engineering Division, and/or Master Planning*
- *Network Enterprise Center (NEC)*

Not all members of the UMCS workgroup need to be involved in the entire planning and implementation process, but all members can be expected to contribute at various stages of plan development. A statement of intent should be communicated to the Director of Public Works, the garrison commander, and others as applicable through a memo, e-mail, or meeting since support from these individuals will be essential to the successful development and implementation of the plan.

4.2.2 Assistance from others

Planning can benefit from, and may depend on, other individuals and organizations who are not necessarily members of the UMCS workgroup:

- ***Director of Public Works***—A director can assist the workgroup with advocacy across all DPW offices and between the DPW and other groups such as the NEC, Job Order Contracts group and Plans & Programs office, etc.
- ***Garrison Commander***—A garrison commander who recognizes the value of a functional UMCS can be a powerful advocate. The commander's buy-in is critical.
- ***Contracting Officer***—UMCS contracts can be challenging due to complex requirements and potentially burdensome contracting procedures, such as the establishment of an indefinite delivery, indefinite quantity (IDIQ) contract for system integration and support services.
- ***Major Tenants***—Facility managers of large buildings or tenant organizations on post might want to have input to UMCS planning and implementation decisions since the UMCS provides infrastructure support of their missions.
- ***Corps Area Engineer and/or Resident Engineer***
- ***Corps of Engineers District Designer***—Designs must be accomplished in accordance with the installation's UMCS master plan (assuming one exists) and requirements while working within the framework of UFGS 23 09 00 and UFGS 25 10 10. Membership in the

workgroup is optional, but communication and coordination with the Corps district is essential.

- ***External Consultants***— Open Control Systems implementation can be more challenging than proprietary procurement. For this reason, and particularly in the initial phases, it can be beneficial to obtain outside expert assistance from the following:
    - Huntsville Center UMCS Mandatory Center of Expertise
    - Huntsville Center Control System Cybersecurity Mandatory Center of Expertise
    - Engineer Research and Development Center, Construction Engineering Research Laboratory (ERDC-CERL)
    - Industry consultants may be equally valuable. However, few may have sufficient familiarity with the installation and its UMCS and BCS history and related needs and challenges. Also, few have in-depth familiarity with DoD UMCS and BCS criteria.

4.2.3 Coordination

UMCS planning and implementation must be coordinated with different entities (organizations and branches) during the various phases of implementation. These entities play critical roles in the success of the implementation effort and are described below.

4.2.3.1 DPW Design Branch and/or Plans & Programs and/or Planning Division

Local DPW design entities such as the Design Branch and/or Plans & Programs are highly enabling participants in the UMCS implementation effort. They likely have in-house template designs and specifications for UMCS technologies. They should participate in the UMCS workgroup (including master plan development), help with the UMCS design, and review any statement of work (SOW) developed as part UMCS implementation.

The local designers and specifiers should coordinate with the servicing Corps of Engineers' district office. This is likely already being done at some level in coordination with any existing project manager (PM) forwards (program management liaisons from USACE at some Army installations). A coordination goal between the local designers and the Corps district might be a set of installation specifications that can be used as a template for UMCS and BCS projects.

4.2.3.2 DPW O&M shops and O&M chief

DPW O&M shop personnel and the O&M chief should participate in the development or review of a UMCS master plan. They should also take part in the drafting or review of any SOW regarding UMCS implementation.

4.2.3.3 DPW energy manager

The energy manager should participate in the development or review of a UMCS master plan. They may also take part in the drafting or review of any SOW regarding UMCS implementation.

4.2.3.4 Corps of Engineers district

The Corps of Engineers should assist with the UMCS design. The Corps district should participate in the development or review of a UMCS master plan. They will develop SOWs for USACE projects and should be coordinated with on an ongoing basis to ensure in-house SOWs and USACE SOWs are not in conflict. The USACE district office can also be helpful because of their familiarity with the use of *SpecsIntact* software and related document files. *SpecsIntact* is used to edit UFGS files.

4.2.3.5 Network Enterprise Center

The Network Enterprise Center (NEC) typically provide the basewide transport IP network for the UMCS and, in some cases, may also host the UMCS front end applications. The NEC should participate in the development or review of a UMCS master plan. They should also take part in drafting or review of any SOW that involves IT infrastructure and cybersecurity for the UMCS implementation.

4.2.3.6 HNC and others

Other agencies, and even specific individuals, can be essential participants. One example is the Huntsville Engineering and Support Center (HNC) Mandatory Center of Expertise for UMCS. They can help with any aspect of UMCS master plan development and execution. They do so on a reimbursable basis.

4.2.4 Defining a vision for future UMCS

The workgroup should create a vision of the ideal UMCS that describes an aspirational future state of the UMCS. This vision will be a key component of the master plan for UMCS. Consider "What does a successful UMCS look like?" An example vision is the following:

> Our UMCS front end will be our primary tool for managing our HVAC systems to maintain energy efficiency, meet tenant mission requirements, address tenant issues before they rise to the level of tenant service calls, conduct proactive maintenance, and be a diagnostic tool when a service call is received.

A second example might be

> Our vision for the UMCS is to integrate all appropriate building control systems into a unified basewide system with a common operating picture to improve facility operations.

4.2.5 Understanding the current status and identifying current issues and anticipated challenges

The UMCS workgroup should discuss the current status of the UMCS and the equipment it controls at the installation. The group may decide to conduct some baseline information gathering or site surveys to better understand the present condition and use of the UMCS. All workgroup members should provide input. Contributions from an assortment of stakeholders (those impacted by workgroup decisions) and particularly DPW O&M staff are needed.

The workgroup must identify current issues that need to be resolved and anticipated obstacles in moving the installation toward the aspirational UMCS. It is important to be aware of the many factors at play in UMCS operations as they will need to be coordinated and harmonized going forward. Preliminary broad objectives and supporting goals based on these issues, as well as potential methods to address issues, may also be captured and logged for future development. This process includes creating lists of issues, goals, and obstacles. These lists do not need to be rigorously detailed but should be as comprehensive as possible since they will be an important part of the final implementation plan for the UMCS. Also, the lists help identify any “broken” policies or procedures that need to be addressed.

4.2.5.1 Common issues

It is important to identify the primary issues that exist with the current system or that the workgroup believes might exist with future system additions. This list of issues will be used to help formulate the goals for the future UMCS. Some issues commonly experienced by installations are

- ***Multiple UMCSs exist.*** In some cases, installations have made the decision to maintain multiple independent UMCSs as a means to allow competitive procurement. In other cases, multiple UMCSs are a result of the procurement of incompatible systems. In either situation, it is generally more costly to maintain and expand multiple systems than a single system (particularly for smaller installations where the burden of maintaining multiple incompatible systems will strain limited staffing resources). Multiple UMCSs generally lead to the following specific problems:
    - **Many O&M laptops that are not used.** This often occurs when systems from many manufacturers are installed, and these software tools are provided with limited training. Without training in, and frequent use of, these tools, skills deteriorate and the installation’s ability to troubleshoot and manage its systems is hampered.
    - **Too many front-end software packages.** There may be too many front-end computers when multiple UMCSs exist. Each system requires its own front-end interface, and it takes several interfaces (software packages) to monitor the entire network. An installation may find it difficult to maintain training and skills on multiple front ends, which often hampers its ability to effectively use the UMCS systems.
- ***Lack of a front end.*** At the other extreme, the installation may have no front-end computer or other operator interface at all. These systems are extremely difficult to use and maintain since it is difficult to determine what they are doing.
- ***Insufficient training.*** The O&M staff is not adequately trained on the use and operation of the system.
- ***Insufficient or superfluous UMCS features***. The UMCS includes features that are not needed and possibly confuse operators, or the

UMCS does not include features that are needed or desired by the installation (such as sufficient points to allow proper control and troubleshooting of underlying systems).

- ***Systems never worked.*** Systems are accepted even though they are not functioning properly. This is a result of poor commissioning of the systems, which in turn can be due to
    - **Time constraints**. Lack of time at the end of the project to adequately commission the systems (often due to delays earlier in the project and/or tenant-imposed deadlines for completion)
    - **Complexity of Systems.** Specification of overly complex systems (i.e., systems beyond the technical expertise of the commissioning agents to adequately evaluate)
- ***DPW not involved.*** The DPW is not involved in the acceptance process for UMCS, so there is no sense of ownership by those that will have to maintain the system.
- ***UMCS is underused.*** This usually occurs because the UMCS is not properly configured to provide useful feedback to the operators or is due to inadequate training—or in extreme cases, there are no operators. As a result, systems are generally operated in a “full manual” mode, with systems running 24/7 under fixed operating conditions. While systems operated in this manner may be configured to satisfy occupant comfort or to conserve energy, they cannot satisfy occupants *and* conserve energy.

4.2.5.2 Issue and goal identification prompts

The range of UMCS-related issues and challenges to consider is broad and includes implementation activities, staffing, training, technology capabilities and selections, existing equipment status, acceptance process, and cybersecurity. This nonexhaustive list is designed to prompt full-spectrum, thoughtful discussions to identify issues and to generate goals for an optimal UMCS:

- ***Implementation Activities***
    - **Implementation activities checklist**. Table 2. UMCS implementation planning, scoping, and coordination provides several suggested high-priority tasks. Identify issues and challenges related to the checklist items or pertinent to the local UMCS. Many of the items listed below elaborate or overlap with the implementation checklist.

- ***Staffing and Training***
    - **System support requirements**. Consider what is needed so that the UMCS and BCSs (currently and in the future) are supported, operationally and maintenance wise. This will inform staffing and training needs.
    - **Management and leadership**. Someone must manage the UMCS through its life cycle. This technical guide refers to this person as the UMCS manager, whose responsibilities are described elsewhere.
    - **Users and stake holders.** Who are they? The DPW, O&M staff, designers and specifiers? Identify and coordinate with the appropriate branches, offices, shops, and individuals. Who might, will, or should use the UMCS and how? For example, consider the need for an operator workstation in the energy manager's office, in each O&M shop or work leader's office, and in each shop common area. The UMCS must be actively used to troubleshoot, maintain, and improve facility operations. Will it be? How and by whom? Identify well-defined UMCS operator processes (as further described in Section 6).
    - **Front-end users.** Who will be the UMCS front-end users and operators? Decide who needs and will have a client UMCS workstation. Outline what the workstations will be used for and who will use them.
    - **Technical Support.** Determine what resources (both in-house and external) are available to help make technical selections and decisions.
    - **Vendors/Contractors.** Who is technically qualified to provide UMCS technology (e.g., qualified to provide BACnet, LonWorks, or Niagara systems)? Which contractors are competent? It is beneficial to know which vendors and contractors available to do work at the installation are viewed as effective and responsive by the in-house staff. A mediocre product installed by a quality contractor will likely outperform a technically superior product installed by a second-rate contractor.
    - **Training.** What training is needed? UMCS and BCS training ranging from Open Control Systems concepts to detailed DoD and Army-specific control system commissioning requirements is likely needed. These are discussed in Section

4.6. Vendor or product-specific training is also likely necessary to make the most of a specific brand of UMCS front end or BCS.

- ***UMCS technology and functions***
  - **Desired system capabilities.** What are the DPW's (and others) UMCS front end and BCS preferences, needs, and desires? For example, the front end can monitor building HVAC systems and generate alarm(s) when something is wrong, provide scheduled on or off capability for all primary equipment, and incorporate preventive maintenance features, such as pump run time monitoring. Consider details such as
    - What is the process for troubleshooting service calls?
    - Which shops and individuals should system alarms be directed to (e.g., freeze alarms, system malfunctions, etc.)?
    - What kinds of alarms are needed and useful (i.e., alarms must be reasonable and carefully selected so that the quantity of alarms does not overwhelm the operators)?
    - Which operator workstations will be used to set up and change equipment schedules, etc.?
  - **Technology options.** Investigate and identify desired UMCS technology, features, functions, capabilities, etc. as part of the planning process. Review Open Control Systems technology and communications protocols, including which of the four Open Control Systems technology options the installation should consider or pursue. Consider UMCS technology already in place at the installation that can serve as a basis for system expansion. Refer to Section 3.2. Refer to existing UMCS UFCs listed in Section 3.3. Availability of local vendor or contractor support for Open Control Systems (e.g., Niagara, BACnet, and LonWorks) is critical. What UMCS technology and functionality does the DPW want, need, or prefer?
  - **Existing front end.** Is there an existing viable UMCS front end that can be used as the basis for future growth?
  - **Front-end current use.** How is BCS and UMCS front end technology used now regarding scheduling, alarms, trends, graphics, diagnostic tool, etc.? (See Section 3, which describes typical functions). Who currently uses the existing

UMCS and how? Is it being used effectively and to its fullest capabilities?

- **Front end selection, administration, and maintenance**. Consider what manufacturer or brand of front-end M&C software the installation prefers to have basewide. This is important because the UMCS front-end software (e.g., the user interface software) will be procured from and (except for Niagara Framework) will be proprietary to a single vendor. The installation will use (and in the worst case "be stuck with") this front end indefinitely. Consider if and how the installation will procure the services of a UMCS front-end contractor to service the front end, including performing activities such as integration or connection of BCSs into the UMCS front end. This is described more in Section 4.7. Also important is determining who will manage day-to-day operation of the UMCS computer and servers, such as backups, security updates, etc. Consider the backup equipment and procedures (such as the inclusion of a mirror drive, reportedly a hard lesson learned at one installation where a disk drive failure resulted in the UMCS going down).
- **Metering.** Identify needed interaction and overlap with any energy metering work. Consider if, when, and how to tie Army Metering Program (AMP) meters or the Enterprise Energy Data Reporting System (EEDRS) to UMCS.

- ***Existing Equipment Conditions***
  - **Existing equipment condition.** What is the current state of preexisting UMCS front end and BCS infrastructure and the underlying HVAC mechanical systems? What are the good and bad things with the existing UMCS/BCS technology? For most installations, identifying existing conditions can require a significant effort since visual inspection or even performance testing many mechanical systems is almost certainly required. The planning workgroup might consider doing (at least) a mini site survey (perhaps executed by the DPW) to get a sense of what UMCS vendors, technology, and infrastructure exist on post. Consider a more extensive survey. What buildings and systems should be part of the UMCS initially and in the future?

    - **Repair and replacement needs**. Many preexisting BCS/HVAC control systems may be in desperate need of repair or replacement. These underlying systems must be in good working order for any centralized control to be useful. Consider how to prioritize/phase these repairs along with implementation/inclusion of UMCS/BCS technology, such as prioritizing mission-critical facilities and facilities with high energy costs. Consideration should be given to funding repair and replacement projects.
- ***Commissioning and System Acceptance Process***
    - **Commissioning process**. Ideally, the installation has a defined commissioning process. The UMCS workgroup should assess and, as needed, update or define a commissioning and system inspection, testing, and acceptance (system turnover) process for UMCS front end and BCS projects. This is discussed in Chapter 6.
- ***Cybersecurity***
    - **Cybersecurity.** UMCS cybersecurity requirements must be addressed and can create additional burdens on the design and DPW staff, in part, because cybersecurity is often outside the working discipline of UMCS implementers and owners. Resources for understanding and dealing with the Risk Management Framework along with Army staff who specialize in this, such as at the MCX for cybersecurity, are available.
- ***Miscellaneous***
    - **Procurement**. What is the procurement methodology, funding, and timetable to move forward? In particular, as the UMCS grows, how will new buildings be added to the existing UMCS?
    - **Documentation needs.** What supporting documentation needs to be developed? How will systems be specified (e.g., an in-house developed specification)? Will there be an installation design guide (IDG) that provides specific requirements?
    - **Future plans**. What are the long-range plans for the installation? What are plans for growth? Who are the existing and future tenants, and what are their mission requirements?
    - **Documentation management.** Who will generate construction documents? Where will they be stored? How will

they be accessible to interested parties over time? How will they be kept current over time?

4.2.6 Charting a path forward

With a vision for the desired future state of the UMCS, and an understanding of the current status of the present UMCS and its operational environment, the workgroup should chart a path forward for UMCS activities. The workgroup should create a long-term plan and direction for the installation to successfully procure, install, operate, maintain, and sustain the UMCS. A set of broad objectives, supporting goals, and detailed tasks should be developed to move the UMCS toward the desired future state vision. Supporting goals are best is they are SMART (specific, measurable, achievable, realistic, and time bound). Table 2 and Section 4.2.5 can serve as a detailed guide of considerations to chart a course of action. Some example objectives, goals, and tasks might be

- ***Long term objective:*** The UMCS will be established, fully functioning, used, maintained, and sustained.
- ***Goal:*** The UMCS will have sufficient and effective staff.
- ***Task:*** Characterize staffing needs for UMCS front-end operators
- ***Task:*** Identify training needs and sources for UMCS front-end operators.
- ***Task:*** Identify costs, budgets, and funding sources for UMCS front-end operator staff.

After identifying the objectives, goals, and tasks, the workgroup may choose to identify and rank their relative importance and set timeframes for accomplishing them. Many objectives will require multiple paths and attempts to achieve success. Consideration of local obstacles and approaches to obstacle resolution can aid in objective attainment.

4.2.6.1 Common obstacles

The UMCS workgroup should identify obstacles that might impact their ability to realize those goals. Some common obstacles are

- ***Lack of Cooperation between Groups.*** It is essential that the assorted stakeholders are kept apprised of the goals and activities of groups outside their primary influence, and potential areas of conflict between groups are addressed calmly and collaboratively.

- ***Lack of Technical Resources.*** Insufficient expertise within the DPW staff or otherwise available to enable the installation to operate and maintain the system will prevent goal attainment. In particular, there needs to be a long-term commitment of personnel to support and maintain the system.
- ***Lack of Commitment from Management.*** Management must make a long-term commitment to establishing a UMCS that meets the workgroup's established goals.
- ***Training Limitations***. To properly operate and maintain the system may require significant training. The amount of training time and funds available may impact the ability to train DPW staff to operate and maintain the system.
- ***Lack of User Buy-in and Support***. The users (the DPW and maintenance staff) must buy-in to the system and support it for the workgroup's established goals to be met.
- ***Cost.*** Systems meeting the implementation plan defined by the workgroup may be more costly than other alternatives in the short term, but having a single coherent and working system will prove beneficial in the long term and meet the Army's strategic goals. If cost is the determining factor in awarding future construction, systems that are incompatible may be procured (e.g., if a contractor submits a "value engineering" proposal and it is awarded).

4.2.6.2 Approaches to obstacle resolution

Once the workgroup has identified obstacles that may hamper the execution of the plan, it should identify an approach to addressing these obstacles. In general, the obstacles will fit one of three categories:

1. ***Fixable.*** These are obstacles that the workgroup can eliminate such as policies that the workgroup can change (or get someone to change) or management buy-in that the workgroup can obtain.
2. ***Addressable***. These are obstacles that the workgroup cannot change; however, they can work around the obstacles (or mitigate their impact) in some fashion, such as by obtaining exceptions from policy or by including specific requirements to be met by the system.
3. ***Unavoidable***. These are obstacles that the workgroup cannot change or work around and must avoid. Policies that do not offer exceptions or hard limits on funding are two examples. The workgroup should identify the appropriate actions to remove, modify, or avoid "fixable" and "addressable"

obstacles and begin to resolve these issues. “Unavoidable” obstacles should be carefully documented and a means to avoid them should be identified.

4.3 Design guidance

The UMCS workgroup in coordination with the DPW and others should identify and gather (and in some cases develop) design and specification guidance policy, sources, methods, and considerations for the UMCS front end and BCSs, such as

- UMCS Master Plan
- ASA-IEE BAS Implementation Policy
- DSC-G9 BAS Implementation Guidance
- Installation Design Guide (IDG)
- In-house (DPW) Specs, Unified Facilities Guide Specifications (UFGSs), and Unified Facilities Criteria (UFC) for UMCS and BCS as described in Section 3.3
- Design Coordination Checklists—Specification Preferences
- Points Schedules and Points Schedule Management
- Point Naming Convention
- Other Documents that describe installation or DPW preferences

Details on the above design guidance items are described below.

The UMCS Master Plan. The UMCS master plan developed by the UMCS workgroup will contain information needed by the designer or specifier, such as the protocol option selected by the workgroup. The plan might duplicate or include some of the items listed below, such as the IDG. This is a living document and will evolve over the life of the UMCS.

ASA-IEE BAS Implementation Policy. The ASA-IEE BAS implementation policy was described in Section 1.1. It calls for UMCS implementation where cost effective.

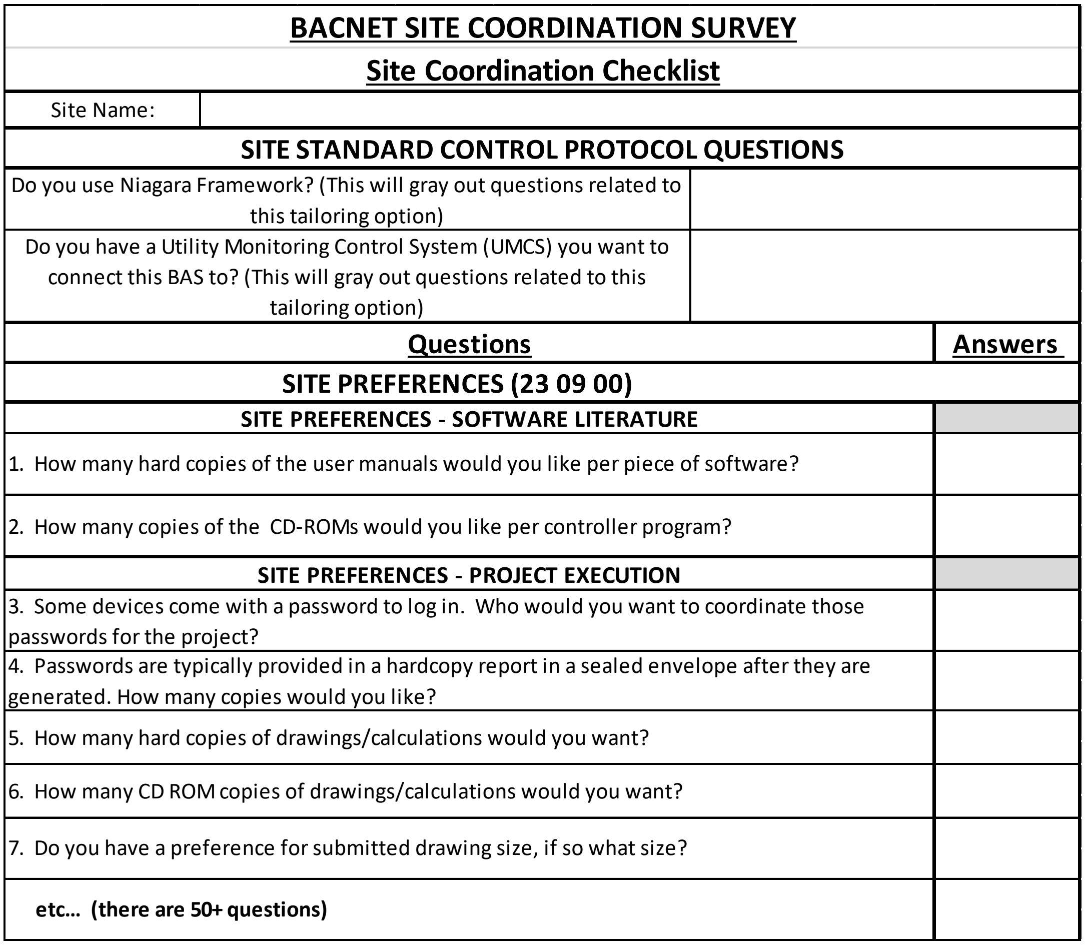
DSC-G9 BAS Implementation Guidance. The DSC-G9 BAS implementation guidance was described in Section 1.1. It establishes multileveled Army engagement on UMCS and provides direction on economic analysis, system design, and cybersecurity.

The Installation Design Guide (IDG). The IDG may contain UMCS and BCS requirements and preferences. Ideally, the UMCS workgroup will update (or create) the installation-level IDG to include applicable elements of the UMCS master plan. The intent of the IDG and its UMCS and BCS content is to provide a big picture vision but also provide at least a general direction to a contractor performing minor repair or upgrade work, especially in the absence of a detailed specification.

In-House (DPW) Specs and UFGS/UFCs for UMCS Front End and for Building Control Systems. In-house (DPW) specs and UFGS/UFCs for UMCS front end and for building control systems were described in Section 3.3. In addition to being used by the local USACE district for military construction projects, these documents can become the basis to help define requirements for in-house projects. The UFGS are in *SpecsIntact* format (an automated system for preparing standardized facility construction specifications), but some installations have used the content of the UFGS to develop in-house specs.

Design Coordination Checklists for Specification Preferences. The DoD UFGSs, used by the local USACE district to specify a UMCS and BCSs, contain a multitude of bracketed options where the designer or specifier makes selections amongst the bracketed options contained in the UFGS. A review of the bracketed options contained in the UFGSs can help identify DPW preferences and requirements for the installation's UMCS and BCSs and ultimately lead to specifications tailored to the local site and project needs. One way to facilitate a review of the bracketed options is to have someone (often the UMCS workgroup) go through the UFGS and excerpt each bracketed option into a succinct list to help facilitate DPW or workgroup preferences and selections, which can include high-level selections, such as the choice between the LonWorks or BACnet protocols and technologies, in addition to finer details, such as whether or not temperature controllers should be provided with hand-off-auto (manual or automatic control) switches. Designer coordination checklists are available at: https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-3-410-02. Figure 13 is a screenshot of a partial checklist.

Figure 13. Site coordination survey—for control system specs (partial screenshot).



BACNET SITE COORDINATION SURVEY

Site Coordination Checklist

Site Name:	

SITE STANDARD CONTROL PROTOCOL QUESTIONS

Do you use Niagara Framework? (This will gray out questions related to this tailoring option)	
Do you have a Utility Monitoring Control System (UMCS) you want to connect this BAS to? (This will gray out questions related to this tailoring option)	

Questions	Answers
SITE PREFERENCES (23 09 00)	
SITE PREFERENCES - SOFTWARE LITERATURE	
1. How many hard copies of the user manuals would you like per piece of software?	
2. How many copies of the CD-ROMs would you like per controller program?	
SITE PREFERENCES - PROJECT EXECUTION	
3. Some devices come with a password to log in. Who would you want to coordinate those passwords for the project?	
4. Passwords are typically provided in a hardcopy report in a sealed envelope after they are generated. How many copies would you like?	
5. How many hard copies of drawings/calculations would you want?	
6. How many CD ROM copies of drawings/calculations would you want?	
7. Do you have a preference for submitted drawing size, if so what size?	
etc... (there are 50+ questions)	

Points Schedules and Points Schedule Management. Under the current DoD UFGS procurement specifications, the absolutely most important project-specific document is the Points Schedule. The installation should require, enforce, and manage the use of Points Schedules on all projects. This document exists through the life of a project and goes through the following steps:

1. The designer develops the initial version, which defines the hardware points in the system. This document becomes part of the system definition in the contract package.
2. The installing contractor uses the Points Schedule as a system requirements document. As they install the system, they fill out additional columns on the Points Schedule and then submit this to the Government.
3. The Government uses and verifies the Points Schedule during commissioning to ensure that the installing contractor has met the requirements of the project.

4. When it is desired to integrate the completed BCS to a UMCS, the Government uses the Points Schedule (submittal from the BCS contractor) as a contract document to both provide information to the integration contractor and to define integration requirements.
5. The integration contractor uses the information in the Points Schedule to define the integration requirements and then fills out additional fields on the Points Schedule and submits it to the Government.
6. The Government uses and verifies the Points Schedule during commissioning to ensure that the integration contractor has met the requirements of the project.
7. The final accepted Points Schedule becomes a key document for the O&M staff in describing the system.

Point Naming Convention. A standard or well-defined point naming convention is an important procurement requirement, particularly in a multivendor system. At the very least, the naming convention used for identical points (e.g., supply air temperature) should be the same on graphics pages across all systems, regardless of the installing vendor or contractor. A more comprehensive approach—again, particularly in a multivendor system—is to have point names at all levels of the system (not just on the graphic) adhere to a well-defined convention. For example, in addition to the supply air temperature being labeled SA-T on a graphic, the actual analog input in the hardware field controller should also be named SA-T in that controller, not AI-15, Pt27, or some other cryptic reference.

In the past, it was difficult to standardize a naming convention as many vendors were limited in their ability to support reasonable-length names in their hardware, but this is no longer the case. An excellent reference for a point naming convention is Appendix E of UFC 3-410-02 (DoD 2018a). The specific names in the UFC are HVAC specific, but the convention outlined could easily be used for other systems.

In addition to point names as defined in the UFC, there should be a requirement for fully qualified point names at the front-end computer or server. The point naming convention in the UFC describes the convention for a point within a specific mechanical system (e.g., an air handling unit [AHU]), whereas a fully qualified point name would provide a unique name for all points across the entire UMCS. So, while SA-T is a unique name within, say, AHU-5, AHU-6 probably also contains a point SA-T. What is needed is a way to distinguish those two SA-T points. One possible approach is to prefix additional information to the point name, such as <Building>/<System>/<PointName>. In the above example, one point might be BLDG_1023/AHU-5/SA-T, and the other BLDG_1023/AHU-6/SA-T. This requirement should not be required at the field controller (since the field controller is already, by definition, dedicated to AHU-5 in building 1023) but should only be required at the front end.

The installation should consider requiring the use of the point naming convention in UFC 3-410-02 on all projects and should extend that to fully qualified point names as described above. Exceptions could be granted in the rare case where no appropriate standard point name exists.

Other Documentation/Training. Other documents might include a description of current DPW UMCS (including BCS) training needs and requirements, which can be used as a guide for defining and developing specification requirements and contractor-supplied training agendas. The intent is to help identify and meet immediate specific training requirements and needs since training requirements can change rapidly (e.g., due to DPW new hires) and are hard to anticipate. Meeting these needs might be as straight forward as UMCS manager involvement in the review and approval of contractor-supplied training agendas, assuming the UMCS manager has sufficient familiarity with the training needs of the targeted trainees. It might also necessitate carefully crafted specification language specific to DPW needs.

4.4 Cybersecurity

Cybersecurity is a critical consideration and is discussed in detail in Section 8 but is mentioned here because it is an important part of UMCS planning. It is important to engage with the NEC early and consider cybersecurity as part of UMCS planning (and sustainment).

4.5 Staffing

UMCS staffing is a critical consideration and is discussed in detail in Section 7.2 but is mentioned here because it is an important part of UMCS planning.

In summary, UMCS staffing roles and responsibilities include the UMCS manager, UMCS (IT) administrator, system integrator (on-staff), system integrator (project-specific), energy manager, UMCS operators, controls technicians, HVAC mechanics, and technical experts. Other staffing roles, such as an HVAC-specific mechanical engineer, are described in Section 7.2.

The UMCS workgroup should consider, What staffing resources are available? How many staff are needed? How many people are available, and what is their level of training? Should the staff be Government or contractor? Are there options to add staff? How much flexibility is there in staffing? Personnel constraints may require contracting out UMCS roles (staffing) that are not inherently Governmental (e.g., technicians, programmers, or system integrator). External assistance and resources should also be considered. The planning workgroup is advised to discuss staffing with the O&M chief and/or director of DPW.

4.6 Training

UMCS and BCS training needs should be identified for designers, specifiers, O&M staff, system operators, and others who will use the UMCS.

O&M staff and system operators are targeted in the UMCS and BCS UFGSs, where the installing contractor is required to provide training. Although the intent of the training requirements in the specifications is to achieve a degree of proficiency in system operation and maintenance, it should not be assumed that this training is sufficient. Individual installations and staff members may have specific training needs. The training requirements in these specifications can be edited to meet specific needs. Beyond this, it is likely that a degree of formal and specialized training will be needed to meet the complex demands of microprocessor-based controls including UMCS and BCS hardware and software. Possible training options include the following:

1. ***Vendor-Specific DDC Guide Spec Training.*** Most construction contracts, specifically those that originate at the Corps district level, include contractor-provided training requirements. UMCS workgroup and O&M staff should review and help edit the training requirements and specs during the design phase.
2. ***Vendor-Specific UMCS Guide Spec Training.*** The contractor-provided training on the UMCS front-end M&C software is extensive and specified in the UFGS in great detail. Still, additional training may be warranted depending on the extent that the system operator(s) will be involved with the operation and management of the UMCS. Individuals that

will perform system integration functions should receive formal vendor training, such as that offered at the vendor's formal training facility.

3. ***Proponent Sponsored Engineer Corps Training (PROSPECT).*** Training is available from the USACE Learning Center. This includes course 340, "HVAC Control Systems Design and Quality Verification," which provides instruction on BACnet, LonWorks, and Niagara Framework technologies along with control systems specific to the requirements in the BCS and UMCS guide specs. Although designers and quality verification staff are targeted, O&M staff would also benefit from this course. The course schedule is available from the "USACE Learning Center."
4. ***Vendor Training.*** Most UMCS and BCS system manufacturers offer product-specific training at the manufacturer's formal training facility. This type of training can provide in-depth familiarity with specific products, including software tools such as the configuration and programming tools and the UMCS M&C software.

4.7 System integration

4.7.1 Background and considerations

System integration consists of connecting one or more BCSs to the UMCS front end and configuring the front-end M&C software to perform supervisory monitoring and supervisory control of the connected BCS(s).

System integration must be planned. This should be done while considering the procurement and funding mechanisms discussed in Sections 5.4 and 5.5. This is important because following the initial procurement of the UMCS front end, the addition, expansion, or upgrade of any subsequent BCS ordinarily will require integrating these BCSs into the existing UMCS front end. An existing UMCS front end will be vendor specific and, therefore, will require a prenegotiated contractual relationship with the front-end vendor. Niagara Framework may be an exception because of its open licensing arrangement (described previously), which means any Niagara BCS contractor can potentially also provide front-end integration services.

This suggests a potential significant benefit with the Niagara Framework approach in that it can eliminate a potentially time-consuming and costly contracting step. Another benefit is the transition (i.e., handoff) from performing BCS activities to performing system integration activities is potentially smoother. A disadvantage is that with more than one BCS contractor performing SI services there may be some inconsistency in the look, feel, and possibly performance of the front end. One example is graphics created by one BCS/SI contractor are likely to be different than those created by another.

4.7.2 Non-Niagara Framework systems

The discussion in the rest of this Section pertains especially to non-Niagara Framework UMCS and BCS. That said, at least portions of the subsequent content can apply to a Niagara Framework system, but keep in mind the distinction between Niagara and non-Niagara systems described in Section 4.7.1 above and differences in execution covered in Section 5.6.

The Open Control Systems technology specified in UFGS 25 10 10 and UFGSs 23 09 23.01 and 23 09 23.02 provides some flexibility in contracting systems integration along with protection against being locked in to a specific company or individual. Should the need arise, the UMCS front end can be replaced without replacing the database or any of the building-level systems installed under UFGS 23 09 23. Replacing the UMCS front end, however, requires not only the procurement of new software but the labor to set the new M&C software to replace the old UMCS and, thus, should be avoided when possible.

There are two main issues to be considered:

- UMCS work is an ongoing process. While the UMCS front end is procured once, building integration to the UMCS is a process that can span many years over the entire life of the UMCS. The question of how to accomplish future integration work should be addressed during initial system design as summarized above. As an extreme worst-case example, there are small controls software vendors that can install a custom UMCS front end that they developed themselves. However, use of such a UMCS essentially guarantees that future integration work will have to be performed by the developing shop.
- Contractually, it might be easiest to procure the initial UMCS front end from a BCS contractor as part of a building-level controls project. The danger in this approach is that allowing the same contractor to install both requires extra vigilance on the part of the Government to ensure that the interface between the UMCS front end and the building is fully compliant with UMCS UFGS 25 10 10 (the Niagara Framework is an exception as described above). As an extreme case, the contractor might install a UMCS that works fine with the contractor's controls but

will not work with other building control systems that are compliant with the DoD specifications.

4.7.3 System integration approaches

A system integration approach should be identified as early in the planning and implementation process as possible particularly in the case of a non-Niagara Framework system. Ideally, the approach is chosen well before UMCS front end procurement so that as new BCSs are competitively procured there is a plan in place to integrate them into the basewide UMCS. Although the UMCS front end may be procured separately from system integration services, the approach used to obtain system integration services can greatly impact the procurement of the UMCS front end. This is particularly true if some type of long-term contracting mechanism will be used for both the initial UMCS front end procurement and subsequent system integration services. As discussed previously, the Niagara Framework open systems licensing can simplify system integration because it allows the BCS contractor to perform system integration.

Ideally, the installation will have a specific individual responsible for the integration of all new buildings into the UMCS. This person—the SI—will be familiar with the system and the procedures for integration and would, therefore, be able to efficiently integrate new buildings. While it may be possible to get near this ideal through a long-term contract of some sort, it is not always feasible (in which case, the integration may have to be performed on a case-by-case basis).

The following sections describe system integration approaches, as listed in Table 3, which are largely for non-Niagara systems, and include:

- In-House SI
- Long Term Contract for System Integration
- Case-by-Case Integration (Using separate dedicated contracts)
- Case-by-Case (Using a combined building contract and integration services)

Table 3. Possible integration approaches and associated contracting mechanisms.

		System Integration Approach			
		In House	Long-Term Contract	Case-by-Case Separate Contractor	Case-by-Case, Building Contractor
Contracting Mechanism	Local office	Yes	Maybe[*]	Yes	Unlikely[†]
	ESPC/UESC[‡]	Yes	No	No	No
	District IDIQ	No	Yes	Yes	No
	Center IDIQ	No	Yes	Yes	No
	District MILCON	No	No[§]	No[**]	Yes

4.7.3.1 *In-house system integrator*

The preferred approach to meeting system integration needs is for the installation to train, hire, or contract for an in-house SI. By having the SI on staff, the installation benefits from maximum flexibility in the use of the SI. The installation does not have to issue task orders or a new contract to get systems integrated and can benefit from ongoing system maintenance. Contracting approaches that fit this category include

- Hiring or training a Government employee. This is becoming less probable an option due to staffing shortfalls and the trend towards staff reductions.
- Hiring a contractor through an existing services contract
- Establishing a service contract
- Obtaining services though another mechanism—such as an ESPC. Since an ESPC contract is generally for a long period and generally includes more than system integration service, caution should be exercised with this approach to be sure the installation will be able to effectively work with the ESPC contractor.

A key aspect of the in-house SI approach is that the system integration services are provided at a fixed cost. However, it is important to realize that this fixed cost generally equates to a certain number of person-hours, so the amount of time it takes to integrate a building and the number of

[*] Be cautious as the installation contracting office may be resistant to this type of contract.

[†] The building contract is usually awarded by a Corps district not the local contracting office.

[‡] Energy savings performance contract/utility energy services contract

[§] Via MIPR of funds from the Corps district to Huntsville Engineering and Support Center to award

[**] This mechanism cannot be funded as part of the district-awarded MILCON job, but the Corps district can MIPR funds to be used by one of the other methods.

buildings that can be integrated will depend on the SI’s workload. The purchase of products needed to perform the integration is still dependent on the buildings that are integrated, but this amount is small.

4.7.3.2 Long-term contract

With the long-term contract approach, the installation establishes an IDIQ or similar contract with an SI. This approach allows the installation to obtain integration services from the same entity as each new building system is installed but will generally require issuing task orders for the integration, which may take additional time. A key aspect of this is to obtain uniform pricing per system for the integration. For example, UFGS 23 09 93 contains sequences of operation for many defined HVAC control systems. The IDIQ contract should specify pricing for integrating these defined systems. An ESPC or utility energy services contract (UESC) are not an applicable contracting mechanism for the long-term contract approach (shown in Table 3) because system integration services are line-item tasks not typically included in these types of contracts.

4.7.3.3 Case-by-case integration (using separate dedicated contract)

With the case-by-case integration (using a separate dedicated contract) approach, whenever a new building is procured, a separate specification for integration of the building to the UMCS is issued. Maintaining this as a separate contract (rather than including it with the building control system specification) reduces the competitive advantage that could be generated by combining the two tasks (see Section 4.7.3.4 below). Since the original installer of the UMCS will be most familiar with the system, they may, in practice, have a small advantage in winning the integration contract, but this is a small task dollarwise compared with the building control system. However, anyone familiar with the UMCS software can perform this integration, so proprietary procurement can be avoided. Note that for many vendors’ systems there may not be other contractors qualified to work on the system. In this approach, tasks other than integration, such as system upgrades and maintenance, need to be accomplished under a separate contract. As in the combined building and integration contract, if the integration contract is awarded to the building control system contractor, extra care needs to be taken to ensure that the building contractor does not cut costs by omitting some of the necessary requirements for an Open Control Systems in the integration.

Ideally, the agency issuing the contract to install a building system will set aside funds to pay for integration services. For example, if the USACE district awards a MILCON project for a building control system, and the installation has an IDIQ contract in place for SI services, the district can MIPR funds to the installation to award an integration task on the IDIQ. A drawback to this process is that the administrative cost of issuing the contract (or IDIQ task) can be high and, therefore, is best used where multiple buildings are to be integrated. Plus, the process assumes that there is an IDIQ contract in place and available for use.

4.7.3.4 Case-by-case (using combined building contract and integration services)

With the case-by-case (using combined building contract and integration services) approach, the integration of the building into the UMCS is included in the building controls system specification contract; a single contractor performs both tasks. This can give a competitive advantage to the original UMCS installer or manufacturer since they will generally be able to integrate the building more inexpensively than could the competition. This can be particularly problematic when the contractor cut costs by omitting some of the necessary requirements for an Open Control Systems or provides value engineering to reduce the level of openness in the building control system since an open building (necessary for integration when the contracts are separate) is typically more costly than a closed building. While this is less of a problem with the “case-by-case integration using a separate dedicate contract” approach, it may become problematic when the contracts are combined because this advantage depends not only on the integration but also on the building control system, which can be a large (i.e., costly) project. This is the least desirable approach and is discouraged.

4.7.4 Integrating existing systems

Prior to integrating existing systems (typically legacy but might also include systems not meeting UFGS 23 09 *xx* series guide specifications), it will often be necessary to survey those systems to identify what control system is in place and the state of the control system (how well it is or is not functioning). If a system is not fully functioning, it may be necessary to repair the system before integration.

4.8 Site survey

A site survey should be performed to help the workgroup make informed decisions and, ideally, should be done as part of initial development of the master plan. Appendix C contains a scope of work for a site survey focusing on the following elements:

- ***Building List*** that prioritizes buildings to include as part of a basewide UMCS and the approximate number of systems, which can be used to estimate the total number of points (for UMCS licensing purposes)
- ***UMCS Front End(s)***, including those that preexist and are candidates to be the basewide front end
- ***Documentation and Policies*** that preexist that may be applicable to UMCS and building control system planning and guidance

The most significant part of the site survey is likely to be the building list of prioritized buildings that might become part of a basewide UMCS. The building survey is not intended to be a comprehensive assessment that delves deeply into the condition of the buildings or its control systems in sufficient detail to award individual repair and upgrade contracts. But at least general observations regarding the building and control system condition are needed in order to help prioritize. Some building prioritization categories contained in the SOW are

- Building end use activity and size (floor area, ft^2) of each building
- HVAC metrics (i.e., type, quantity of AHUs, boilers, and chillers) with a point count estimate plus an estimate of the number of alarms, trends, and occupancy schedules required for the installation as may be necessary to meet licensing requirements for the front-end M&C software. Note that the Points Schedules associated with UFGS 23 09 93 can be very useful in estimating these numbers.
- Estimated energy consumption of the building
- Fuel sources used by each building including the associated energy prices
- Mechanical system(s) and control system(s) condition. A numeric rating (e.g., 1–10) of the suitability of the system for integration based on the judgement defined by the contractor to account for condition, age, and modernity of the controls and the HVAC system. The condition as-

sessment should include the numeric readiness score and a brief commentary concerning whether or not to incorporate the system into a basewide UMCS.
- Control system(s) technology—pneumatic, electric, or DDC. For DDC, the manufacturer/brand(s) and communications protocol/technology used (e.g., proprietary, BACnet, LonWorks, or Niagara Framework) should be noted.

Certain buildings should be excluded from the survey, such as housing, nonpermanent structures, and buildings or structures with no heating or cooling.

4.9 UMCS master plan

A UMCS master plan should be created. This should be a living document and evolve over the life of the UMCS. It can be complex and detailed, so it might be best to start with a draft to identify, outline, and briefly describe important content, chapters, elements, and issues based on the content of this section and other applicable content in this technical guide.

The plan could potentially be developed by or with assistance from a contractor, perhaps as part of a site survey. It is recommended that the plan be coordinated with the installation master plan. Possible UMCS master plan content includes the following:

- Background, overview, recommendations, and executive summary
- Stakeholders, reviewers, consultants, and plan developers or workgroup
- Plan execution and schedule
- Vision, status, objectives, and goals
- UMCS overview and UMCS technology description
- Preexisting UMCS/BCS, protocols, hardware, and software
- UMCS technology functions and features (needs and preferences)
- Scope, site map and list of buildings, and systems to consider and include
- Issues and challenges
- Staffing and training
- Design guidance, including sources and methods for design, development and use of in-house (DPW) UMCS and BCS specifications, and Open Control Systems technology options and selection

- System integration, including process, requirements, and contracting and execution approach
- Commissioning, including inspection, testing, and system acceptance process
- Cybersecurity, including, but not limited to, the process for adding new connections to the UMCS
- Funding and resource information, including budget and costs.
- Site survey (Section 4.8)

Based on the results of a site survey (Section 4.8) and the installation master plan, the UMCS master plan should contain planning details, such as

- Year-by-year list of buildings and systems to be integrated to UMCS
- Year-by-year list of renovations of existing systems on UMCS
- Budget estimates for the above
- Staffing needs

The plan should be reviewed by the workgroup and coordinated with any other individuals or offices and agencies who will be affected by it. Appendix K contains an example plan.

5 UMCS Procurement

Procurement processes used by the Army can be difficult to navigate and use for both the initial UMCS implementation and (more importantly) the growth of the UMCS. The nature of Army installations and the overall construction process means that installations do not procure and install an entire (basewide) UMCS as a single project; instead, they organically grow a UMCS by procuring parts and pieces over time. Starting with a core nucleus of a UMCS front end and a few building control systems, building control systems are added as individual buildings are built or renovated. Growth of the UMCS should be driven by the UMCS master plan.

“WAR STORY”

Installation X received two prices for an HVAC renovation project:

- *~$320K from the existing proprietary UMCS contractor*
- *~$45K from a competitor*

Puzzled by the price from the UMCS contractor, the USACE area engineer dug deeper and discovered, amongst other things, it included the purchase of a pickup truck. When confronted, the contractor said something to the effect of “that’s just what it costs for us to continue to support the installation. . . . you can go elsewhere, but I do not know how well we’ll be able to continue to support your UMCS.” ***The contractor actually expected the Army would pay nearly eight times as much because the Army was “locked in” to the UMCS contractor’s proprietary system.***

A considered procurement approach along with Open Control Systems technology, inherent to the DoD UMCS technology, is necessary to help avoid sole-source proprietary procurement. Without an Open Control Systems approach, new building control systems are interoperable with an existing UMCS only if the new BCS is from the same vendor as the existing UMCS. A major driver behind the current DoD Open Control Systems requirements and associated contracting approach is to avoid having to return to the same vendor and, instead, allow for open competition between vendors.

5.1 Budget and costs

For planning and budgeting purposes this Section describes approximate costs for UMCS and BCS procurement and integration. Every system and location is different; therefore, the cost to implement a UMCS can vary. The costs do not include contract administration.

5.1.1 UMCS front end

The installed cost for a UMCS front end is approximately $75,000 and is based on an existing BCS already fielded at the building level and includes the purchase and setup of a new server. This includes the software, hardware, and licensing required for the front-end server. This does not include RMF accreditation.

5.1.2 UMCS integration

The integration of a new BCS into a UMCS front end can range from $500 to $3,000 per unit (e.g., built-up AHU terminal unit, packaged unit, chiller, or boiler) and depends on the size and complexity of the units. For a typical 30,000 ft^2 building, the cost can range from $10,000 to $25,000. An alternate related budgetary metric is $0.50 to $1 per square foot depending on the complexity of the building or systems.

5.1.3 Building control system

BCS installation cost can range from $2.50 to $7.50 per square foot building floor area and depends on control system complexity. Installation cost includes sensors, actuators, controllers, cabling or wiring, and raceway as required per code along with installation and programming. It does not include additional security requirements or mechanical equipment.

5.1.4 Risk Management Framework

RMF for cybersecurity of a UMCS is $250K, according to *Army Facility Investment Guidance (FIG)* for MILCON planning, (DA 2021). Anecdotal experience suggests the MILCON cost estimate is conservative.

5.2 Initial implementation and procurement of UMCS

The procurement order described below is a rough order that conveys the intent, but the order can vary.

The current approach, inherent to the current UMCS-related UFGS and UFC criteria, acknowledges that most installations would like a single system with a single front end (useable by multiple simultaneous operators, not literally a single screen limited to one user) connected to most (or ideally all) of their BCSs. While no installation has achieved this, there are vastly more connected buildings than there are systems, which is a good trend. Additionally, the sheer size of these systems (based on the number of connected buildings) makes it highly unlikely that any given installation will be able to—in a single project—install a complete basewide UMCS. In almost all cases, it is essential that an existing UMCS be expandable by the addition of more BCS that are procured as part of a later project. A large part of the existing suite of UFGSs is designed to support this approach of

- Installing a single UMCS, consisting of a front end and a small nucleus of connected BCS, and overtime,
- Growing the UMCS by installing new BCSs and integrating (i.e., connecting) those systems to the existing UMCS.

The goal of the current set of UMCS and BCS UFGS is to deliver a system that

- Is Government-owned and not dependent on one contractor
- Consists of multivendor devices that can communicate and therefore interoperate
- Any qualified entity can readily operate, modify, or upgrade the system
- Devices can be replaced with different vendor devices
- Is the opposite of a closed or proprietary system
- Integrates all buildings into a common front end

5.3 Extent of system procurement

When first installed, the new UMCS front end may be connected only to the new BCS(s) procured at the same time, may be integrated to existing buildings, or both.

Depending on what systems the installation has, the establishment of a basewide UMCS can be as small of a project as the procurement of a new front end connected to just a few buildings, or as large as the procurement of many new BCSs all connected together to a common front end.

The process used to procure the system and the applicable funding source will be impacted by the scope of the work. For example, MILCON funds will likely be easier to use when a new front end is procured along with a new BCS rather than trying to procure a new front end only.

5.4 Funding mechanisms

There are multiple ways to fund the implementation of a UMCS: MILCON, sustainment, restoration and modernization (SRM), ESPC (or other third-party financing), or as part of the DoD's Environmental Security Technology Certification Program (ESTCP) or similar demonstration. Procurement via MILCON will generally entail procuring the front end as part of a project procuring multiple new BCSs. The other three funding sources may support the procurement of a new UMCS front end connected to only existing systems.

A brief description of the typical approaches used by installations to meet their respective UMCS acquisition needs is as follows:

- ***Military Construction (MILCON):*** as part of new military construction or major renovation project, HVAC controls and UMCS integration into existing basewide front ends should occur. A specific type of MILCON appropriation, the Energy Resilience and Conservation Investment Program (ERCIP) is also available to support the installation's strategy to enhance their UMCS capability. ERCIP is a subsection of the Defense-wide MILCON Program specifically intended to fund projects that save energy and water, reduce DoD's energy costs, improve energy resilience and security, and contribute to mission assurance. ERCIP projects are allocated across two categories: energy conservation (renewable energy, energy efficiency, and water conservation) and energy resilience and energy security.
- ***Facilities Sustainment, Restoration and Modernization (SRM):*** provides funds to keep the installation's inventory of facilities in good working order, (i.e., day-to-day maintenance requirements). In addition, it provides resources to restore facilities whose age is excessive or have been damaged by fire, accident, or natural disasters, and to alter facilities to implement new or higher standards to accommodate new functions or missions. Most installations use SRM funding to execute their respective UMCS repair or upgrade, or otherwise, retrofit failed (including technologically obsolete) building controls system projects.

    - Base Operations and Support (BOS): SRM funding also accommodates most BOS activities on the installation. BOS funds are not appropriate for construction or major repair tasks; however, they may be a viable option for procuring report services related to the UMCS assessment, planning, or inventory.
    - Third-Party Financing: Another option that is available to the installation is the use of third-party financing to support their energy strategy initiatives. The use of the various third-party-financed programs can be leveraged to implement energy conservations measures (ECMs). UESCs and ESPCs are the two primary third-party financing mechanisms.
        - UESCs are limited-source contracts between the installation and its serving utility for energy- and water-efficiency improvements and demand-reduction services.
        - ESPCs contracts are a partnership between the installation and an energy service company (ESCO)

Third-party-financed contracts are innovative arrangements for designing, installing, and financing energy improvement projects where the savings achieved by the project are intended to provide a return on investment over the term of the agreement. UESCs and ESPCs are typically long-term agreements (10+ years) and are adaptable to site-specific needs

5.5 Procurement mechanisms

Most BCS installation work is procured via either in-house work or Huntsville IDIQ, followed by mechanisms used as part of third-party procurement. Very few installations use USACE district contracts for BCS installation.

Local mechanisms for UMCS procurement and repair include

- In-house HVAC controls technicians or DPW maintenance staff can encounter repairs that require purchase of parts or subsystems that involve or impact connectivity of a BCS to the UMCS. This might require small purchases or even a larger procurement to replace a DDC controller or an entire package unit that comes bundled with DDC hardware. In either case, the controls need to be connected to the control network. This might be accomplished by the DPW staff with a credit card purchase or might require in-house contracting services. Minimally, a working understanding by the DPW of the task at hand and possibly detailed specifications may be required.

- Base operations (BASEOPS) O&M-contracted technicians
- BOS-funded service contractors
- Job order contract (JOC) contractors
- Mission Installation Contracting Command (MICC) contracts (8A, open procurement, etc.)

Other mechanisms (locally accessible) for UMCS/BCS support include the following:

- USACE district contract, IDIQ
- US Army Huntsville Engineering and Support Center has a number of single and multiple award task order (SATOC, MATOC) contracts available for use by installations. This includes assistance with development of a UMCS master plan and system integration services. System integration services include procurement such as that available as a task order on a MATOC, where the DPW might want to integrate buildings installed under or subsequent to a MILCON project. While requirements of these SATOC/MATOC contracts do not support the approach recommended in this technical guide, the fact remains that Huntsville has a great deal of contracting expertise that could likely be leveraged for future IMCOM-wide contracting efforts. Huntsville also has maintenance and services (M&S) contracts available to support ongoing management, operation, and cybersecurity of installation UMCS.

5.6 Execute procurement

5.6.1 Non-Niagara Framework

The typical approach (for a non-Niagara Framework system) has three distinct steps:

1. ***Initial UMCS (Front End) Procurement***

The installation procures a single UMCS front end. The installation selects a UMCS technology from one of the following options: ANSI 709.1. (LonWorks) using LonWorks Network Services, ASHRAE-135 (BACnet), or Niagara Framework. While in theory the UMCS front end could be procured in isolation, in general it is obtained as part of a larger project, which includes installing BCSs and integrating them to the new front end. This step should only happen once—this is the front end for the basewide UMCS.

Note that while the intent is for the front end to use an open protocol, and the installation should have all the licenses and tools to fully utilize the front end since the front end is a complex application, and component parts of the application will have many vendor-specific aspects. For this reason, the front-end vendor will have a higher level of specialized knowledge about the front end and will have a competitive advantage on any procurement action involving the front end (including, in particular, system integration).

2. *Install BCSs*

Separate, open-competition building projects procure and install new (or upgraded) BCS in buildings. These projects constitute the majority of controls work at the installation and happen regularly over the lifetime of the UMCS through a variety of procurement mechanisms.

As with the front end, while the BCSs are required to use an open protocol, they are complex applications and component parts of the application will have many vendor-specific aspects, and a BCS vendor will have a competitive advantage on any future procurement action (e.g., perhaps a partial building renovation or expansion) involving their particular BCS.

3. *System Integration—Connect BCS to the UMCS Front End*

Once there is a front end and the BCSs are in place, those BCSs can be integrated into the front end. System integration should be a separate procurement activity from the BCS installation for the following reasons:

a. Integration requires detailed specialized knowledge of the front end (e.g., how to develop graphics for the front end). For this reason, the front-end contractor will have a large competitive advantage in bidding the integration project. This cost is small compared to the overall UMCS/BCS cost, and so it is common to accept that integration is often a proprietary task. However, Open Control Systems requirements prevent an advantage on the integration piece to translate to an advantage on the BCS installation.

b. Installations want the same look and feel of UMCS front-end graphics across different BCSs. The specs are vague and do not define graphics at a great level of detail. For this reason, installations often want and benefit from the same system integrator on all their integration projects.

System integration considerations and approaches are discussed in Section 4.7.

Steps 2 and 3 are then repeated to add more and more BCSs over the life of the UMCS. A similar process can also be used to add utility control systems (UCSs) to the UMCS.

5.6.2 Niagara Framework

The process for a Niagara Framework system is very similar except that each BCS to be connected to the Niagara Framework UMCS will have one or more Niagara Framework Supervisory Gateways installed in the building. Because of this, system integration (between a Niagara Framework building and s Niagara Framework front end) is a more straightforward process and can likely be done by the BCS contractor:

- Performing integration as part of the BCS installation provides for a simpler process and also makes commissioning of the BCS easier.
- Having a different contractor integrating each BCS may make it more difficult to get a consistent look and feel at the front end.

6 Commissioning

6.1 Background

The commissioning process for building construction projects is defined by ASHRAE Standard 189.1 as "a quality-focused process for enhancing the delivery of a project. The process focuses on verifying and documenting that the facility and *all* of its systems and assemblies are planned, designed, installed, tested, operated, and maintained to meet the owner's project requirements" (ASHRAE 2017). ASHRAE Standard 202 further states that "The Commissioning Process is a quality-based method that is adopted by an owner to achieve successful construction and renovation projects. It is not an additional layer of construction or project management. In fact, its purpose is to reduce the cost of delivering construction projects and increase value to owners, occupants, and users" (ASHRAE 2018).

Army commissioning requirements were first developed and included in construction specifications for BCS and UMCS in the 1980s. An Army Engineering Regulation titled *Systems Commissioning Procedures* was published in 1995 and focused on properly commissioning building HVAC control systems (USACE 1995).[21] Eventually, the Army's commissioning guidance was expanded to include commissioning requirements for most building systems, and the process became known as Total Building Commissioning (ASHRAE 2017).[22] Properly executed, Total Building Commissioning includes actions throughout the planning, design, construction, and operation of a facility. UFC 1-200-02, *High Performance and Sustainable Building Requirements*, calls for commissioning to be included in Army projects and mentions an operations team but, otherwise, does not specifically address execution requirements at the level of detail that might be needed at the installation DPW level.

6.2 The Army experience

The Army's experience with construction of thousands of facilities of every description has repeatedly proven the importance of properly commissioning a facility's systems. Although commissioning had been required for BCS and UMCS for almost all Army construction projects since the 1980s,

[21] Superseded by USACE (2017) (*Total Building Commissioning Procedures*, ER 1110-345-723).

[22] See also DoD (2021) (*Total Building Commissioning*, UFGS 01 91 00.15) and USACE (2017)

for many years the construction industry failed to take commissioning of these systems seriously, and the Government failed to establish realistic and enforceable commissioning requirements to be followed during the construction portion of the Total Building Commissioning process for these systems.

As facilities became increasingly complex, inadequate commissioning practices became more visible as many completed projects failed to perform as intended or, in some cases, not at all. Even though they do not function, all too often systems are accepted due to a variety of reasons, some of which are poor planning, lack of time at the end of the project, tenant-imposed deadlines, specification of overly complex systems, and requirements that stretch the technical expertise of the contractors and may exceed the capability of the commissioning agents to evaluate. In response to numerous customer complaints, USACE and the Tri-Service community decided to seriously address the need to properly commission facilities. Over a period of years and through a number of iterations, detailed commissioning requirements to be used during the construction of BCSs were developed and included in the appropriate Tri-Service construction UFGSs. For example, current UFGS 01 91 00.15 10, *Total Building Commissioning*, dated May 2019, provides very detailed commissioning requirements for building HVAC control systems (DoD 2020b).

Proper commissioning of the UMCS front end and each BCS is an ongoing challenge. Improper commissioning, particularly during the construction process, typically results in turnover of a building or system that quickly becomes a maintenance burden. Systematic commissioning, including thorough inspections and testing, should be a routine part of USACE's (in new construction) and the DPW's (in retrofit or local DPW construction) acceptance process to ensure that the Government gets what they paid for, gets what they need, and sets the Government up for ongoing successful building performance.

6.3 Inspections, testing, and acceptance

Ideally, the installation has a defined commissioning process. If not, the UMCS workgroup should define a system acceptance methodology for UMCS front end and BCS projects, including expected inspections and tests. This might include the development of checklists identifying project-monitoring activities and project requirements. The workgroup may decide to create a team, which includes specific offices, shops, or individuals to oversee and participate in inspections, testing, and acceptance.

One technical source is the UMCS and BCS UFGSs, which contain checklists in their appendices. These checklists can be used as a baseline but are not a complete acceptance methodology.

Some key project-monitoring requirements include tracking and review of the project schedule to ensure that it identifies key activities and submittals (especially product data, contractor design drawings, O&M manuals, and as-built drawings), contractor testing procedures and results, and training. An especially important test is one that verifies that the BCS performs in accordance with the specified sequence of operation.

“WAR STORY”

We were serving as the unofficial commissioning agents representing a critical tenant on their portion of a larger DoD construction project. At numerous meetings, we raised important construction deficiency issues, which were often echoed by the official contractually hired commissioning agent for the overall project. Our greatest opposition came, not from the controls contractor, not from the mechanical contractor, not even from the general contractor, but from the ***Government Commissioning Authority****, who appeared to be largely motivated by schedule and budget.*

If it were not for the fact that we represented an important tenant, one with the authority to halt the entire project, it is unlikely the deficiencies would have been addressed.

7 UMCS Sustainment and Growth

7.1 Background

Would a company purchase a fleet of buses without also hiring drivers, mechanics, dispatchers and someone to manage the whole thing?

Of course not. If they did, the company would fail, and the buses would end up sitting unused in a lot somewhere. Just like the fleet of buses, the success of a UMCS depends on it being properly used, managed, maintained, and grown. Historically, Army installations are not accustomed to providing this type of support—often there is insufficient controls expertise among maintenance staff, who are stretched too thin; generally insufficient IT expertise within the DPW; no dedicated operators for the system; and no individual at the installation who is truly responsible for the UMCS with the authority or job description to manage the UMCS. Traditionally, the installation DPW (O&M) has admirably managed to do as much as they can with their constrained resources but often leave much undone.

7.2 Staffing roles, responsibilities, and tasks

“WAR STORY”

Installation B, an early innovator in UMCS technology, experienced both the joys and the challenges of employing advanced technology. The joys included the promise of state-of-the-art automation that would simplify and optimize building operations, but the accompanying challenge was the reality of staffing requirements for even an automated system. Growing their Niagara Framework system by leaps and bounds their ambitious but meager UMCS staff of three struggled to keep up with the alarms and only rarely used the system to check things before they ran out to perform repairs—the three of them filled ALL the staffing roles.

There are several roles that need to be filled and multiple tasks performed to support a UMCS and the associated BCS. The various roles and tasks are not new requirements—they were always needed to properly support a UMCS. This is a formalization of those requirements.

Appendix G contains a position description for a UMCS manager. The appendix also contains a basic statement of work for a UMCS contractor to provide support for the following roles: system administrator, system integrator, and control technicians.

Each UMCS/BCS support role listed here is not necessarily a full-time staffed position. With the exception of the UMCS manager, these roles can be filled with contracted personnel (and this is essentially the model used by Fort Leonard Wood). However, the UMCS manager must be able to represent and commit the Government so must be a Federal employee. In practice, it likely makes sense to combine the UMCS administrator and technical expert roles. Staffing requirements are a function of the size and growth rate of the UMCS and are discussed later.

UMCS support roles include

- ***UMCS Manager.*** This role is responsible for managing all aspects of the UMCS and is the individual at the installation with the responsibility and authority to make local decisions concerning the UMCS, including planning and project prioritization. In general, the UMCS manager should understand but not necessarily be proficient in using a UMCS, have at least a macro-level familiarity of the installation, a cross-organizational influence, authority to make local UMCS decisions, and the ability to delegate technical work in coordination with other divisions and offices. Historically, when this role has been filled, it has typically been filled by the DPW energy manager, but this individual ordinarily does not have the time, designated responsibility, or authority to do so effectively. This can easily be a full-time position at most installations and should be someone in a supervisory-level position. This must be a Government employee. They do not necessarily have to use the UMCS themselves but should serve as an advocate for the UMCS. Key responsibilities include the following:
    - **Develops and Maintains a UMCS Master Plan:** This plan is described in Section 4. While details in the plan may be developed by a contractor, there are a number of critical decisions that will affect the installation for years to come. These decisions need to be made by someone with the authority to commit the installation to a long-term path.[23]

[23] Note that they should have a support staff to assist in the development of a master plan, but the decision needs to reside with the UMCS manager.

  - **Takes Responsibility for the System:** As such, this person should be designated as the cybersecurity system SO.
  - **Develops, Documents, and Maintains Policies and Procedures:** This individual is responsible for UMCS-related policies such as those in the IDG, a UMCS integration methodology, personnel requirements, etc.
  - **Competes for Resources:** Every installation operates in a resource-constrained environment, and the UMCS must compete against other activities for scarce funding. Someone needs to champion the UMCS, to fight for funding and resources for the UMCS.
  - **Plans and Programs for the UMCS:** Plans and manages funding and yearly budgets for the UMCS.
  - **Oversees UMCS/BCS Procurement and Installation:** Provides Government oversight and approval of submittals related to UMCS/BCS construction and installation. While reviews may better be performed by other personnel, a Government person with the authority to approve (and more importantly, to reject) submittals and commissioning efforts is critical to ensuring the installation only accepts systems meeting its UMCS master plan requirements. The ability to reject a system on behalf of the installation is one of the essential functions that cannot be performed by a contractor. Provides final system acceptance on behalf of the installation.
  - **Coordinates UMCS Use and Sustainment:** A number of DPW personnel are needed to maintain the UMCS; an even greater number should use the UMCS as part of their job duties. While these people may not work directly under the UMCS manager, the UMCS manager should be involved in ensuring they are aware of the system optimization benefits of the UMCS and interact productively with the UMCS. Some staff that the UMCS manager is encouraged to engage include the energy manager, mechanical engineers, and electrical engineers to obtain their help to optimize the comfort and BCS sequences of operation as well as to identify power quality, reactive load, and other electrical system issues
- ***UMCS (IT) System Administrator.*** This role provides the necessary IT expertise to the DPW in support of the UMCS, performs IT management for the UMCS, and coordinates UMCS IT issues with

NEC. The UMCS administrator role may be met by a combination of a DPW information assurance security officer (IASO), NEC service agreements, and contracted service agreements (SA). The role of managing the IT related aspects of the system is one of the biggest challenges facing a UMCS at most installations due in large part to information assurance (IA) requirements. Note that the NEC is not ordinarily responsible for the UMCS, so the DPW has to manage it themselves or pay NEC to do so. Tasks can be random (for instance, troubleshooting why the UMCS is not communicating) or ongoing (for instance, ensuring Federal Information Security Modernization Act [FISMA] compliance). This role must help bridge the language barrier between DPW and NEC because when talking about networks they talk different languages and even common terms can mean different things to the DPW and NEC. The UMCS administrator can get help from the UMCS MCX. Key responsibilities include the following:

  - **Manages the UMCS Front-End Applications:** Maintains the front-end applications. Manages user accounts on the applications. Keeps track of software licensing and updates.
  - **Manages UMCS Front-End Standard IT Applications (web server, database back end, etc.):** This will likely be performed by the NEC.
  - **Manages the UMCS Front-End Computer Hardware and OS:** This will likely be managed or coordinated with the NEC.
  - **Manages the UMCS IP Network:** In most cases, the UMCS will utilize the basewide IP network for transport, and this task will be performed by the NEC.
  - **Coordinates with NEC:** Where NEC has primary responsibility for tasks, coordinates with NEC to ensure that their activities (e.g., security patch installation) do not disrupt the UMCS operation.
  - **Obtains and Maintains Cybersecurity:** Takes primary responsibility for RMF for the UMCS.

- ***UMCS Operators.*** Next to the UMCS manager, this is the most important role since it encompasses the primary users of the UMCS. The purpose of this role is to take advantage of the power and capabilities of the UMCS. The UMCS should be the first stop for troubleshooting a controls or mechanical issue, with the UMCS operator playing a vital role. Key responsibilities include the following:

  - **Supports Troubleshooting:** Provides remote troubleshooting and diagnostic support using graphic displays, trends, and alarms. Assists and coordinates with maintenance staff and technicians to troubleshoot and address underlying issues. Manipulates the system via overrides, changing of setpoints, etc. For example, an operator might command a valve to open or close to support an HVAC mechanic troubleshooting a mechanical system.
  - **Monitors Operations:** Views graphic displays of the connected BCSs to help troubleshoot and proactively monitor system performance to identify abnormal or improper performance and help remedy problems. Views and analyzes historical trend data.
  - **Manages Alarms:** Configures and manage alarms (i.e., monitors, acknowledges, and clears alarms). Coordinates with troubleshooting staff to address underlying issues.
  - **Adjusts Operational Parameters:** Adjusts equipment operating schedules, sets up trends, and configures demand limiting.
  - **Analyzes Operations:** Runs reports to aggregate system data, analyzes energy usage, assesses BCS performance, etc.
  - **Coordinates Repairs**: Creates service or work requests and notifies pertinent personnel.
- ***System Integrator (On-staff).*** A system integrator has specialized knowledge of the UMCS front end and requirements needed to communicate with the front end. An on-staff system integrator (as opposed to a system integrator hired on an integration project-by-project basis) can complete the following:
  - **Reviews Submittals:** Provides technical reviews of contractor-provided BCS submittals for implementation projects, especially the Points Schedule submittal to ensure that integration requirements are being met.
  - **Oversees Commissioning (Cx):** Participates in BCS commissioning, as the Government representative to verify integration requirements
  - **Supports Others:** Uses their detailed knowledge of the UMCS front end software to support UMCS operators and other UMCS staff. This might take the form of UMCS troubleshooting or configuring the UMCS for additional user interface functionality.

Appendix H contains sample statements of work for contract support for the UMCS admin, control tech, and on-staff system integrator roles.

- ***System Integrator (Project-specific).*** This role physically executes system integration: the connection of a BCS to the UMCS front-end software. This role is separate from the on-staff system integrator role as there may be contractual or staffing reasons to keep these roles separate. This role, while vital, is of less concern in the context of this technical guide since this task is project specific and is funded via project-specific funds. Appendix I contains a sample SOW for project-specific system integration.
- ***Controls Technicians.*** This role provides control systems operation and maintenance and repair expertise. This can include, but is not limited to, diagnostics, troubleshooting, repair, replacement, and documentation of control systems, hardware, instrumentation, and devices. Key responsibilities include the following:
  - **Adjusts Operational Sequences**: Possesses technical knowledge of the underlying mechanical systems and largely understands the sequences of operation.[24] They troubleshoot and perform in-house modifications.
  - **Configures Controllers**: Use and configure field level controllers.[25] This skill is primarily used while troubleshooting the underlying mechanical system but may also be used during in-house repairs, replacements, and upgrades.
  - **May Configure Front End:** May possess a detailed knowledge of the front end to perform more in-depth configuration of the front end than a UMCS operator
  - **May Review Submittals:** May perform technical reviews of contractor submittals during projects as they are likely the most technically qualified individuals at the installation to evaluate technical submittals for a BCS project
  - **May Assist Cx:** May assist with Cx of a BCS project, particularly when familiar with the specific systems and products, but if not, then their general knowledge will still be valuable, and they should become experts in the new system to help support the installation in the future

[24] This is not at the level of designing new systems; they are not mechanical designers but can understand and work on a system once it is explained as part of system training during acceptance of new systems.

[25] They may not know how to fully program controllers; the installation may have to rely on the installing contractor for that level of system modification.

    - **May Assist RCx:** May assist (along with UMCS operators) in RCx of existing systems to help perform periodic system overhauls and tune-up
- ***Energy Manager.*** The energy manager uses the UMCS to implement energy savings and track energy savings via metering. While the current de facto situation at many installations is that the person filling the energy manager position description often attempts to execute the UMCS manager role, these are fundamentally different roles, and there is no fundamental reason that one person should fill both roles.
- ***HVAC Mechanics and Technicians.*** While not typically considered part of the UMCS staff, their presence in sufficient numbers is critical—if the underlying mechanical systems do not work, then there is no point to the control systems or UMCS. In some cases, it can be useful to subdivide HVAC mechanics into two skill levels:
    - A basic skill level, where the person is qualified to perform most PM activities and basic repairs
    - A more advanced skill level, where the person is also qualified to perform major overhauls and replacements. This level is also capable of troubleshooting and problem solving, usually working in conjunction with a controls technician or UMCS operator.

Other roles, while important, are probably too specialized or used too seldom to justify being implemented by installation personnel and may require support at the command level:

- ***Vendor Expert.*** This person has an in-depth understanding of the UMCS, beyond what would typically be needed or available at the installation. For the BCS, they understand how to add new devices, program devices, etc. For the front end, they know how to create new graphics or create scripts to automate front-end tasks. The installation may have an on-staff system integrator who has this knowledge, but generally, the installation will turn to contracted support for this expertise.
- ***HVAC-Specific Mechanical Engineer.*** This person is critical to help get the UMCS initially operational and to provide long-term support for the UMCS. This person has a deep understanding of HVAC: mechanical systems, commissioning, retrocommissioning, sequences of operation, thermodynamics, ASHRAE standards, O&M support, etc.

Commissioning is a key role and is discussed in Section 7.5. This expertise should be available locally, ideally through a staffed position within the DPW but may be obtained temporarily or for specific projects via contracted consulting help or from the UMCS-MCX at Huntsville.

- ***UMCS Expert.*** This person thoroughly understands the relevant UFGSs related to UMCS: UFGS 23 09 00, UFGS 23 09 23.XX, UFGS 23 09 13, UFGS 23 09 93 (BCS requirements), and UFGS 25 10 10 (UMCS front-end requirements). While this may be an outside consultant, often the first place to look for this expertise is the UMCS-MCX at Huntsville.
- ***Cybersecurity Expert (for the Control System).*** This person thoroughly understands the RMF process, the process for including cybersecurity in the design and construction process defined in UFC 4-010-06 and UFGS 25 05 11, and the unique aspects of implementing cybersecurity for control systems. This individual will require experience in both cybersecurity and control systems. Installations seeking this assistance with cybersecurity should consider starting with the USACE Control System Cybersecurity MCX at Huntsville Center.

7.3 Staffing estimates

UMCS staffing needs are defined by the roles and responsibilities of each staff member and are a function of the size of the UMCS. Table 4 and Table 5 provide staffing estimates for four different sizes of UMCS, based on the number of buildings connected to the UMCS. Staffed positions are based on the roles described above and on the basic tasks described below. Actual staffing hours are likely higher. Full-time-equivalent calculations are based on an 1800-hour work year to take into account holidays, annual leave, sick leave, etc.

Table 4. UMCS staffing estimate.

		Size of UMCS		
	X-small	Small	Medium	Large
Number of UMCS Buildings ->	25	100	300	1,000
UMCS Manager				
Hours (annual)	518	578	796	1,566
FTE	0.25	0.28	0.38	0.75
Energy Manager				
Hours (annual)	108	420	1,260	4,200
FTE	0.05	0.20	0.61	2.0
UMCS Administrator				
Hours (annual)	1,073	1,199	1,569	2,864
FTE	0.52	0.58	0.75	1.38
UMCS Unified Guide Spec Technical Expert				
Hours (annual)	44	92	252	812
FTE	0.02	0.04	0.12	0.39
Controls Technician				
Hours (annual)	542	1,760	4,920	15,800
FTE	0.26	0.85	2.4	7.6
UMCS Operator				
Hours (annual)	902	335	9,845	32,630
FTE	0.43	1.60	4.7	15.7
FTE Total	1.3	3.3	8.6	27.1

Table 5. HVAC technician and mechanic staffing estimate in support of UMCS.

	Size of UMCS			
	X-small	Small	Medium	Large
Number of UMCS Buildings ->	25	100	300	1,000
Basic HVAC Technician				
Hours (annual)	1,162	4,630	13,890	46,300
FTE	0.56	2.23	6.68	22.26
Advanced HVAC Technician				
Hours (annual)	1,070	4,250	12,750	42,500
FTE	0.51	2.04	6.13	20.43
FTE Total	1.1	4.3	12.8	42.7

The staffing tables include the previously described roles: UMCS manager, energy manager, UMCS administrator, technical expert, controls technician, and UMCS operator. System integrator is not included because this role is assumed to be absorbed into the overall cost of each individual project. HVAC mechanics and technicians are critical contributors and are included in Table 5

Note that in some cases one individual can fulfill more than one role. For example, the UMCS administrator and technical expert may be the same individual. With the exception of the UMCS manager, these roles can be filled with contracted personnel. The UMCS manager, however, must be able to represent and commit the Government so must be a Federal employee. Figure 14lists 29 basic tasks associated with the support and use of a UMCS. Each task includes additional information describing the task, including an indication as to whether or not a contractor can perform the task. The cells in this matrix show an estimate of the amount of time required to accomplish each task. An “X” indicates primary or direct responsibility and a “/” indicates partial or secondary responsibility. The columns are as follows:

- **Roles:** The roles that need to be performed or supported. An individual can perform more than one role. Note that roles are being defined here. This is not an attempt to match up, for example “UMCS Admin” with specific tasks. Instead, the list of tasks defines the UMCS admin role.
- **#:** Sequential numbering of items listed in the matrix
- **Ctr:** Whether or not the task can be done by a contractor
- **Tasks:** Short description of the task
- **Startup:** Indicates if there is a startup cost associated with the task. Startup costs include the development of documents, procedures, and processes, for example. Startup costs are not quantified here.
- **Time Category:** Each task includes an estimate of the amount of time required to perform the task. Some tasks are estimated differently than others and, therefore, have different time category units. These include
    - hours/year
    - hours/new building per year
    - hours/year per existing building
    - hours/year per person managed
    - hours/year per HVAC tech

Figure 14. UMCS staffing matrix.

	#	Ctr?	Tasks	Startup?	Time Category	UMCS Manager	Energy Manager	UMCS Admin	UMCS Technical Expert	SI	Controls Tech	UMCS Operator	Basic HVAC Tech	Adv. HVAC Tech	NEC
UMCS Management	1	Y	UMCS policies/procedures (system integration method, etc.)	Y	hours/year	12.0		24.0	12.0	/					
	2	N	UMCS planning (decisions)	Y	hours/year/new building	2.0									
					hours/year	80.0									
	3	N	UMCS champion (funding and utilization advocate and monitor)	Y	hours/year/new building	2.0									
					hours/year	200.0									
	4	N	Program Lead w/ delegating authority (Manage other roles and tasks)	N	hours/year/new building	2.0									
					hours/year/person managed	8.0									
	5	N	UMCS (not BCS/System integration) COTR	N	hours/year	120.0									
BCS Installation/Integration	6	Y	Review BCS proposals (prior to award)	N	hours/year/new building	1.00			4.00		2.00				
	7	Y	Review BCS designs	N	hours/year/new building	1.00			4.00		3.00				
	8	Y	Review BCS submittals (during construction)	N	hours/year/new building	1.00			4.00		2.00				
	9	N	BCS document approvals	N	hours/year/new building	2.00									
	10	Y	BCS testing/Cx	N	hours/year/new building	1.0			4.0		8.0		2.0	2.0	
	11	N	BCS Acceptance	N	hours/year/new building	4.0									
	12	Y	Integrate BCS into UMCS	N	hours/year/new building			2.00		X					
IT Tasks	13	Y	System database mgmt./coord.	N	hours/year/building			1.0							
					hours/year/new building			3.0							
					hours/year	20.0		80.0							
	14	Y	Interface with NEC	N	hours/year/new building			4.0		/					
					hours/year			40.0							
	15	Y	Maintain ATO	Y	hours/year/new building			8.0							/
					hours/year			500.0							/
	16	Y	IT hardware admin	N	hours/year			50.0				40.0			/

	#	Ctr?	Tasks	Startup?	Time Category	UMCS Manager	Energy Manager	UMCS Admin	UMCS Technical Expert	SI	Controls Tech	UMCS Operator	Basic HVAC Tech	Adv. HVAC Tech	NEC
	17	Y	IT- OS admin	N	hours/year			100.0							/
	18	Y	IT- application admin	N	hours/year	20.0		180.0							
	19	Y	Maintain IT Certification	Y	hours/year			40.0		/					
Use and Sustainment	20	Y	Alarm management (alarm receipt)	N	hours/year/ building							9.0			
					hours/year							40.0			
	21	Y	Work order generation	N	hours/year/ building							4.0	2.0	2.0	
	22	Y	UMCS/Front end ongoing configuration	N	hours/year/ building							1.0			
					hours/year/new building							4.0			
	23	Y	UMCS system "browsing"	N	as time permits						/	X			
	24	Y	UMCS trouble call receipt	N	hours/year/ building							9.0	4.0	4.0	
					hours/year/new building							2.0	4.0	8.0	
	25	Y	UMCS remote diagnostics	N	hours/year/ building						4.0	6.0		8.0	
					hours/year/new building						1.0	4.0			
	26	Y	HVAC mechanical & BCS equip work	N	hours/year/HVAC Tech						160.0				
					hours/year/ building								40.0	24.0	
	27	Y	Train (or get training for) HVAC Techs	N	hours/year/HVAC Tech	1.0					20.0		X	X	
	28	Y	RCx	N	hours/year/ building						2.0	2.0		4.0	
	29	Y	Energy Management	N	hours/year/new building		4.0					1.0			
					hours/year/ building		4.0					1.0			
					Total Hours/Year	578	420	1199	92	0	1760	3335	4630	4250	
					Decimal FTE Positions	0.32	0.23	0.67	0.05	0.00	0.98	1.85	2.57	2.36	

7.4 UMCS operations and best practices

The following recommended best practices for UMCS operation supplement the staffing roles described above. While these best practices are primarily grouped under the specific staffing role to which they apply, in some cases the execution of the best practice is dependent on a different staff role. Additional insights on utilization of best practices at Army installations is discussed in Westervelt et al. (2020).

HVAC Technician and Controls Technicians—Best Practices

1. ***Troubleshoot Control Systems using the front end (controls techs).*** Perform routine control system troubleshooting of the control hardware, such as sensors, actuators, and controllers. Controls technicians typically have access to an operator workstation to inspect alarms, view trend logs, and check setpoints, or UMCS operators might remotely operate equipment in response to technician requests during troubleshooting.
2. ***Troubleshoot Mechanical Equipment (HVAC techs).*** HVAC techs perform routine mechanical equipment troubleshooting through repairs of mechanical equipment, such as replacing broken belts, leaking coils, sticking or leaking valves and dampers. Some of these tasks, such as valve repair or replacement, may overlap with controls tech tasks and are coordinated between the two positions.
3. ***Routinely Inspect Controls and Equipment.*** On a regular schedule, controls techs inspect and calibrate sensors and actuators, and step controls through key sequences of operation to verify proper functionality. Similarly, HVAC techs routinely inspect and adjust mechanical equipment, such as motors, belts, fans, filters, and coils.
4. ***Engage Contractor Support.*** Coordinate with controls and equipment contractors to ensure that the installation's HVAC systems, equipment, and controls application requirements are met, including contractor participation in system startup, commissioning, and contractor-supplied training. The UMCS manager, in an oversight role, must help to ensure that contractors are capable of supporting the needs of the installation's UMCS.
5. ***Identify Needed Upgrades.*** Regularly inspect equipment to identify inefficient, aging, or outdated hardware, systems, or technology and recommend beneficial control system and equipment upgrades.
6. ***Assign Buildings to Technicians.*** Divvy up buildings or building areas and assign as the responsibility of specific technicians so that they can get to know and understand their buildings through repeated visits.

7. ***Organize Documentation.*** Gather, organize, and keep up-to-date system documentation (including paper and electronic format as-built documentation and drawings) in a central location, such as a DPW library, DPW software platform, on O&M laptops, or accessible from the UMCS front-end graphics page. Hard copies posted in the mechanical room can also be helpful. Ensure that system documentation is received at system turnover.
8. ***Log System Changes.*** Log, in some agreed upon fashion (notebook, online, etc.), changes made to systems so that other equipment operators will be aware of changes that have already been made and not inadvertently undo fixes. As a practical matter, logs can be difficult to keep up; some UMCS front-end software provides this built-in functionality, including an electronic trail of adjustments and configuration changes.
9. ***Post Equipment Maps.*** Post maps of equipment zones in mechanical rooms to identify which equipment serves each area. Verify that contractors post drawings and other documents in mechanical rooms as called for in contract documents.

UMCS Operators—Best Practices

1. ***Change Parameters Centrally.*** Adjust system operating parameters from the UMCS front end, such as setpoints, building occupancy schedules, and overrides. Use overrides (both temporary and otherwise) to adjust actuator positions and system setpoints to accommodate temporary needs and requirements and to assist in troubleshooting. Operational setpoints (such as interior temperatures) need to be coordinated with end users to avoid undesirable outcomes.
2. ***Troubleshoot Using Graphics.*** Use system graphics to step through systems and spot anomalies and cascading effects. Take advantage of graphics to review alarms and trend logs during troubleshooting. Assist mechanics or technicians with routine troubleshooting, where the UMCS operator can, for example, remotely actuate or operate equipment in response to a technician request during troubleshooting in a building or mechanical room.
3. ***Schedule HVAC Systems.*** Set up and adjust equipment start/stop schedules for systems according to occupancy schedules. Include special event and holiday scheduling.
4. ***Review History and Trends.*** Use history and trend logs to help diagnose problematic systems or points. Preemptively inspect history and trend logs to identify problems.

5. ***Use Fault Detection and Diagnostics.*** Utilize fault detection and diagnostic routines, where available, to signal failed equipment, such as failed automatic control valves on heating and cooling coils.
6. ***Manage System Alarms.*** Set up alarms to indicate system parameters that are out of bounds. Identify routing of alarms so that those who need to see them do and by the appropriate means (route to email, cell phone, etc.). Set alarm priority so that critical failures are readily recognized and attended to, especially for mission-critical buildings and supporting assets. Limit alarms to only those really necessary to avoid information overload and dismissal.
7. ***Maintain Equipment Proactively.*** Test operational conditions for indications of reduced equipment performance and act before issues turn into complaints.
8. ***Use Dashboard Reporting and Analysis.*** Identify, be familiar with, and use common metrics and graphs on the system dashboard (display screens) to perform rapid system performance analysis. Create performance reports. Identify dashboard improvements.
9. ***Log System Changes.*** Controls technicians log, in some agreed upon fashion (notebook, online, etc.), changes made to systems so that operators will be aware of changes that have already been made and not inadvertently undo fixes. As a practical matter, logs can be difficult to keep up; some UMCS front-end software provides this built-in functionality, including an electronic record trail of adjustments and configuration changes.

UMCS Administrator—Best Practices

1. ***Establish System Access Authority.*** Ensure personnel access to the UMCS is defined with an established hierarchy, such as read, write, and overwrite privileges along with access to and control of passwords, database, graphic display editing, and computer programs and code.
2. ***Perform Backups.*** Perform regularly scheduled database backups. Automated daily backups are recommended.
3. ***Manage Server Space.*** Keep track of disk space use to avoid system crashes due to disk full errors from excess interval data logging. At least every six months, perform a full archive backup of the server database(s) to a disk drive suitable for long-term storage. Optionally, remove any database time-series data more than three years old from the production server but retain the data.

4. ***Maintain UMCS Cybersecurity Posture.*** Manage the UMCS applications in accordance with the approved policies and procedures documented in the system ATO.

System Integrator—Best Practices

1. ***Incorporate Intuitive and Accurate Graphics.*** Standardize equipment layouts, but tailor to actual conditions. Make adjustments/updates to graphic displays to best represent the system and make displays user-friendly to UMCS operators, technicians, and mechanics, as applicable. Assist UMCS operators to create trends and define trend parameters, especially for problematic systems/points. Include ready access (via penetration scheme or hierarchy) to schedules and trends on equipment graphics.
2. ***Develop UMCS Functionality.*** Set up and configure the UMCS to allow UMCS operators to adjust schedules; create, modify, or delete alarms; respond to alarms; and create, modify, or delete trends. Set up overrides for setpoints and actuators. Where possible, configure graphics so that overridden points are highlighted or otherwise made evident of their overridden state.
3. ***Establish Dashboard Reporting and Analysis.*** Put common metrics and graphs on a system dashboard (display screens) for quick/efficient overview.
4. **Provide Detailed Operator Instructions.** Assist with the development of written step-by-step instructions for common tasks, especially for UMCS operators as UMCS M&C software use and operations can be cryptic.
5. **Organize Documents and Manuals**. Make documents easy to find and use. Help ensure system documentation, including documentation in electronic format, is organized and kept current, ideally in a DPW library and DPW software platform. This includes control system as-built documentation and drawings, UMCS M&C software, and other front-end-related manuals along with BCS hardware and software manuals. Coordinate with UMCS manager.

UMCS Manager—Best Practices

1. ***Be the Central Point of Contact (POC).*** Be the one person who serves as the hub for UMCS/controls activities.

2. ***Verify New Controls Match Plans.*** Make sure system additions, upgrades, and repairs meet design specifications and requirements and are compatible with current systems and standards.
3. ***Advocate for Resources.*** Advocate for funding, staff, training, etc.
4. ***Establish Sustainment Processes.*** Plan for ongoing maintenance and upgrade.
5. ***Resolve Stakeholder Conflicts.*** Coordinate and arbitrate conflict resolution. Stay calm and respectful. Allow people to share their perspectives.
6. ***Institute Facility Performance Accountability.*** Make the end results of performance part of people's job performance expectations.
7. ***Develop Detailed Operator Instructions.*** Identify and develop (with UMCS administrator) step-by-step instructions for common tasks, especially for UMCS operators.
8. ***Establish Adequate Contractor Support.*** Provides oversight and guidance to ensure that contractors are capable of supporting the installation's UMCS needs. Works with HVAC mechanics and controls technicians to identify support requirements.
9. ***Provide Training Resources.*** Make training resources available to all parties through video, online, in-house seminars, contractor-provided seminars, etc.

Mechanical System Troubleshooting—Best Practices

As an example of the capabilities of the UMCS, consider the following possible troubleshooting process scenarios:

A. Troubleshooting without use of the UMCS

1. Tenant calls and complains they are too hot.
2. Mechanic gathers some hand tools (e.g., wrenches), gets in their truck, drives to building.
3. Mechanic attempts to satisfy the tenant complaint—often without addressing the underlying problem. Perhaps they decide the delivered air needs to be colder and they go to the air handler unit (AHU), disconnect the cooling coil valve from the AHU controller, and manually adjust it to 100% open.

B. Troubleshooting with the UMCS but without alarms at the UMCS front end

1. Tenant calls and complains they are too hot.
2. UMCS operator checks Zone Temperature and Zone Temperature Setpoint.

   a. The actual temperature is compared to the setpoint. If the setpoint can be lowered, the operator adjusts the temperature. PROBLEM SOLVED

3. If, instead, actual temperature is not at setpoint, the troubleshooting continues:
4. The operator looks at delivered airflow and temperature:
   a. The actual airflow is compared to how much air should be flowing. The damper is checked for percent open.
   b. If there is an airflow problem and the damper is not wide open, the operator overrides it to full open and flags that Variable Air Volume (VAV) box for further investigation by a controls tech. PROBLEM SOLVED (temporarily)
   c. If there is an airflow problem and the damper is wide open, the operator flags the potential AHU or duct problem.
   d. The operator checks that the delivered air temperature is correct. If not, there is an AHU problem.
5. If the VAV box is behaving properly, the problem is upstream, perhaps at the AHU.
6. If there is a flow problem, the operator checks the airflow at the AHU. The Duct Static Pressure is compared to its setpoint. The supply fan is checked for percent full speed.
7. If there was a temperature problem, the operator checks the temperature at the AHU. The Supply Air Temperature is compared to the Supply Air Temperature Setpoint. The cooling coil valve is checked for percent open. If the valve is wide open, the delivered chilled water temperature is checked.
8. This process goes on in a systematic investigation until the root problem is uncovered. Often temporary corrective action (e.g., override of some mechanical component) can provide a quick fix until the underlying problem can be addressed.
9. All of this happens from the UMCS front end. While it is often required that someone visit the building, no one drives out to the building without knowing exactly where in the system the problem is located.

C. Troubleshooting with the UMCS and use of zone-level alarms

1. System generates an alarm stating, “Zone Temperature High.”
2. At this point the UMCS operator proceeds as in case B with Step 2.

Note that the tenant never calls to complain, the system acts proactively to correct issues before they rise to the level of a tenant complaint.

D. Troubleshooting with the UMCS and use of system-level alarms

1. System generates an alarm stating, “Supply Air Temperature High.”
2. At this point, the UMCS operator proceeds as in case B but can jump into the troubleshooting process at the point where they have identified the problem as being with the Supply Air Temperature.

Some observations based on the above troubleshooting approaches are as follows:

- Effective troubleshooting requires a systemic process to ultimately determine the root cause of the problem.
- Effective troubleshooting uses system alarms to
    - Diagnose and correct problems before the tenant gets involved and
    - Help isolate the problem component to shorten the troubleshooting process.
- Effective troubleshooting must use system data. These data are most readily available at the UMCS. Even where the ultimate fix requires a mechanic with appropriate hand tools (e.g., wrenches) to go to the building, those hand tools must be properly directed as the result of a systematic process involving the UMCS.
- Some problems can be SOLVED directly from the UMCS.
- Other problems can be temporarily fixed from the UMCS. Note that these temporary fixes cannot become permanent—once the problem has been identified, someone (likely with hand tools) still needs to go fix the underlying problem.
- Attempting to troubleshoot without use of the UMCS is highly problematic as it is difficult to know where the root cause is, and apparently corrective actions—while superficially solving the problem—in the long run create more problems than they solve. In the above example without the UMCS, Scenario A, the cooling valve is now wide open all the time. When heating season comes around, the AHU will still be in full cooling. The UMCS has been taken out of the loop.

All too often, installations—despite their best efforts—are largely in Scenario A: no UMCS troubleshooting. While many installations use their alarms for troubleshooting for some small subset of their buildings, almost no installations are consistently (across all their connected buildings) using their alarms to support one of the two “alarms” troubleshooting approaches.

7.5 Continued support—UMCS RCx

In spite of the UMCS being an automated system, it needs manual human intervention on a regularly scheduled basis, as do most complex and dynamic mechanical and electrical systems. Although many of the component parts of the system will receive ongoing maintenance as part of standard and emergency facility maintenance and many sections of the system may be newly constructed and commissioned facility control systems, it is recommended that every four years the overall basewide network of controls (as opposed to individual building components) and its supporting business processes should be systematically evaluated and repaired or adjusted to meet ongoing operational needs. This is referred to as retrocommissioning the UMCS, ensuring that the system is fit for service. To the extent feasible, this would include a high-level review for accurate and appropriate functioning, compliance with requirements, use of best practices, and ready posture for future needs. Significant input to this installation-level effort can be gleaned from the required facility-level energy evaluations.

Federal law mandates regular facility-level energy evaluations for DoD facilities, which include not only comprehensive energy and water evaluations (CEWE) (often referred to as energy audits) but also RCx assessments (operational evaluations) for larger or energy intensive facilities and follow-on detailed RCx investigations where appropriate.

The Energy Independence and Security Act (EISA) of 2007, Section 432, established the original criteria for these energy evaluations. This act was later amended by The Energy Act of 2020. Presently, each installation is required to select a group of facilities that comprise at least 75% of its purchased energy use to be designated as “covered” facilities, or subject to energy evaluation, and to receive a CEWE every eight years. RCx candidate facilities (covered facilities that are >50K ft^2 or >25K ft^2 and energy intensive) should also receive RCx assessments every eight years, and detailed RCx investigations will be performed where deemed appropriate by first-level RCx assessments. Admittedly, DPW budget constraints make any system review a challenge, but the current eight-year interval is quite long between checkups and can allow significant deviation from optimal performance. Energy intensive and critical facilities should be prioritized for more frequent RCx review as practicable. One ready reference detailing the retrocommissioning of existing Army buildings is *Army RCx Technical Guide, A Phased Approach for In-House or Contracted Existing Building Commissioning,* ERDC/CERL SR-18-1. Additionally, USACE-ERDC-CERL provides blended online and in-person RCx training to learn skills and methods.

The Federal Energy Management Program (FEMP) has multiple resources for energy evaluations and optimization at https://www.energy.gov/eere/femp/energy-and-water-audits-federal-buildings, and https://www.energy.gov/eere/femp/operations-and-maintenance-federal-facilities. Additionally, the Whole Building Design Guide has training courses on building tuning at https://www.wbdg.org/continuing-education/femp-courses.

These mandatory RCx evaluations provide valuable equipment inventories, BCS details, and identification and analysis of operational improvement measures at the building level. The operational improvement measures include recommendations for the replacement, repair, or calibration of failed components (such as failed or broken sensors, actuators, or dampers), modification of system components or operation to achieve correct equipment functioning (such as corrected equipment installation or layout, repair of network communication issues), and the addition or modification of equipment control schemes to achieve greater system efficiencies (such as adjustment of schedules, setpoints, and reset routines.) Additionally, the RCx evaluations may provide information on controls network challenges or failures and desirable control enhancements. It would be time and cost efficient to specify that RCx evaluations collect the building-level data desired for the UMCS RCx.

The outcomes from individual building RCx efforts can be collated and distilled into an installation-wide status summary, with insights on the extent of issues and opportunities for improvement. There may well be opportunities to implement installation-wide measures, such as including verification of correct air handler damper functioning during routine maintenance visits.

Additional steps for the overall UMCS include evaluation of the reliability of the network, speed of the network, available capacity of the network, currency of software updates, diversity of systems, availability and accuracy of documentation, centralization of information, commonalities of operational issues, friendliness of interfaces, reliability of components, extent of power backup for data, and ease and availability of servicing.

Primary steps of the UMCS RCx process will include data collection, documentation of existing systems, interviews with assorted stakeholders, field inspections, functional tests, operational data trend review, identification and analysis of improvement alternatives, implementation of selected measures, and verification of intended operations.

As infrastructure is updated over time, incorporation of automated fault detection and diagnostic features into UMCS software will enable monitoring-based commissioning that flags needed repairs or opportunities for proactive adjustments as soon as operations are outside of prescribed limits.

7.6 Future expansion and growth

Once stood up, a UMCS is grown by

- Integrating new BCSs for new construction,
- Integrating new or renovated BCSs from building renovations, or
- Integrating existing BCSs.

Generally, all new construction and major renovation (all MILCON) must (IAW 10 USC § 2867) integrate to the basewide UMCS. Renovated control systems should also integrate.

The decision of whether to integrate existing systems, and, if so, which ones, should consider the technology, age, and use of the buildings.

The advantage of an Open Control Systems approach as defined in UFGS 23 09 *xx* series and UFGS 25 10 10 is not obvious during the initial UMCS front-end procurement because it is easy to get that first group of building controls to function with their front end. The payoff of the rigorous Open Control Systems approach only becomes apparent when the second group of buildings is integrated into the UMCS. At that point, either everything goes smoothly because the procurements (initial UMCS front end and subsequence buildings) all followed the guide specs, ***or*** the guide specs were not followed, and integration becomes a disaster.

The UMCS expansion follows a regular process:

1. The UMCS master plan is consulted to help determine which buildings should next be integrated.
2. A contract is awarded for a new group of buildings using the same specs and tailoring options as the original procurement.
3. The SI provides key reviews for the Government on the BCS contractor's Points Schedule. The SI is highly motivated to make sure the Points Schedule is accurate because if the Points Schedule is incomplete or in error and the Government accepts it, there will issues during integration that the SI will have to address.
4. By this time, there should be an approved process (such as in the UMCS master plan), which establishes coordination with the NEC for adding new buildings to the existing UMCS authorization.
5. The SI integrates BCSs according to UFGS 25 10 10. The UFGS defines integration in three steps, where the last step, the creation of system graphics, is of prime importance. Even though the buildings are installed and integrated at different times, operators desire a common look and feel—a graphic for an air handler installed in 2010 should look very similar to the graphic for an air handler installed in 2020 (assuming the AHUs are mechanically similar). One way to ensure this is to always hire the same firm (and ideally the same person) to develop graphics. Another approach is for the installation to develop a graphics standard, which defines the look and feel for standard mechanical systems. This graphics standard could be part of the IDG and be included with integration contracts.
6. Periodically, the UMCS master plan should be revisited to ensure the installation is still moving in the right direction.

8 Cybersecurity

Cybersecurity for a UMCS project cannot be treated as an afterthought. Careful consideration of the cybersecurity measures and the requirements of the RMF is critical to ensure that UMCS functionality is not inadvertently limited or compromised by the application of cybersecurity measures. Note that a UMCS falls under the category of a facility-related control system (FRCS) and that there are DoD cybersecurity criteria that pertain to and thus impact any FRCS project.

It is important to note that with control system components becoming more interconnected on IP-based networks the need for secure network architectures is critical. It is equally important to provide a level of cyber protection comparable to the potential impact of an exploitation and the cyber threats and vulnerabilities that the control system is exposed to. For example, implementing a high level of cybersecurity protection on a control system that is a low-risk or low-impact asset is not ideal. Inversely, implementing a low level of cybersecurity protection on a high-risk or high-impact control system is not ideal either. As owners look to the future of control system technology and implementations, whether it be through new construction projects or through facilities' sustainment, restoration, and modernization (SRM) projects, having an integrated cybersecurity plan that accompanies those new implementation strategies and plans is paramount for project success.

8.1 Basic considerations

One unintended consequence of the current DoD multivendor Open Control Systems procurement approach is that, from a cybersecurity perspective, every system is unique requiring a custom approach.

The practical solution to cybersecurity lies in some basic concepts:

1. Have the UMCS workgroup engage with the local NEC early in the project. See Appendix D "Cyber: An Introduction to Building Control Systems for the IT Person."
2. Employ an appropriate mix of technical and project management personnel to support the project.

3. Develop a plan that addresses the defined functionality, roles and responsibilities, and dependencies on external stakeholders and service providers.
4. Leverage existing standard IT solutions to the greatest extent possible.
5. Design IAW DoD building codes (UFC and UFGS).
6. Work closely with the network service provider organization's authorizing official (AO) and their staff to reach a common understanding of the purpose, use, and nature of control systems to allow for an increased understanding of capabilities and risk. Inform the AO of the noncyber risks routinely accepted for the control systems to help define the overall risk posture of the system.
7. Address cybersecurity in the design, installation, and operation of control systems in a manner that provides security without compromising functionality.
8. Obtain ATO via the RMF.

8.2 Planning

The first step in cybersecurity planning is requirements gathering. The focus should be on information related to the existing site conditions that support FRCS and facilitate the follow-on design efforts. Below are some questions to ask during the planning process that will assist the workgroup in formulating project costs, design requirements, cybersecurity execution requirements, and SOW development. The questions below are not exhaustive but, rather, a sampling of questions that can assist the workgroup:

- Does the UMCS have an existing RMF ATO?
- Does the UMCS communicate (with IP) over the installation's common use network (i.e., installation campus area network [ICAN])?
- Do any other FRCSs intend to integrate to the UMCS for monitoring and or control?
- What is the planned risk impact level (CIA) of the systems within the scope of the project? See Appendix E for an explanation of impact rating and a detailed decision flow chart that assists the SO to determine the overall impact level associated with the control system.
- Have the SO (generally the UMCS manager) and AO roles been defined for the UMCS?

A clear definition of the roles and responsibilities of the workgroup is a vital step in ensuring that the workgroup members know the *who*, *what*, *when*, *where*, *how*, and *why* aspects of the project. Considering the unique nature of cybersecurity and the fact that it crosses into multiple technical disciplines and interfaces with multiple internal and external stakeholders, it is important to understand and track those interfaces. A powerful yet simple tool that can be used by the workgroup is a responsible, accountable, consulted, and informed (RACI) matrix that lays out the granular associated tasks, who the touch points are, and their actions in execution (see Appendix F).

A critical decision that must be determined early on in the project development and planning phase is the determination of the control system's risk impact level. This decision is critical not only for RMF purposes long term, but for the control system design phase as well. The determination of the risk impact level establishes the baseline for the cybersecurity controls[26] that will be incorporated into the cybersecurity design of the HVAC control system. This determination can often be a challenge to the UMCS workgroup in selecting the appropriate risk impact due to the multiple areas of risk and their association to other project elements, which often end up creating an artificial over categorization of impact. To assist the UMCS workgroup in determining the appropriate risk impact to the control system and its relation to the overall mission, a detailed decision flow chart has been included in Appendix E that will assist the SO to determine the overall impact risk level associated with the control system.

8.3 Personnel considerations

Addressing cybersecurity requirements is a critical part of UMCS planning and project execution. This will require someone within the workgroup to have a technical background in cybersecurity and information technology (IT). This additional workgroup member(s) should ideally work internally with the workgroup's mechanical and electrical engineers to evaluate functional requirements of the UMCS project, apply cybersecurity design features, acquire necessary IT support requirements from the local NEC (or network service provider), and generally execute or oversee the execution of the RMF process.

[26] Cybersecurity controls are policies, procedures, or techniques that support system confidentiality, integrity, and availability. Example cybersecurity controls are passwords, two-factor identification of users, file encryption, or physical fences protecting equipment.

Below are some of the key knowledge, skills and abilities (KSA) this workgroup member should have. This list of KSAs is by no means exhaustive:

- Foundational knowledge in control system communication protocols and communication mediums (i.e., IP, Modbus, BACnet, LonWorks, MS/TP, TP/FT-10, etc.)[27]
- Advanced knowledge in TCP/IP network communications[28]
- Foundational knowledge in client/server technology
- Theoretical knowledge of cybersecurity principles and Risk Management Framework
- General understanding of the vertical construction process
- Ability to read and write technical specifications and drawings
- General project management skills
- Ability to communicate and translate technical requirements across multidisciplinary technical fields (e.g., ability to understand and be able to translate what the mechanical engineer is saying to nonmechanical engineers in the IT or cybersecurity disciplines and vice versa)

Typically, Government civilian personnel who would have these KSAs could be in multiple 0800 Engineering job series (i.e., 0830 Mechanical Engineering, 0850 Electrical Engineering, 0802 Engineering Tech, etc.) or the 2210 IT Specialist job series. Unfortunately, finding a singular individual who has the knowledge base to perform these duties is quite rare and unique in the Federal Government at this time. However, this will likely change over time due to the ever-increasing dependency UMCSs and other FRCSs have on traditional IT networks and the market space's continual push to have their product lines integrated to support real-time data analytics.

[27] TP/FT-10 is twisted pair free topology media.

[28] TCP/IP is Transmission Control Protocol/Internet Protocol media.

8.4 Cybersecurity in the design, installation, and operation of control systems

8.4.1 Design: Unified Facility Criteria (UFC) 4-010-06, *Cybersecurity of Facility-Related Control Systems, and Unified Facility Guide Specification*; (UFGS) 25 05 11, C*ybersecurity for Facility-Related Control Systems*

UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*, describes requirements for incorporating cybersecurity in the design of all facility-related control systems. It defines a process based upon the risk management framework suitable for control systems of any impact rating and provides specific guidance suitable for control systems assigned a LOW or MODERATE impact level. The UFC applies to all planning, design and construction, renovation, and repair of new and existing facilities and installations that result in DoD real property assets, regardless of funding source. The UFC has a very narrow focus in that it supports design-related activities, not full life-cycle activities; it is not the full RMF process, and it provides guidance to designers of record. It does not cover O&M activities.

UFGS 25 05 11, *Cybersecurity for Facility-Related Control Systems (FRCS)*, is the Tri-Service-approved specification to execute FRCS cybersecurity requirements. The UFGS consolidates all cybersecurity construction submittals and related testing into one specification. It currently covers FRCSs that are designed at the LOW and MODERATE impact level and includes requirements in support of the RMF. The UFGS covers a wide range of FRCSs (e.g., ESS, HVAC, fire, elevator, etc.). Project specifications should be developed utilizing this UFGS. Similar to the UFC, this UFGS only supports design and construction activities; it does not cover all the aspects of cybersecurity in the RMF.

The UFC and UFGS are found at https://wbdg.org/ffc/dod.

8.4.2 Installation and operation: Risk Management Framework and IT network service provider

8.4.2.1 Risk Management Framework

In 2014, the DoD implemented (via DoDI 8500) the National Institute of Standards and Technology (NIST) Risk Management Framework as the DoD's process to manage and assess risks related to IT systems and applications. The DoD RMF authorization process is a critical-path task for any

FRCS project in the DoD to execute in full or in part, and it must be accounted for in all execution plans. The RMF provides a disciplined and structured process that combines information system security and risk management activities into the system development life cycle and authorizes their use within the DoD. The RMF changes the traditional focus of certification and authorization as a static, procedural activity to a risk management approach that provides the capability to manage system-related cybersecurity risks more effectively in a relative environment. The RMF applies to all DoD IT (which includes FRCS) that receives, processes, stores, displays, or transmits DoD information. These technologies are broadly grouped as DoD information systems (IS), platform IT (PIT), IT services, and IT products.

The RMF process and authorization strategy must be accounted for in all UMCS projects. SOs whose control system strategy may include the integration of third-party analytic solutions, cloud computing services, intelligent sensors, and other advanced technologies into existing control system boundaries, must account for these inclusions via the RMF process and other supporting stakeholders' (i.e., network service providers, IT governance staff, etc.) input and approvals. Executing the RMF process is a very labor- and time-intensive effort. It requires personnel who understand both technical and procedural aspects of the RMF to be successful in its implementation. Detailed instructions on RMF are defined in the most current instruction in accordance with DoDI 8500. As of this publication the applicable instruction is *Risk Management Framework (RMF) for DoD systems,* DoDI 8510.01 (DoD 2022), and *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 rev 5. (NIST 2020). Guidance for using the RFM process is given in Long et al. 2019.

8.4.2.2 IT network service provider

Typically, large-scale campus environments to include military installations utilize large-scale distributed networks to provide data, voice, and video to the tenants on the respective campus or military installation. On military installations, these networks are typically operated and managed by the installation network service provider. The installation network service providers vary by service and agency. For example, on Army installations, the installation network service provider is the NEC. The installation NEC is the single authority for providing common-use IT services (for example, command, control, communications, computers, and information management [C4IM] services list). The NEC is the starting point for tenant organizations and activities to obtain support for unique IT services that are not provided in the C4IM services list. The installation NEC is the only organization on the installation authorized and responsible for providing common-use baseline services on a nonreimbursable basis to all installation tenants as prescribed by the Army C4IM services list. The Army C4IM services list is a vital reference source to be utilized when developing a service-level agreement and memorandum of agreement with the local NEC.

8.5 Cybersecurity details

Cybersecurity and IT requirements and strategy are very deep topics that constitutes the need for multiple reference resources to effectively navigate the numerous requirements and considerations required to successfully execute a project. Listing each specific requirement to the depth and specificity needed within this technical guide is not ideal. To provide workgroup members a more detailed list of references and resources to assist them in their planning and execution efforts, the bibliography of this technical guide provides a more comprehensive listing of these references and resources.

Bibliography

Related UMCS and BCS implementation guidance and information are available.

American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE)

ASHRAE (American Society of Heating, Refrigerating, and Air-Conditioning Engineers). 2017. *Standard for the Design of High-Performance Green Buildings*. ASHRAE Standard 189.1. Peachtree Corners, GA: ASHRAE.

ASHRAE (American Society of Heating, Refrigerating, and Air-Conditioning Engineers). 2018. *Commissioning Process for Buildings and Systems*. ASHRAE Standard 202. Peachtree Corners, GA: ASHRAE.

Army Regulations (AR):

DA (Department of Army). 2012. *Army Facilities Management*. AR-420-1. Washington, DC: Department of Army. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN15517_R420_1_admin_FINAL.pdf.

Department of the Army. 2020. *Army Installations Strategy: Supporting the Army in Multiple Domains*. Washington, DC: Department of the Army. https://www.asaie.army.mil/Public/SI/doc/Army_Installations_Strategy_(AIS)_FINAL_Signed.pdf.

Department of Defense Instructions (DoDI):

DoD (Department of Defense). 2022. *Risk Management Framework (RMF) for DoD systems* DoDI 8510.01. Washington, DC: Department of Defense.

DoD (Department of Defense). 2016. *Installation Energy Management*. DoDI 4170.11. Change 1, effective March 16, 2016. Washington, DC: Department of Defense.

USD(A&S) (Under Secretary of Defense for Acquisition and Sustainment). 2020. *Operation of the Adaptive Acquisition Framework*. DoDI 5000.02. Washington, DC: Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf.

Engineering And Construction Bulletins (ECB):

USACE (US Army Corps of Engineers). 2020. *Facility-Related Control System Cybersecurity Coordination Requirement—Category: Directive and Guidance*. USACE ECB 2020-10. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/engineering-and-construction-bulletins-ecb/usace-ecb-2020-10.

Engineering Regulations (ER):

USACE (US Army Corps of Engineers). 1995. *Systems Commissioning Procedures*. ER 1110-345-723 [superseded by *Total Building Commissioning Procedures*, ER 1110-345-723 (USACE 2017)]. Washington, DC: Department of the Army.

USACE (US Army Corps of Engineers). 2017. *Total Building Commissioning Procedures*. ER 1110-345-723. Washington, DC: Department of the Army. https://www.publications.usace.army.mil/Portals/76/Publications/EngineerRegulations/ER_1110-345-723.pdf.

USACE (US Army Corps of Engineers). 2019. *USACE Critical Infrastructure Cybersecurity Mandatory Center of Expertise*. ER 25-1-113. Washington, DC: Department of the Army. https://www.publications.usace.army.mil/Portals/76/Users/182/86/2486/ER%2025-1-113.pdf?ver=CWGVBUsmJ4bMuJ3kSM2L-A%3d%3d.

Policy and Legislation:

ASA-IEE (Assistant Secretary for Installations, Energy and Environment). 2020. *Army Policy on Building Automation Systems*. Memorandum. Washington, DC: Department of Defense.

CNSS (Committee on National Security Systems), 2014. *Security Categorization and Control Selection for National Security Systems*. CNSSI No. 1253. Ft. Meade, MD: National Security Agency. CNSSI_No1253.pdf (dcsa.mil).

DA (Department of the Army). 2020. *Army Installations Strategy: Supporting the Army in Multiple Domains*. Washington, DC: Department of the Army. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN32810-SD_07_STRATEGY_NOTE_2020-01-000-WEB-1.pdf.

DA (Department of the Army). 2021. *Army Facility Investment Guidance (FIG): Annual Update for POM 20-24*. Washington, DC: Department of the Army.

DCS (Deputy Chief of Staff), G-9 Installations. 2021. *Department of the Army Guidance for Implementation of a Building Automation System (BAS)*. Washington, DC: Department of Defense.

Energy Monitoring and Utility Control System Specification for Military Construction and Military Family Housing Activities. 10 USC § 2867 (2009). https://www.govinfo.gov/app/details/USCODE-2011-title10/USCODE-2011-title10-subtitleA-partIV-chap169-subchapIII-sec2867.

National Defense Authorization Act for Fiscal Year 2018. Pub. L. No. 115-200. (2017). https://www.govinfo.gov/content/pkg/CRPT-115hrpt200/pdf/CRPT-115hrpt200.pdf.

NIST (National Institute of Standards and Technology). 2004. *Standards for Security Categorization of Federal Information and Information Systems*. Federal Information Processing Standards (3-540) 199. Washington, DC: US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.

NIST (National Institute of Standards and Technology). 2008. *Volume II: Appendices to Guide for Mapping Types of Information and Information System to Security Categories*. NIST SP 800-60. Gaithersburg, MD: NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf.

NIST (National Institute of Standards and Technology). 2020. *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53 Rev.5. Gaithersburg, MD: NIST. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

Technical Reports on Building Controls:

Clark, Brian, Matt M. Swanson, Sean M. Wallace, Eileen T. Westervelt, and Jay H. Tulley. 2018. *Army RCx Technical Guide, A Phased Approach for In-House or Contracted Existing Building Commissioning*. ERDC/CERL SR-18-1. Champaign, IL: ERDC-CERL. http://dx.doi.org/10.21079/11681/26414.

Long, Michael Cary, Joseph Bush, Steven Briggs, Tapan Patel, Eileen Westervelt, Daniel Shepard, Eric Lynch, and David Schwenk. 2019. *Army Guide to Navigating the Cybersecurity Process for Facility Related Control Systems: Cybersecurity and Risk Management Framework Explanations for the Real World*. ERDC-CERL SR 19-5. Champaign, IL: ERDC-CERL. http://dx.doi.org/10.21079/11681/35294.

Schwenk, David M., Joseph Bush, and David M. Underwood. 2005. *Heating, Ventilating, and Air-Conditioning (HVAC) Control Systems Operations and Maintenance at Fort Bragg, NC: Training and Technical Assistance*. ERDC/CERL TR-05-14. Champaign, IL: ERDC-CERL. http://hdl.handle.net/11681/20112.

Schwenk, David M., Joseph Bush, Lucie M. Hughes, Stephen Briggs, and Will White. 2008. *IMCOM LonWorks Building Automation Systems Implementation Strategy*. ERDC/CERL TR-08-12, Champaign, IL: ERDC-CERL. http://hdl.handle.net/11681/20158.

Schwenk, David M., David M. Underwood, Joseph Bush, Brian Clark, Tapan Patel, Annette L. Stumpf, and Susan J. Bevelheimer. 2017. *Utility Monitoring and Control System (UMCS) and Utility Metering Plan and Specifications for Fort Leonard Wood, MO*. ERDC/CERL TR-17-15. Champaign, IL: ERDC-CERL. http://dx.doi.org/10.21079/11681/22742.

Shepard, Daniel A., Joseph Bush, Eric Lynch, Alan Schuld, Andrew Spear, Fred Abbitt, and Dahtzen Chu. 2018. *Facility Related Control Systems (FRCS) Architecture Report*. CEHNC-TR 18-01. Champaign, IL: ERDC-CERL.

Westervelt, Eileen, Paul Loechl, Sarah Clark, and Courtney DuPont. 2020. *Enhancing Army Energy Culture with Behavioral Approaches*. ERDC/CERL TR 20-5. Champaign, IL: ERDC-CERL. http://dx.doi.org/10.21079/11681/37945.

Unified Facilities Criteria (UFC):

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)]. 2015b. *Mechanical Engineering*. UFC 3-401-01. Change 1, effective 01 October 2015. Washington, DC: Department of Defense.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)]. 2017a. *Cybersecurity of Facility-Related Control Systems*. UFC 4-010-06. Change 1, effective 18 January 2017. Washington, DC: Department of Defense. https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2016_c1.pdf.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)]. 2018a. *Direct Digital Control for HVAC and Other Building Control Systems*. UFC 3-410-02. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-3-410-02.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)]. 2018b. *Utility Monitoring and Control System (UMCS) Front End and Integration*. UFC 3-470-01. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-3-470-01.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)]. 2019b. *Engine-Driven Generator System for Prime and Standby Power Applications*. UFC 3-540-01. Change 2, effective 5 November 2019. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-3-540-01.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)]. 2019c. *High Performance and Sustainable Building Requirements*. UFC 1-200-02, Change 04, effective 01 October 2019. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-1-200-02.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), and HQ AFCEC (Air Force Civil Engineer Center)]. 2019f. *Standard Practice Unified Criteria, Facilities Criteria and Unified Facilities Guide Specifications*. MIL-STD-3007G. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/federal-military-specifications-standards/mil-std-3007.

Unified Facilities Guide Specifications (UFGS):

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2015a. *Instrumentation and Control Devices for HVAC*. UFGS 23 09 13. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-23-09-13.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2015c. *Sequences of Operation for HVAC Control*. UFGS 23 09 93. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-23-09-93.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2017b. *Cybersecurity for Facility-Related Control Systems*. UFGS 25 05 11. Washington, DC: Department of Defense. UFGS: https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2019a. *BACnet Direct Digital Control for HVAC and Other Local Controls*. UFGS 23 09 23.02. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-23-09-23-02.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2019d. *Instrumentation and Control for HVAC*. UFGS 23 09 00. Change 1, effective November 2019. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-23-09-00.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2019e. *LonWorks Direct Digital Control for HVAC and Other Local Controls*. UFGS 23 09 23.01. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-23-09-23.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2019g. *Utility Monitoring and Control System (UMCS) Front End and Integration*. UFGS 25 10 10. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-10-10.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2020a. *Risk Management Framework for Facility-Related Control Systems*. UFGS 25 08 11.00 20. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-08-11-00-20.

DoD (Department of Defense) [USACE (US Army Corps of Engineers), NAVFAC (Naval Facilities Engineering System Command), HQ AFCEC (Air Force Civil Engineer Center), and NASA (National Aeronautics and Space Administration)]. 2020b. *Total Building Commissioning*. UFGS 01 91 00.15 10. Change 2, effective August 2020. Washington, DC: Department of Defense. https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-01-91-00-15-10.

Websites and Brochures:

Chipley, Michael. 2020. "Cybersecurity." Resource Pages. Whole Building Design Guide. https://www.wbdg.org/resources/cybersecurity.

CISA (Cybersecurity & Infrastructure Security Agency). https://us-cert.cisa.gov/.

DISA (Defense Information Systems Agency). "DoD Cyber Exchange." https://public.cyber.mil/.

HQAMC (Headquarters Army Materiel Command). n.d. "G-2/6 Cybersecurity & Compliance Branch [AMC SharePoint]". https://hqamc.aep.army.mil/gstaff/amcio/ia/Pages/Welcome.aspx.

IMCOM (Installation Management Command). n.d. "G6 Information Management [IMCOM SharePoint]" https://army.deps.mil/army/cmds/imcom_HQ/G6/SitePages/DirectorateHome.aspx.

NETCOM (Network Enterprise Technology Command). NETCOM RMF [RMF SharePoint Portal]. https://army.deps.mil/NETCOM/sites/RMF.

NIST (National Institute of Standards and Technology). n.d. "Computer Security Division." Information Technology Laboratory. https://www.nist.gov/itl/csd.

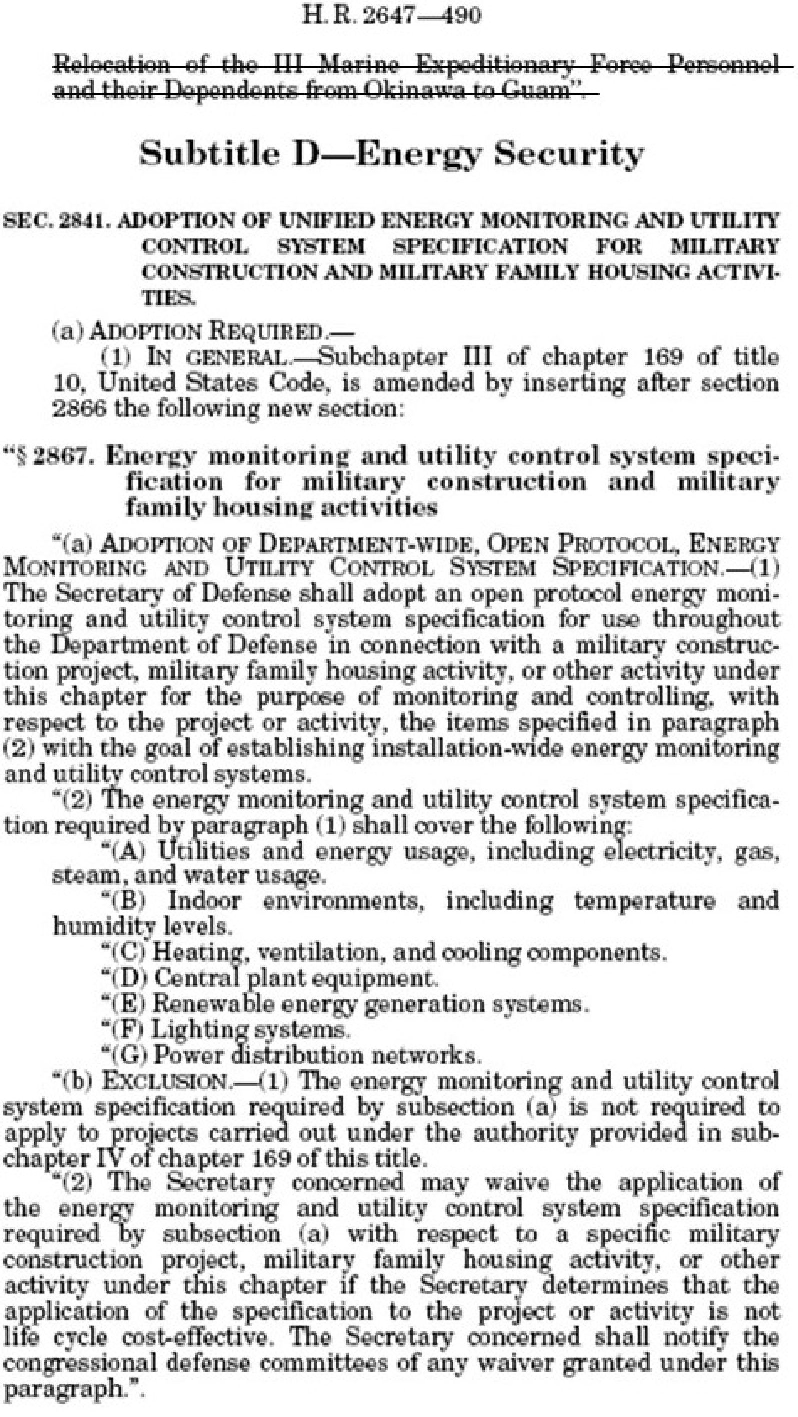
RMF Knowledge Service Portal. https://rmfks.osd.mil/login.htm.

SERDP/ESTCP (Strategic Environmental Research and Development Program, Environmental Security Technology Certification Program). n.d. "Cyber Security." Installation Energy and Water. Tools and Training. SERDP/ESTCP. https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity.

USACE (US Army Corps of Engineers) Engineering and Support Center, Huntsville. *Utility Monitoring and Control Systems*. Huntsville, AL: USACE. https://www.hnc.usace.army.mil/Portals/65/docs/PAO/TriFolds/UMCStrifold%201809.pdf?ver=2018-10-02-095014-430.

WBDG (Whole Building Design Guide). https://www.wbdg.org/.

Appendix A: H.R. 2647, National Defense Authorization Act for FY 2010 (NDAA 2010), Section 2841



H. R. 2647—490

~~Relocation of the III Marine Expeditionary Force Personnel and their Dependents from Okinawa to Guam".~~

Subtitle D—Energy Security

SEC. 2841. ADOPTION OF UNIFIED ENERGY MONITORING AND UTILITY CONTROL SYSTEM SPECIFICATION FOR MILITARY CONSTRUCTION AND MILITARY FAMILY HOUSING ACTIVITIES.

(a) ADOPTION REQUIRED.—

(1) IN GENERAL.—Subchapter III of chapter 169 of title 10, United States Code, is amended by inserting after section 2866 the following new section:

"§ 2867. Energy monitoring and utility control system specification for military construction and military family housing activities

"(a) ADOPTION OF DEPARTMENT-WIDE, OPEN PROTOCOL, ENERGY MONITORING AND UTILITY CONTROL SYSTEM SPECIFICATION.—(1) The Secretary of Defense shall adopt an open protocol energy monitoring and utility control system specification for use throughout the Department of Defense in connection with a military construction project, military family housing activity, or other activity under this chapter for the purpose of monitoring and controlling, with respect to the project or activity, the items specified in paragraph (2) with the goal of establishing installation-wide energy monitoring and utility control systems.

"(2) The energy monitoring and utility control system specification required by paragraph (1) shall cover the following:

"(A) Utilities and energy usage, including electricity, gas, steam, and water usage.

"(B) Indoor environments, including temperature and humidity levels.

"(C) Heating, ventilation, and cooling components.

"(D) Central plant equipment.

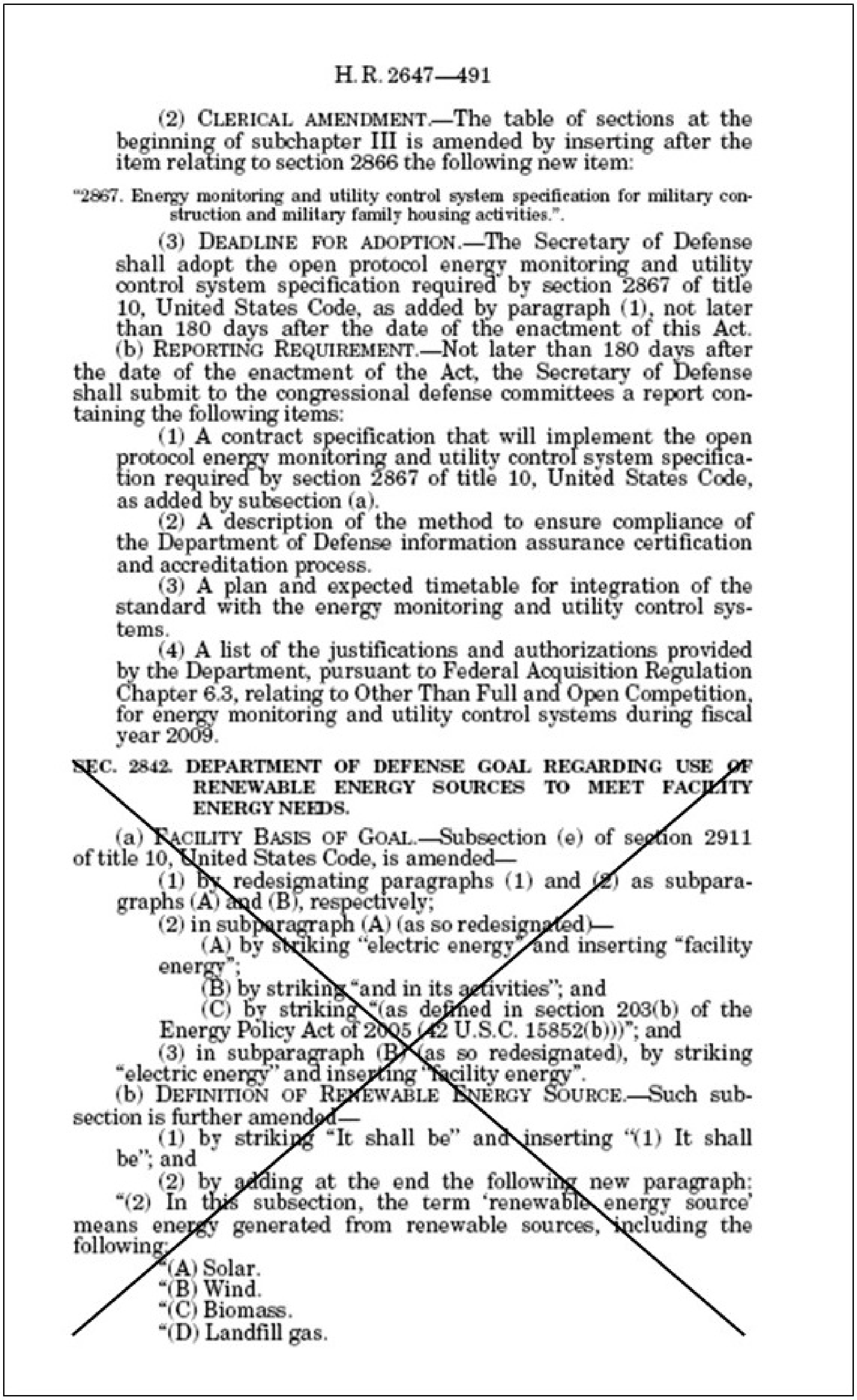
"(E) Renewable energy generation systems.

"(F) Lighting systems.

"(G) Power distribution networks.

"(b) EXCLUSION.—(1) The energy monitoring and utility control system specification required by subsection (a) is not required to apply to projects carried out under the authority provided in subchapter IV of chapter 169 of this title.

"(2) The Secretary concerned may waive the application of the energy monitoring and utility control system specification required by subsection (a) with respect to a specific military construction project, military family housing activity, or other activity under this chapter if the Secretary determines that the application of the specification to the project or activity is not life cycle cost-effective. The Secretary concerned shall notify the congressional defense committees of any waiver granted under this paragraph.".



H. R. 2647—491

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of subchapter III is amended by inserting after the item relating to section 2866 the following new item:

"2867. Energy monitoring and utility control system specification for military construction and military family housing activities.".

(3) DEADLINE FOR ADOPTION.—The Secretary of Defense shall adopt the open protocol energy monitoring and utility control system specification required by section 2867 of title 10, United States Code, as added by paragraph (1), not later than 180 days after the date of the enactment of this Act.

(b) REPORTING REQUIREMENT.—Not later than 180 days after the date of the enactment of the Act, the Secretary of Defense shall submit to the congressional defense committees a report containing the following items:

(1) A contract specification that will implement the open protocol energy monitoring and utility control system specification required by section 2867 of title 10, United States Code, as added by subsection (a).

(2) A description of the method to ensure compliance of the Department of Defense information assurance certification and accreditation process.

(3) A plan and expected timetable for integration of the standard with the energy monitoring and utility control systems.

(4) A list of the justifications and authorizations provided by the Department, pursuant to Federal Acquisition Regulation Chapter 6.3, relating to Other Than Full and Open Competition, for energy monitoring and utility control systems during fiscal year 2009.

~~**SEC. 2842. DEPARTMENT OF DEFENSE GOAL REGARDING USE OF RENEWABLE ENERGY SOURCES TO MEET FACILITY ENERGY NEEDS.**~~

~~(a) FACILITY BASIS OF GOAL.—Subsection (e) of section 2911 of title 10, United States Code, is amended—~~

~~(1) by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively;~~

~~(2) in subparagraph (A) (as so redesignated)—~~

~~(A) by striking "electric energy" and inserting "facility energy";~~

~~(B) by striking "and in its activities"; and~~

~~(C) by striking "(as defined in section 203(b) of the Energy Policy Act of 2005 (42 U.S.C. 15852(b)))"; and~~

~~(3) in subparagraph (B) (as so redesignated), by striking "electric energy" and inserting "facility energy".~~

~~(b) DEFINITION OF RENEWABLE ENERGY SOURCE.—Such subsection is further amended—~~

~~(1) by striking "It shall be" and inserting "(1) It shall be"; and~~

~~(2) by adding at the end the following new paragraph:~~

~~"(2) In this subsection, the term 'renewable energy source' means energy generated from renewable sources, including the following:~~

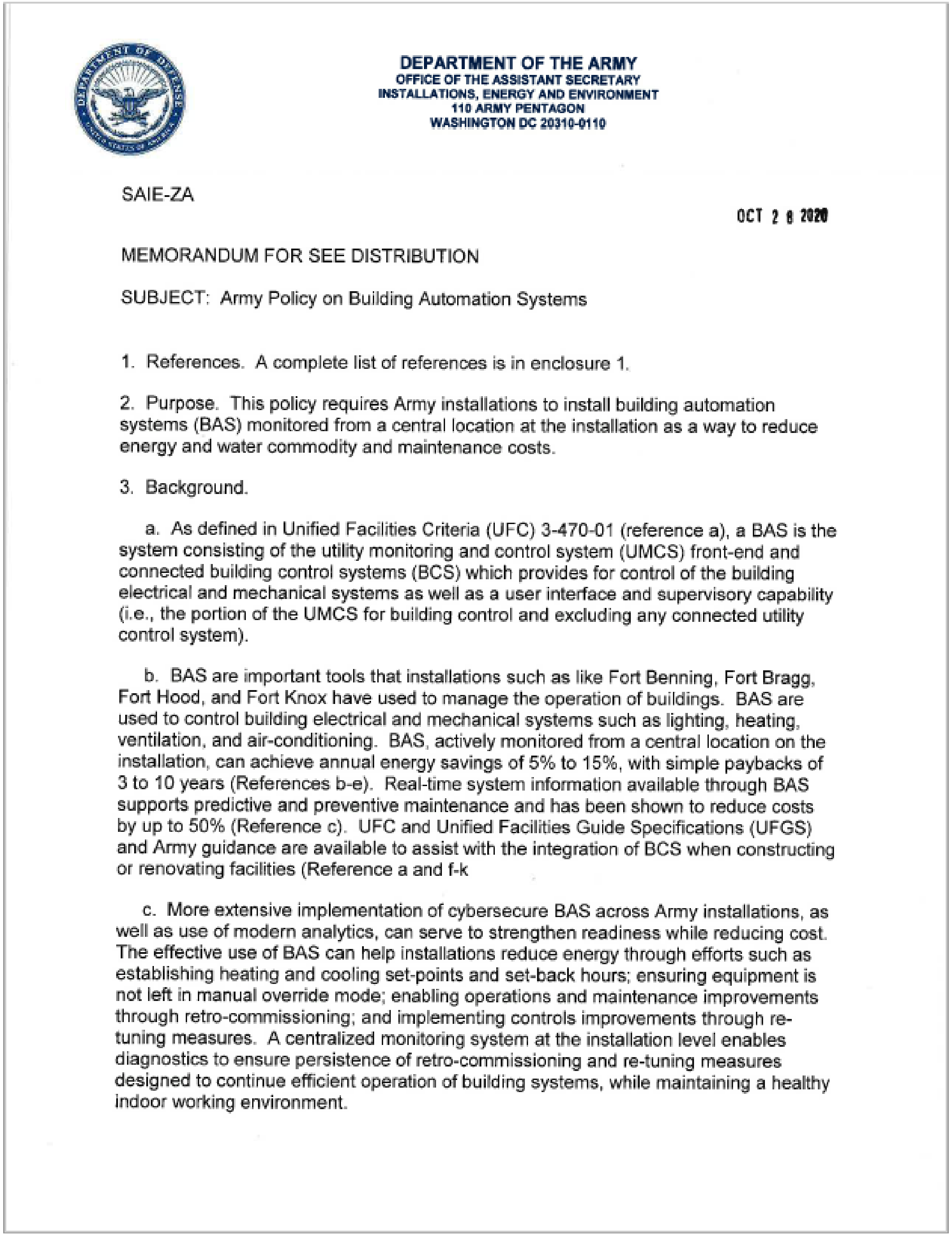
~~"(A) Solar.~~

~~"(B) Wind.~~

~~"(C) Biomass.~~

~~"(D) Landfill gas.~~

Appendix B: Army Policy on Building Automation Systems, Memo, 28 October 2020



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY
INSTALLATIONS, ENERGY AND ENVIRONMENT
110 ARMY PENTAGON
WASHINGTON DC 20310-0110

SAIE-ZA

OCT 2 8 2020

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Policy on Building Automation Systems

1. References. A complete list of references is in enclosure 1.

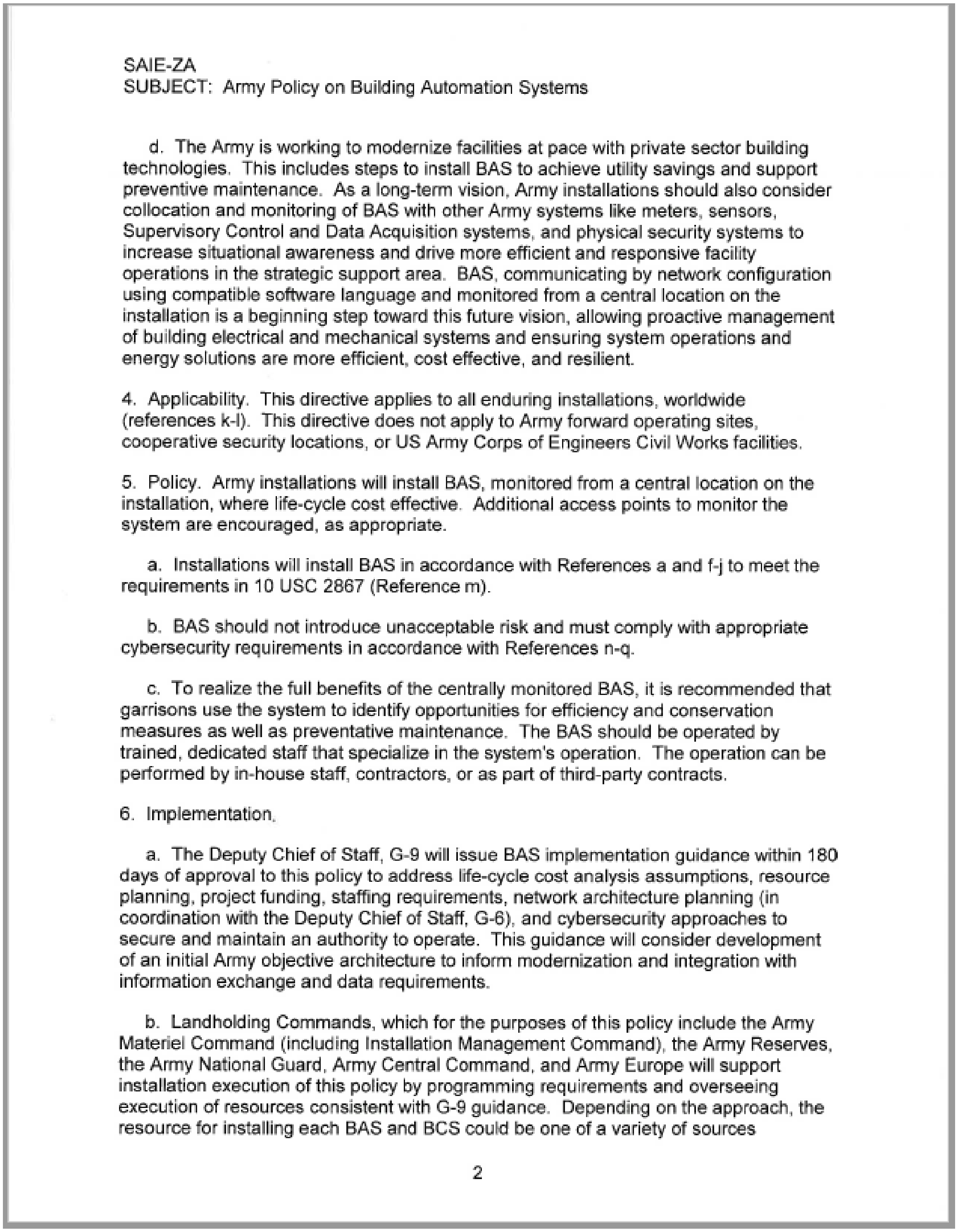
2. Purpose. This policy requires Army installations to install building automation systems (BAS) monitored from a central location at the installation as a way to reduce energy and water commodity and maintenance costs.

3. Background.

a. As defined in Unified Facilities Criteria (UFC) 3-470-01 (reference a), a BAS is the system consisting of the utility monitoring and control system (UMCS) front-end and connected building control systems (BCS) which provides for control of the building electrical and mechanical systems as well as a user interface and supervisory capability (i.e., the portion of the UMCS for building control and excluding any connected utility control system).

b. BAS are important tools that installations such as like Fort Benning, Fort Bragg, Fort Hood, and Fort Knox have used to manage the operation of buildings. BAS are used to control building electrical and mechanical systems such as lighting, heating, ventilation, and air-conditioning. BAS, actively monitored from a central location on the installation, can achieve annual energy savings of 5% to 15%, with simple paybacks of 3 to 10 years (References b-e). Real-time system information available through BAS supports predictive and preventive maintenance and has been shown to reduce costs by up to 50% (Reference c). UFC and Unified Facilities Guide Specifications (UFGS) and Army guidance are available to assist with the integration of BCS when constructing or renovating facilities (Reference a and f-k

c. More extensive implementation of cybersecure BAS across Army installations, as well as use of modern analytics, can serve to strengthen readiness while reducing cost. The effective use of BAS can help installations reduce energy through efforts such as establishing heating and cooling set-points and set-back hours; ensuring equipment is not left in manual override mode; enabling operations and maintenance improvements through retro-commissioning; and implementing controls improvements through re-tuning measures. A centralized monitoring system at the installation level enables diagnostics to ensure persistence of retro-commissioning and re-tuning measures designed to continue efficient operation of building systems, while maintaining a healthy indoor working environment.



d. The Army is working to modernize facilities at pace with private sector building technologies. This includes steps to install BAS to achieve utility savings and support preventive maintenance. As a long-term vision, Army installations should also consider collocation and monitoring of BAS with other Army systems like meters, sensors, Supervisory Control and Data Acquisition systems, and physical security systems to increase situational awareness and drive more efficient and responsive facility operations in the strategic support area. BAS, communicating by network configuration using compatible software language and monitored from a central location on the installation is a beginning step toward this future vision, allowing proactive management of building electrical and mechanical systems and ensuring system operations and energy solutions are more efficient, cost effective, and resilient.

4. Applicability. This directive applies to all enduring installations, worldwide (references k-l). This directive does not apply to Army forward operating sites, cooperative security locations, or US Army Corps of Engineers Civil Works facilities.

5. Policy. Army installations will install BAS, monitored from a central location on the installation, where life-cycle cost effective. Additional access points to monitor the system are encouraged, as appropriate.

a. Installations will install BAS in accordance with References a and f-j to meet the requirements in 10 USC 2867 (Reference m).

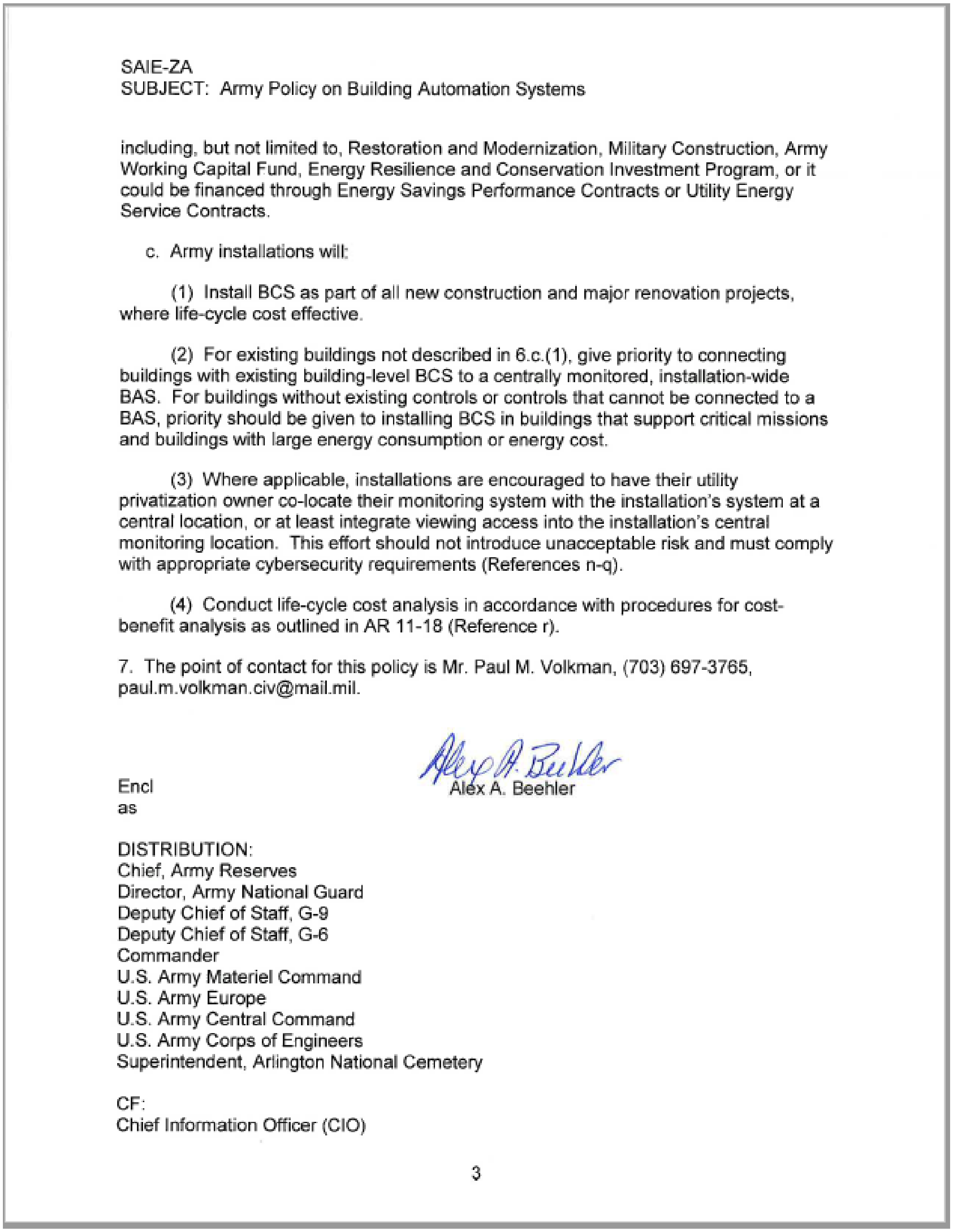
b. BAS should not introduce unacceptable risk and must comply with appropriate cybersecurity requirements in accordance with References n-q.

c. To realize the full benefits of the centrally monitored BAS, it is recommended that garrisons use the system to identify opportunities for efficiency and conservation measures as well as preventative maintenance. The BAS should be operated by trained, dedicated staff that specialize in the system's operation. The operation can be performed by in-house staff, contractors, or as part of third-party contracts.

6. Implementation.

a. The Deputy Chief of Staff, G-9 will issue BAS implementation guidance within 180 days of approval to this policy to address life-cycle cost analysis assumptions, resource planning, project funding, staffing requirements, network architecture planning (in coordination with the Deputy Chief of Staff, G-6), and cybersecurity approaches to secure and maintain an authority to operate. This guidance will consider development of an initial Army objective architecture to inform modernization and integration with information exchange and data requirements.

b. Landholding Commands, which for the purposes of this policy include the Army Materiel Command (including Installation Management Command), the Army Reserves, the Army National Guard, Army Central Command, and Army Europe will support installation execution of this policy by programming requirements and overseeing execution of resources consistent with G-9 guidance. Depending on the approach, the resource for installing each BAS and BCS could be one of a variety of sources



SAIE-ZA
SUBJECT: Army Policy on Building Automation Systems

including, but not limited to, Restoration and Modernization, Military Construction, Army Working Capital Fund, Energy Resilience and Conservation Investment Program, or it could be financed through Energy Savings Performance Contracts or Utility Energy Service Contracts.

c. Army installations will:

(1) Install BCS as part of all new construction and major renovation projects, where life-cycle cost effective.

(2) For existing buildings not described in 6.c.(1), give priority to connecting buildings with existing building-level BCS to a centrally monitored, installation-wide BAS. For buildings without existing controls or controls that cannot be connected to a BAS, priority should be given to installing BCS in buildings that support critical missions and buildings with large energy consumption or energy cost.

(3) Where applicable, installations are encouraged to have their utility privatization owner co-locate their monitoring system with the installation's system at a central location, or at least integrate viewing access into the installation's central monitoring location. This effort should not introduce unacceptable risk and must comply with appropriate cybersecurity requirements (References n-q).

(4) Conduct life-cycle cost analysis in accordance with procedures for cost-benefit analysis as outlined in AR 11-18 (Reference r).

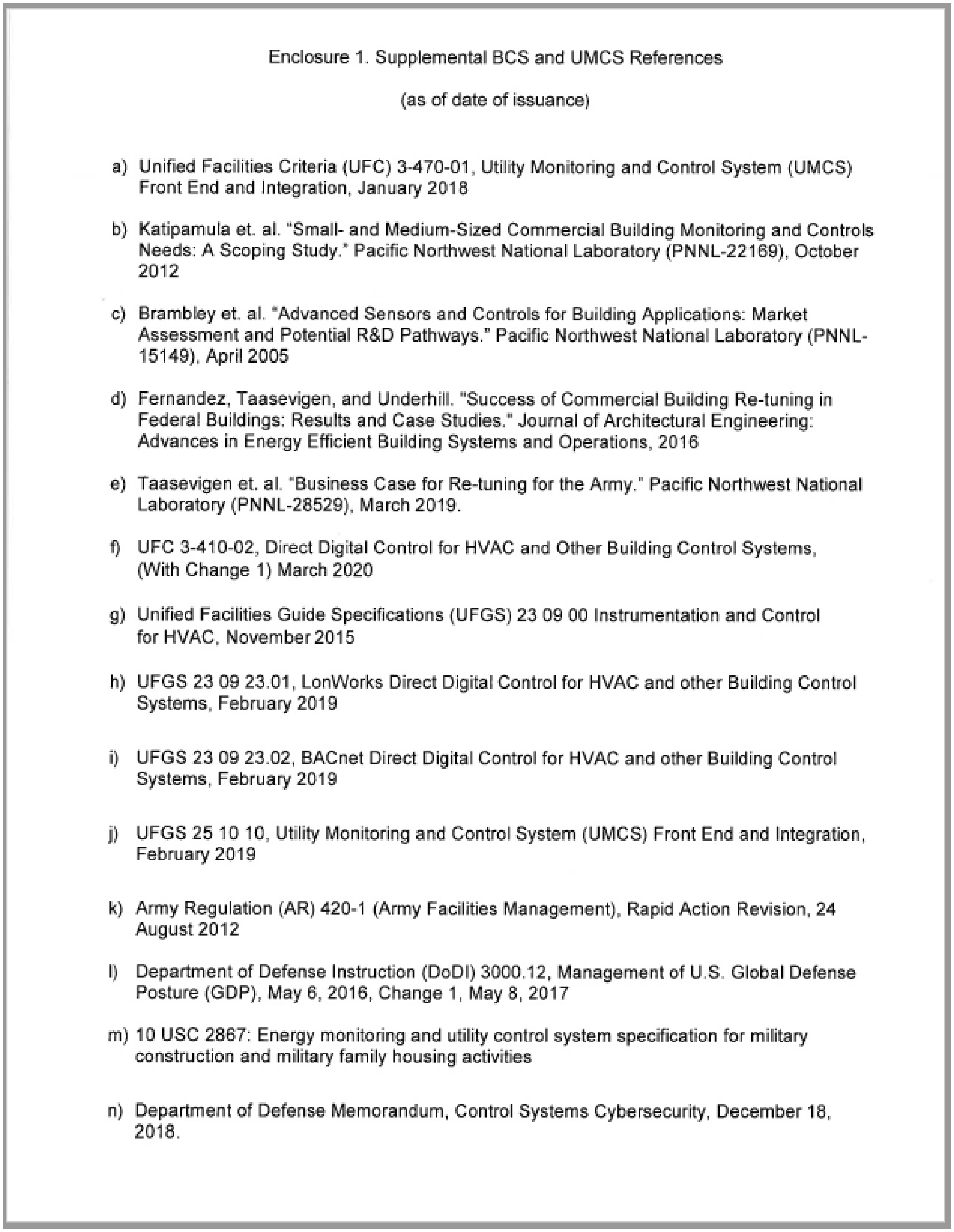
7. The point of contact for this policy is Mr. Paul M. Volkman, (703) 697-3765, paul.m.volkman.civ@mail.mil.

Alex A. Beehler
Alex A. Beehler

Encl
as

DISTRIBUTION:
Chief, Army Reserves
Director, Army National Guard
Deputy Chief of Staff, G-9
Deputy Chief of Staff, G-6
Commander
U.S. Army Materiel Command
U.S. Army Europe
U.S. Army Central Command
U.S. Army Corps of Engineers
Superintendent, Arlington National Cemetery

CF:
Chief Information Officer (CIO)



Enclosure 1. Supplemental BCS and UMCS References

(as of date of issuance)

a) Unified Facilities Criteria (UFC) 3-470-01, Utility Monitoring and Control System (UMCS) Front End and Integration, January 2018

b) Katipamula et. al. "Small- and Medium-Sized Commercial Building Monitoring and Controls Needs: A Scoping Study." Pacific Northwest National Laboratory (PNNL-22169), October 2012

c) Brambley et. al. "Advanced Sensors and Controls for Building Applications: Market Assessment and Potential R&D Pathways." Pacific Northwest National Laboratory (PNNL-15149), April 2005

d) Fernandez, Taasevigen, and Underhill. "Success of Commercial Building Re-tuning in Federal Buildings: Results and Case Studies." Journal of Architectural Engineering: Advances in Energy Efficient Building Systems and Operations, 2016

e) Taasevigen et. al. "Business Case for Re-tuning for the Army." Pacific Northwest National Laboratory (PNNL-28529), March 2019.

f) UFC 3-410-02, Direct Digital Control for HVAC and Other Building Control Systems, (With Change 1) March 2020

g) Unified Facilities Guide Specifications (UFGS) 23 09 00 Instrumentation and Control for HVAC, November 2015

h) UFGS 23 09 23.01, LonWorks Direct Digital Control for HVAC and other Building Control Systems, February 2019

i) UFGS 23 09 23.02, BACnet Direct Digital Control for HVAC and other Building Control Systems, February 2019

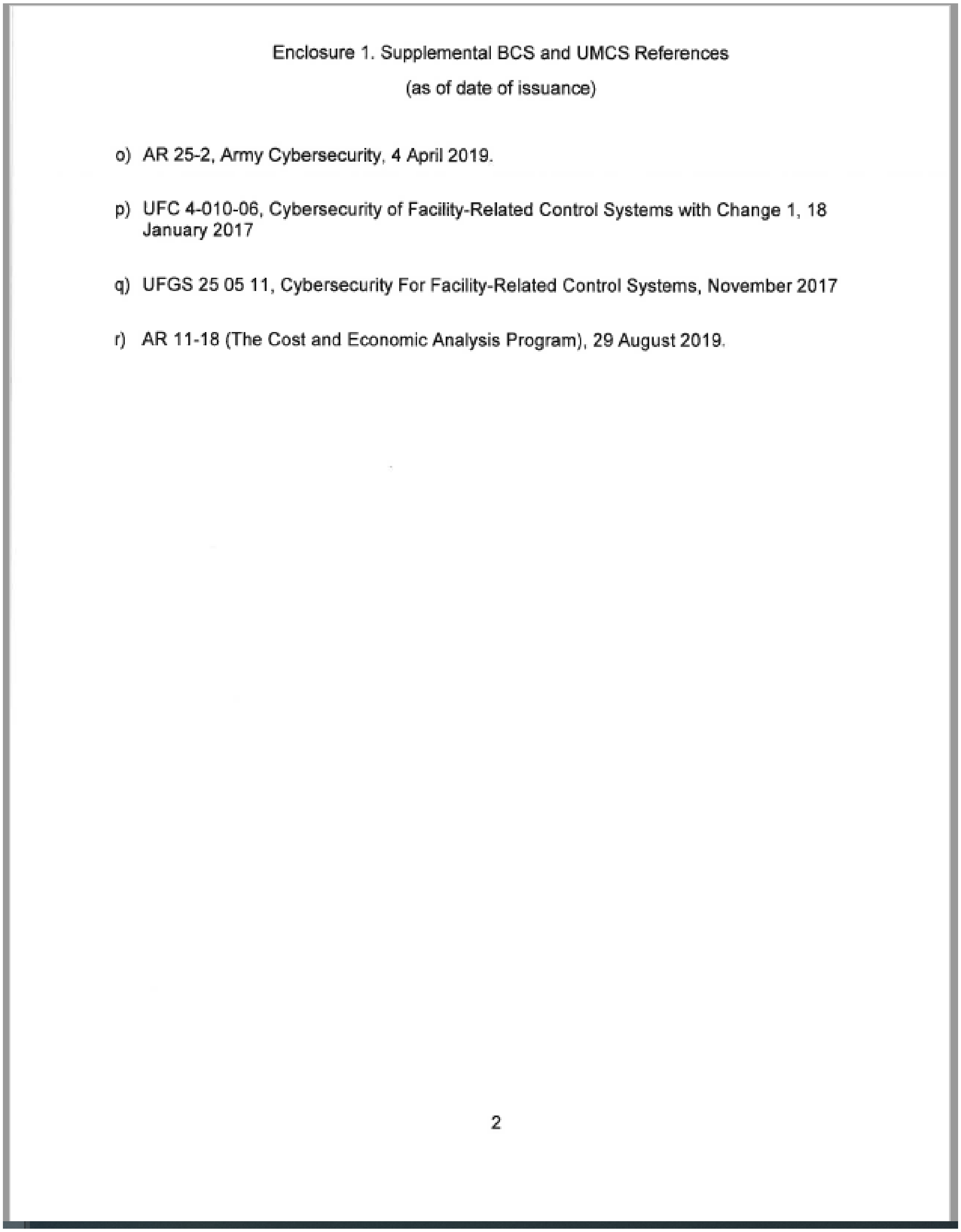
j) UFGS 25 10 10, Utility Monitoring and Control System (UMCS) Front End and Integration, February 2019

k) Army Regulation (AR) 420-1 (Army Facilities Management), Rapid Action Revision, 24 August 2012

l) Department of Defense Instruction (DoDI) 3000.12, Management of U.S. Global Defense Posture (GDP), May 6, 2016, Change 1, May 8, 2017

m) 10 USC 2867: Energy monitoring and utility control system specification for military construction and military family housing activities

n) Department of Defense Memorandum, Control Systems Cybersecurity, December 18, 2018.



Enclosure 1. Supplemental BCS and UMCS References

(as of date of issuance)

o) AR 25-2, Army Cybersecurity, 4 April 2019.

p) UFC 4-010-06, Cybersecurity of Facility-Related Control Systems with Change 1, 18 January 2017

q) UFGS 25 05 11, Cybersecurity For Facility-Related Control Systems, November 2017

r) AR 11-18 (The Cost and Economic Analysis Program), 29 August 2019.

Appendix C: SOW: UMCS Site Survey

STATEMENT OF WORK
FOR
UTILITY MONITORING AND CONTROL SYSTEM (UMCS) SITE SURVEY
at [Post Name]

[***Specifier/designer note:*** *This sample statement of work (SOW) must be tailored to installation-specific requirements. Refer to the yellow-highlighted, square bracket [ ] items for tailoring options and locations that need to reflect local conditions and requirements. This SOW is intended to be a fairly high-level survey, but not intended to obtain sufficient detail or information to write SOWs for the procurement of new/replacement BCSs.*]

1. OVERVIEW

The objective of this work is to create a site survey, execute the site survey, and generate a prioritized list of buildings that are candidates for inclusion as part of a basewide UMCS. The work will also identify and obtain basic information about any preexisting UMCS front end(s) that are candidates for becoming the basewide front end. The work also includes obtaining information about any applicable (prior or ongoing) UMCS and control system planning and guidance such as an Installation Design Guide (IDG).

2. DESCRIPTION OF WORK

Create a site survey based on this SOW and Exhibit A. Execute the site survey via site-visit inspections and interviews. Create a prioritized list of buildings that are candidates to be part of a basewide UMCS. A goal is to help the installation understand the potential to create a UMCS based on an Open Control Systems technology: (using either BACnet, LNS LonWorks, Niagara BACnet, or Niagara Lonworks in accordance with UFGS 25 10 10 and 23 09 23.

This SOW covers all services to perform site visits and prepare reports based on the site visits. These services will include pre-site visit planning and coordination with all team members, on-site coordination assistance/participation, identification of applicable building characteristics and categories, development of site-specific survey procedures, and creation of a UMCS Survey Report.

3. TASKS

The Contractor shall perform the work described in this SOW and the following tasks.

3.1 Pre-site visit activities

a. Conference Call. Participate in a conference call with **[name/office/email]** to review the technical requirements of this SOW. The purpose will be to go over the thrust of the effort, to identify all initial points of contact, and to solidify the details of the site visit and the reports.
Anticipated level of effort: **[0.5]** days.
b. Site Survey Procedure. Prepare the site survey procedure (e.g., spreadsheet, data sheets, logs, etc.) based on exhibit A. Obtain as much information listed in exhibit A as possible in advance of site visits.
Anticipated level of effort: **[5]** days.

3.2 Site visits

Perform site visit(s) to execute the site survey procedure. Contact the Government-supplied site Point of Contact (POC) to schedule site visit(s) with appropriate personnel to assist in performing the tasks described in the SOW. Personnel may include the Energy Manager, DPW Chief of O&M division, DPW Chief of O&M production control, DPW Shop Foreman, DPW Work Leader, Engineering Services Branch Chief, DPW HVAC staff, DPW Controls Staff, DPW A-76 Contractor (Information Assurance Professional [IAP]) HVAC, and the DPW A-76 Contractor controls staff. Notify the Government of scheduled site visit(s).

Anticipated level of effort: **[1 person-day per 2 buildings]**: *Assumes: typical building 30,000 ft^2, much repetition for simple buildings (barracks, dining halls, battalion HQ, etc.)*

3.3 Site survey report

Provide a site survey report documenting the results of the site visits and site survey procedure. The report will include an executive summary, the items listed in exhibit A, and a prioritized list of buildings that are candidates for inclusion as part of a basewide UMCS. The survey report must also include the prioritized list of buildings in a spreadsheet with a sortable column for each piece of information and characterization category.

Anticipated level of effort: **[12]** days. *Assumes: small to medium size installation.*

4. SUBMITTALS AND PERFORMANCE SCHEDULE

4.1 Submittals

Provide all deliverables electronically to **[name and email]**. Deliverables include the following:

- Kickoff meeting or conference call—notes and actions.
- Site Survey Procedure—draft. PDF format.
- Site Survey Procedure—final. PDF format.
- Site Survey Report—draft. PDF format.
- Site Survey Building Priority list—draft. Microsoft (MS) Excel spreadsheet format.
- Site Survey Report—final. PDF format.
- Site Survey Building Priority list—final. MS Excel spreadsheet format.

4.2 Performance Periods and Submission Schedules

The performance periods and submission schedules for each item are indicated below. All activities must be completed by **[date]**.

Item	Due (calendar days)
a. Notice to Proceed	---
b. Kickoff Conference Call	14 days after award
c. Kickoff Conference Call—notes/actions	7 days after item b
d. Site Survey Procedure—draft	30 days after item c
e. Site Survey Procedure—review meeting/conf. call	14 days after item d
f. Site Survey Procedure—final	14 days after item e
g. Site Visit(s)	**[20] [40] [60]** days after item f
h. Site Survey Report—draft (including Site Survey Building Priority spreadsheet.)	30 days after item g
i. Site Survey Report—review meeting/conference call	14 days after item h
i. Site Survey Report—final (including Site Survey Building Priority spreadsheet.)	14 days after item i

5. EXHIBITS.

EXHIBIT A

The **Site Survey Procedure** consists of three parts and will include but will not be limited to the following information:

Part 1. **Documentation and Policies.** The site survey includes general information relative to UMCS front end and building control system planning and priorities and addresses the following questions:

1. Does the installation have an IDG that addresses UMCS or building control systems? What documentation does the installation have that addresses the UMCS or building control system preferences, goals, design, or specifications?
2. Have any prior assessments related to UMCS or control systems been done that might benefit or otherwise impact basewide UMCS plans or priorities?
3. Are there any construction or renovation projects or efforts currently underway that might impact basewide UMCS plans or priorities?

Part 2. **UMCS Front End(s)**. The site survey includes information on preexisting front-end (FE) systems that might qualify as the FE for a (future) basewide UMCS and addresses the following questions:

1. Preexisting UMCS front end(s), manufacturer name, brand, model of FE, number of buildings, list of systems connected to the FE. Is the FE compliant with UFGS 25-10-10? Is the FE judged to be a candidate for being/becoming the FE as part of a basewide system?
2. Condition of front end(s), local staff satisfaction with, impressions of, and/or concerns with the front end(s)
3. Who are the users or operators of the front end(s), including agency, office, branch, and shop (e.g., Energy Manager, DPW Technicians, DPW Engineers, Contracted HVAC Controls, In-House O&M, Contracted O&M, or other)? Do others need or want access?
4. What is the FE(s) used for (e.g., trending, alarming, scheduling, demand limiting, diagnostics, or other)? What is the surveyor's judgement or opinion on the utilization of the FE(s) and how it might be improved?
5. Does the FE(s) have adequate staffing and support?
6. What support mechanisms are available for the FE. (e.g., local Contractors or companies)
7. Does the FE(s) have cybersecurity risk management framework (RMF) authority to operate (ATO)? What is the general status of the cybersecurity situation (local policy status, compliance issues, concerns, challenges, etc.)?

Part 3. **Building List.** The surveyor should obtain basic information and metrics as described in this section and make observations regarding individual buildings and control systems condition as described below:

1. Total number of buildings at the installation to be surveyed is **[quantity]**. Exceptions and clarifications are as follows:
    a. Exclude: Family housing

    b. Exclude: Nonpermanent structures. Do include nonpermanent structures that typically periodically have occupants (e.g., WWII barracks that are still being used)
    c. Exclude: Buildings and structures with no heating or cooling
    d. **[Exclude/Include: describe/list]**
2. General information (for each building)
    a. Building number (building name is optional)
    b. Building or facility usage type (barracks, battalion HQ, training, day care, etc.)
    c. Square footage
    d. Duplicate. Indicate if the building is a duplicate of other building(s)
    e. Networked. Does building have a network connection?
3. HVAC information (for each building)
    a. Type and quantity of mechanical systems or units
        i. Air handling units (AHUs), package units, roof top units, split systems, boilers, chillers, etc.
        ii. Terminal units and small units. Provide an estimate (not an eyes-on count) of terminal units and multiple quantities of small units (e.g., Fan Coil Units (FCUs), perimeter radiators, Variable Air Volume (VAV) boxes, cabinet heaters, etc.).
    b. Point count estimate. Refer to Table [, which includes hardware input and output I/O points, setpoints, and other settings such as those typically displayed on a front-end graphics display.
    c. Point count estimate for front-end licensing. Number of alarms, trends, and occupancy schedules as may be necessary to meet licensing requirements for the front-end monitoring and control (M&C) software. Note: Refer to the Table below and note that the Points Schedules associated with UFGS 23 09 93 can be useful in estimating these numbers.

Table [#] Point count estimates (excerpted from UFC 3-470-01).

System	Points	Trends
Terminal unit (fan coil, VAV box, etc.)	5–15	1–5
Small, packaged AHU	20–30	4–8
Medium, built-up AHU	25–50	10–15
Large, complex AHU	30–60	15–20
Small, package chiller or boiler	10–20	5–15
Large central plant chiller	30–60	20–30
Large central plant boiler	20–40	15–25
Hydronic pumping system	15–25	5–10

4. Energy information (for each building)
    a. Fuel sources used
    b. Mbtu/year estimate for each fuel source (or “actual” if available)
5. Mechanical system(s) and control system(s) condition (for each building)
    a. For each **[system][building]**, provide a numeric rating (e.g., 1 to 10) of the control system(s) condition and suitability for interface with a UMCS. Base the rating on an estimate or judgement defined by the Contractor to take into account the HVAC and control system(s) condition, age, modernity, and type of controls, taking into account the suitability and condition of the HVAC system(s).
    b. For each **[system][building]**, provide a numeric rating recommendation of whether or not to incorporate into a basewide UMCS (e.g., 1=yes, 2=maybe, and 3=no). Include a brief commentary or comment, including the basis for the recommendation.
6. Control system(s) technology for each **[system][building]**
    a. Identify type: Pneumatic, electric, DDC, or other (if other, indicate type).
    b. For DDC, identify manufacturer and brand(s) and communication protocols (and associated technology) used (e.g., proprietary, BACnet, LonWorks, or Niagara Framework). Indicate if there is a router or gateway, along with quantity.

Appendix D: Cyber: An Introduction to Cybersecurity for Building Control Systems for the IT Person

This appendix provides an introduction to cybersecurity for building control systems for the IT person who is concerned with the accreditation of these systems. It includes a presentation of key features of building control systems (BCS) that are different from information technology (IT with a focus on how these differences affect cybersecurity.

Control systems for heating, ventilation and cooling systems (HVAC) and other BCS were once self-contained at the individual pieces of equipment (such as a boiler, chiller, electrical switchgear, etc.). These systems have evolved into more complex interconnected networks that overlap at times with (IT networks. This evolution in these control systems has thrust the IT person into the role of securing the data transmissions to and from equipment controllers.

There are significant differences between the BCS world and IT world that are compiled here for the IT person's reference. The primary differences are often described as "IT vs OT"—whereas a traditional IT system is primarily concerned with the storage, transmission, and security of information; a BCS is operational technology (OT) and is primarily concerned with the operation of physical, real-world equipment.

The IT/OT differences include

- use of identical terms to mean different things,
- what constitutes an "incident,"
- results of incidents,
- variety of attack vectors and constraints,
- corresponding responses to those attacks,
- lifetime and stability of systems,
- monitoring and maintenance requirements, and
- approaches to cybersecurity.

Differences in terminology between IT and OT can lead to confusion because the meaning or intent can become unclear. A simple statement such as “we need to replace the switch in the conference room” can mean two very different things, depending on which “language” one is using, much in the same way “I dropped my torch in the leaves” implies very different levels of danger in American English (where a torch is a flaming piece of wood) and British English (where it is a flashlight). The following table summarizes some notable terminology differences, but it is far from exhaustive. The important point is that when talking about control systems and cybersecurity it is vital to be sure everyone is understanding the “language” being spoken.

Table D-1. Notable terminology differences between IT and OT

Term	IT Perspective	OT perspective
Switch	Ethernet switch. One physical network connection per end device, and one switch per X devices. Tens to hundreds per building	A physical switch—light switch, pressure switch, flow switch, hand-off-auto switches. Many switches may connect using analog signals to a single controller. Hundreds to thousands per building
Gateway	A device on an IP network that sends network traffic to other IP networks	A protocol translator. May or may not use IP at all
Router	An IP router—a device that filters traffic between two or more IP networks. A special type of router in the OT sense of the word	A device that filters control protocol traffic between two or more networks by destination address. Note that there are no conditions on the type of network; there are control protocol routers that have no IP connections. Often defined by the IT world as an “end device”
Network	An IP network or a selection of wireless networks	Any kind of network, including TP/FT-10, RS-485, etc.
Off-Normal Event	Usually, an attempt at unauthorized access	Anything that causes an alarm in the control system (e.g., temperatures too far from setpoint, mechanical actuators not moving as expected, or motors failing to start)

Cybersecurity considers three primary objectives:

a. Confidentiality (safeguarding inside information from exposure to an outsider)
b. Integrity (maintaining accuracy of information in the system)
c. Availability (maintaining functionality of the system so that it is ready to use)

The highest concerns for the cybersecurity[29] of an IT system are typically data confidentiality and accessibility. Common complaints from the loss of those objectives during an off-normal incident take the form of “My data was stolen!” or “I cannot use my computer!” A loss of confidentiality in IT system data generally carries a financial impact (such as the costs of safeguarding individuals from identity theft after the leaking of personally identifiable information (PII), but it can also result in mission impact (with the leaking of classified information that may reveal battle plan methods and vulnerabilities). Loss of the use of data can also impact staff efficiency and business operations by causing the need to reconstruct or regather the data. These tasks may slow daily progress.

However, in HVAC control systems the overriding concern from an off-normal incident is not to protect the data transmissions but to keep mechanical and electrical equipment working and working correctly—which means protecting availability and integrity. The impact of data loss from OT equipment is often minimal or hard to quantify. For example, the knowledge of the room temperature of an office space, or the fact that a circulation fan is on at any particular moment, is not of much value to people outside of the building. The impact of the loss of the equipment itself, or of unauthorized control (not just knowledge) of a system, can affect critical missions through results such as the overheating of computer server rooms leading to computer damage, or the excess growth of mold in an unventilated area leading to unhealthy living spaces, or the waste of natural resources if simultaneous heating and cooling of a space are enabled and result in no net space conditioning or undesirable space conditioning.

Many of these issues are prevented with UMCS design that includes system separation, passwords, protective configurations (e.g., no remote access), software (or hardware) alarms on abnormal conditions, or fault detection diagnostics that check for systems fighting each other.

A common vulnerability of both the IT system and the building control system is that they can both be a platform for attack on other systems, but the vectors and constraints of those attacks are decidedly different. IT systems tend to be more general purpose, where individual components (e.g., computers) have more capability than the typical control system components (e.g., controllers). In addition, computers are connected to an IP network, which by design can carry arbitrary content. This is in marked

[29] See Appendix E and F.

contrast to, say, BACnet over MS/TP, which by design, can only carry BACnet information (e.g., no potential for an SQL injection attack). This is not to imply that control systems are immune from attack or from being used as a platform for attack, but rather, the capabilities of the controller must be understood when evaluating attack vectors. In particular, devices on non-IP networks will likely have limitations on what they are able to do over the network based on the protocol they use.

The results of a compromise must also be evaluated differently in IT and OT systems. The capabilities of information systems are less dependent on outside factors than control systems, and the analysis of the results of compromise for OT systems therefore needs to consider outside factors that IT systems do not. These outside factors can both introduce additional vulnerabilities—new avenues of attack like a pair of wire cutters, a wrench, or a bag of ice draped over a thermostat—and add mitigations, such as physical limits on impact though pressure relief valves and manual controls. The fundamental laws of physics need to be considered—even if one is able to raise the setpoint for a space to 200+ degrees, the space will not ever reach that temperature when the source of heating is hot water at 150 degrees, for example. Similarly, many hypothetical attacks on OT are prevented by building code-mandated hardware safeties—most developed during the early days of OT, when controllers were very prone to failure. For example, one might try to over-pressurize a boiler to blow it up, but the simple pressure relief valve—mandated by code and therefore on every pressure vessel installed in the US—would ensure this did not happen. It is important to note that many of the underlying systems are mechanical in nature—most of the limited O&M budget goes towards mundane activities, such as lubrication, belt and filter replacement, and sensor and actuator calibration. And that most system failures can be traced to a failure of the underlying system.

The lifetime and stability of the two types of systems vary, which affect the monitoring and maintenance requirements. The lifetime of IT systems is short, and there are many changes in software that affect its stability. For example, a department-level server might frequently have user permission changed, storage hardware added or upgraded, new network access, etc. IT systems require frequent changes of automated tools for scanning, patching, and configuration management. IT networks are frequently reconfigured, and VLANs are essential for keeping networks up to date. For this reason, funding is typically reserved with the expectation for regular maintenance (for patches and updates). In contrast, a BCS has a long life, and the stability is static. BCS lifespan is typically 15 years or more, with the underlying equipment having a lifespan of 30+ years in many cases. In contrast to the above server, unless space is reconfigured, a controller on an air handler might never face a changing requirement. Generally, control systems are replaced when they are no longer functioning rather than on a "refresh cycle" like IT, and they are too expensive to replace solely for cybersecurity upgrades. The equipment needs to be maintained, but its configuration seldom changes. Device functionality, programs, and network configuration is largely static over the life of the system. By analogy, the chances are high that one has replaced their home computer in the last few years, but their home furnace or central air conditioner rarely is replaced so quickly. Even updating BCS can be an issue—often updates to BCS are a manual process done locally at the controller, and a bad update can actually cause the system to stop functioning. In addition, as BCSs tend to be under funded and under maintained, available funds tend to be needed more for maintenance to keep the system functioning than for cybersecurity (the idea being that the system MUST work or there is no sense in having it—so a working insecure system is generally preferred to a secure nonfunctional one).

IT approaches to BCS cybersecurity need to recognize the differences between building control systems and IT but also recognize that since some parts of cybersecurity are not technical, policies and procedures for IT and BCS can often be the same. IT functions should be restricted to IT systems. Control systems should not be used for remote access (e.g., for email). Although it is expedient and appropriate to apply standard IT rules and approaches when it makes sense, there are situations that justify modifying the rules. As a simple example—password length and complexity requirements for IT systems will often be impossible for some portions of a control system to meet fully, so reduced requirements will need to be identified and implemented. Of course, the full requirements could be met by the system but only by employing nonstandard solutions and vastly more expensive solutions that HVAC designers, installers, and maintenance staff will not understand—increasing not just the cost but the risk that the system is nonfunctional. The key is to neither arbitrarily require the typical rules for IT nor to dismiss the requirement altogether but, rather, to find a solution that meets the intent of the cybersecurity requirement as much as possible.

A practical approach to cybersecurity of building controls system employs system separation (either physically or logically) and least functionality (configuring a system to provide only essential capabilities) with a prime emphasis on correct HVAC equipment operation. Control systems should be isolated from “business” systems. Maintenance dollars are limited and shared among many parties so cyber solutions should be kept simple to minimize costs and make best use of available resources.

New control systems should be designed with availability and integrity and—if important—confidentiality in mind. This incorporates cybersecurity into the functional design of the system itself. Best practices include utilizing fail-safe operation modes, minimizing reliance on networks, and specifying redundancy of equipment and manual (physical) overrides.

Appendix E: Cyber: Determination of Control System Impact Rating

E.1 Background

This appendix discusses method for determining the cybersecurity impact rating for a building control system. A system is categorized based on an evaluation of the impact associated with the loss of confidentiality (C), integrity (I), or availability (A) (generally written as CIA) in organizational operations, organizational assets, or individuals. The system impact is categorized as high, moderate. or low. This is sometimes referred to as either the CIA level, CIA value, impact level, or security category.

Where this categorization is not provided by the system owner (SO) or authorizing official (AO), the procedures in this appendix may be used to determine interim categorization values to allow the design process to move forward. These values cannot be assumed to be the values that will be used for authorization.

Before defining the system categorization, it is important to understand what is meant by a loss of confidentiality, integrity, or availability, and what is meant by a high, moderate and low impact.

The Risk Management Framework (RMF) considers three types of security breaches:

1. Loss of Confidentiality. Information within the system is leaked to the outside.
2. Loss of Integrity. Information in the system is subject to unauthorized modification.
3. Loss of Availability. The system (or information in the system) is unavailable.

The RMF categorizes systems as LOW, MODERATE, or HIGH based on the potential impact of a security breach. The DoD definitions for LOW, MODERATE, and HIGH impact are given in FIPS-199 (Federal Information Processing Standards) as modified in CNSSI-1253 (Committee on

National Security Systems Instruction,) (CNSSI adds the phrase “exceeding mission expectations” to each definition):

> The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
>
> AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals [exceeding mission expectations].
>
> The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
>
> AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries [exceeding mission expectations].
>
> The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to

have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries [exceeding mission expectations.] (NIST 2004; CNSS 2014)

E.2 System categorization and determination of impact rating

Step 1 of the RMF requires categorizing the system in accordance with Committee on National Security Systems Instruction (CNSSI) 1253. This instruction describes how the CIA impact level is determined by the type of information on the system and mission criticality of the system. Rationales for system categorization will be required and may be supported by four approaches (listed in order of preference):

1. Compare to Similar Systems. This is probably the most defensible and easiest approach: is the project similar to an existing project with established categorization values?
2. Methodical System Review. This is a "common sense" approach to determining impact ratings based on the mission and the relationship the control system has to the mission.
3. Assistant Secretary of the Army (Installations, Energy and Environment) (ASA [IE&E]) Master List. This list included starting-point CIA impact ratings by control system type for three mission criticalities. The values here have generally (and for utility monitoring and control systems [UMCSs], building control systems [BCSs], and utility control systems [UCS] more specifically) been determined through an application of the "common sense" methodical process defined here.
4. National Institute of Standards and Technology (NIST) Guidance. This is the formal way to determine impact ratings but is not easily applicable to control systems. Where it is applicable, the approach used is to determine

CIA using another approach first and then to confirm and document that impact rating determination using the NIST guidance.

E.2.1 Compare to similar systems

At many sites, the project will be similar to existing control systems in similar mission space. It may be possible to simply determine what categorization values were used in the other project and assume those same values in the current project. Note that "similar" in this context must include the following elements (in order from most to least important):

- The other project should have the same organizational AO. Since acceptance of risk is subjective, it is vital to have the same organization accepting the risk.
- The other project must have a control system supporting a mission with a similar impact of the mission itself. Note: this has nothing to do with the control system, it is the criticality of the mission itself. Even if the mechanical systems were identical, a project supporting a mission of "processing real-time battlefield intelligence" cannot be compared to a project supporting a mission of "providing recreational facilities to soldiers."
- The other project must have a similar dependency between the control system and mission. The key question here is "if the control system fails, how much impact is there on the mission?"

If there is a similar project that can be referenced, then a reasonable assumption is that "similar projects will have similar [CIA] impact categorization values." (CNSS, 2014)

E.2.2 Methodical system review

In almost all cases, loss of confidentiality of the information in the control system is of little or no consequence (even when it is, it is generally much less important than integrity or availability) and the impact of the control system is primarily due to loss of integrity or availability. Loss of integrity or availability relates to how these losses may impact the mission supported by the specific facility-related control system (FRCS). Determination of impact for the control system is typically a two-step process:

1. What is the impact of the mission? Will loss of the mission result in a LOW, MODERATE, or HIGH impact?

2. How much will a loss of (integrity or availability of) HVAC controls impact the mission?

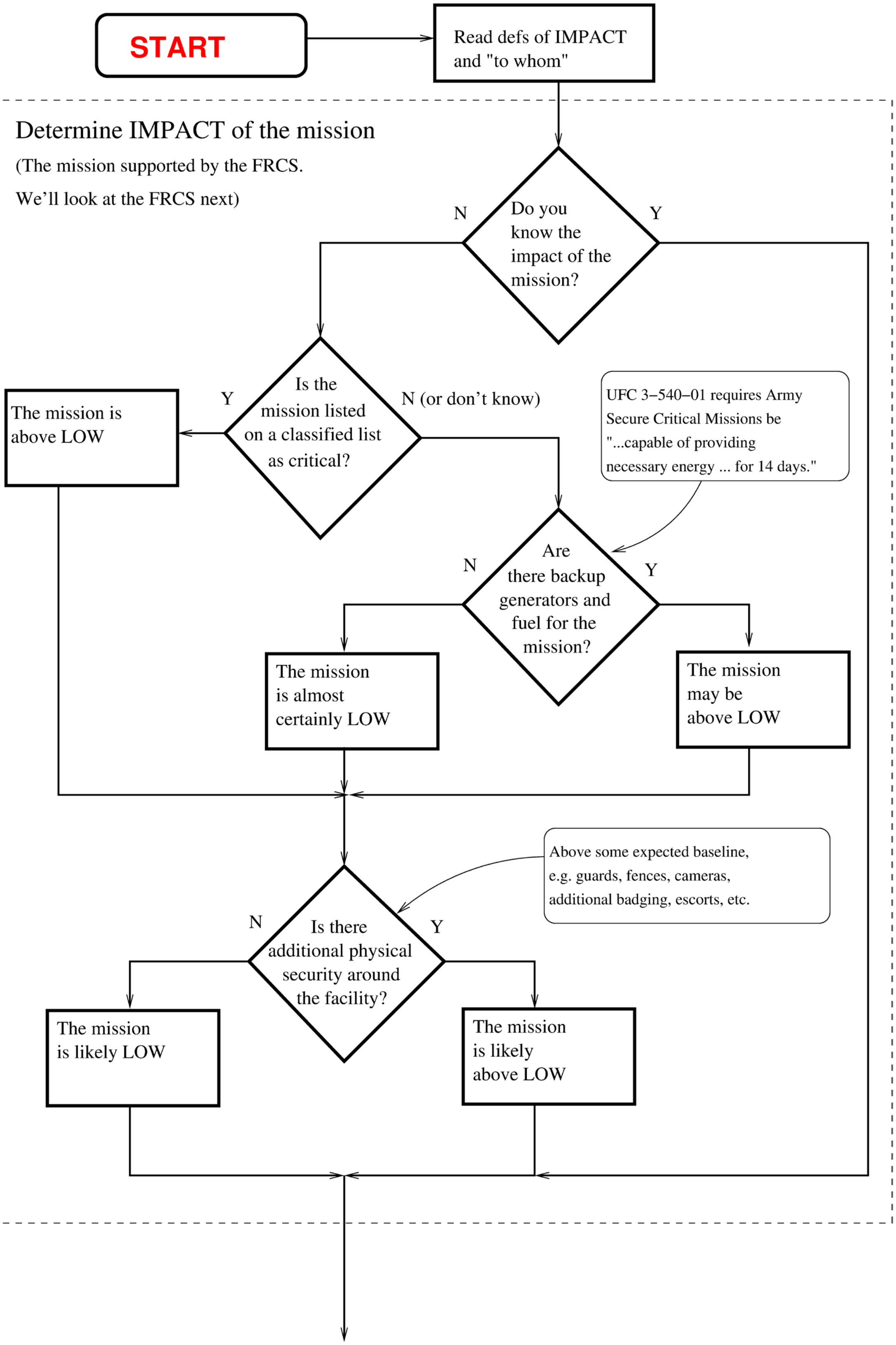
This process will provide a rational ("common sense") starting point for determining criticality of an FRCS but is not official policy. **Ultimately, system criticality is determined by the AO (in coordination with the SO and based on input from the designer of the control system).**

E.2.2.1 Impact of the HVAC control system

Ideally, the AO, SO, or mission tenant will identify the mission impact, but this is often not feasible (mission tenants may not in fact know and frequently overstate their own importance). In cases where the mission impact is not known, or when the claimed mission impact seems exaggerated and confirmation is desired, the flow chart in Figure E-1, Figure E-2, and Figure E-3 may be helpful. The flowchart assumes that availability and integrity have the same impact rating and disregards confidentiality. (Although this is a single flowchart, it has been broken out across three figures to facilitate discussion of the flowchart).

1. The first part of the flowchart, Figure E-1, deals with the determination of the impact of the mission itself. This chart relies on three observations: critical mission facilities are often on a (classified) list of critical facilities.
2. Critical mission facilities generally have a requirement for local backup generators. UFC 3-540-01, *Engine-Driven Generator Systems for Prime and Standby Power Applications* requires that "For Army Secure Critical Missions, the Army will reduce the risk by being capable of providing necessary energy and water for 14 days" (DoD 2019b).
3. Critical mission facilities generally have a requirement for physical security above and beyond what is typical on the installation. Note that this is not definitive: child development centers typically have additional security but might not be considered Mission Critical. These security measures might include such things as additional fencing, cameras, security guards, additional badging, or requirements for escorts inside the facility. When electrical and mechanical infrastructure is outside the facility (e.g., a diesel generator), there is typically a security fence surrounding the facility and the electrical and mechanical infrastructure.

Figure E-1. FRCS impact determination flowchart, part 1—determining mission impact.


START
Read defs of IMPACT and "to whom"
Determine IMPACT of the mission
(The mission supported by the FRCS.
We'll look at the FRCS next)
Do you know the impact of the mission?
N
Y
Is the mission listed on a classified list as critical?
Y
N (or don't know)
The mission is above LOW
UFC 3–540–01 requires Army Secure Critical Missions be "...capable of providing necessary energy ... for 14 days."
Are there backup generators and fuel for the mission?
N
Y
The mission is almost certainly LOW
The mission may be above LOW
Above some expected baseline, e.g. guards, fences, cameras, additional badging, escorts, etc.
Is there additional physical security around the facility?
N
Y
The mission is likely LOW
The mission is likely above LOW

Once the impact of the mission is known, the impact of the FRCS on the mission is evaluated. The flowchart continues in Figure E-2 and Figure E-3 and considers the relationship between the FRCS, the underlying equipment, and the mission itself:

- The consideration is whether the mission depends at all on the equipment controlled by the FRCS. A computer server room is clearly dependent on continuous cooling for operation, while an outdoor training area is clearly not. Other related considerations are
    - How long the mission can function before a loss of the controlled equipment will cause a mission failure. For example, a computer server room might fail completely if it loses cooling for 30 minutes, while an office environment (even one performing a critical function) might continue to function for hours before their mission was impacted and may be able to carry on indefinitely (with some reduced efficiency) without completely failing at their mission.
- The next consideration is the extent that the controlled equipment relies on the FRCS for operation. For example, a lighting system controlled by an occupancy sensor that also has a manual ON/OFF switch relies very little on the occupancy sensor for meeting mission goals. The next several considerations address whether the equipment controlled by the FRCS is critical and examine several factors for indication that the equipment is not critical to the mission. If the equipment is critical, it will likely
    - require the same level of backup power as the supported mission, which normally means local backup power generation,
    - have redundant equipment to allow for failure (e.g., mechanical failure) of a piece of equipment (e.g., broken belt or burned-out bearing), or
    - have local controls available that will allow staff (either installation operations and maintenance [O&M] staff or adequately trained mission staff) to restore operation of the equipment before the mission fails. Note that these manual controls might lead to reduced energy efficiency, but the key point is that the mission can continue with minimal disruption.
- The ability of O&M staff to repair or restore system operation before the mission fails due to the loss of the systems must be considered, as

this ability to repair before failure is a mitigation that would lower the FRCS impact level.

- Finally, the Integrity and Availability impact of the FRCS controls must be equal to or less than the supported mission impact. However, in cases where confidentiality is important, the Confidentiality impact rating of the FRCS impact may exceed the mission impact.

Figure E-2. FRCS impact determination flowchart, part 2a—determining FRCS impact based on mission impact.

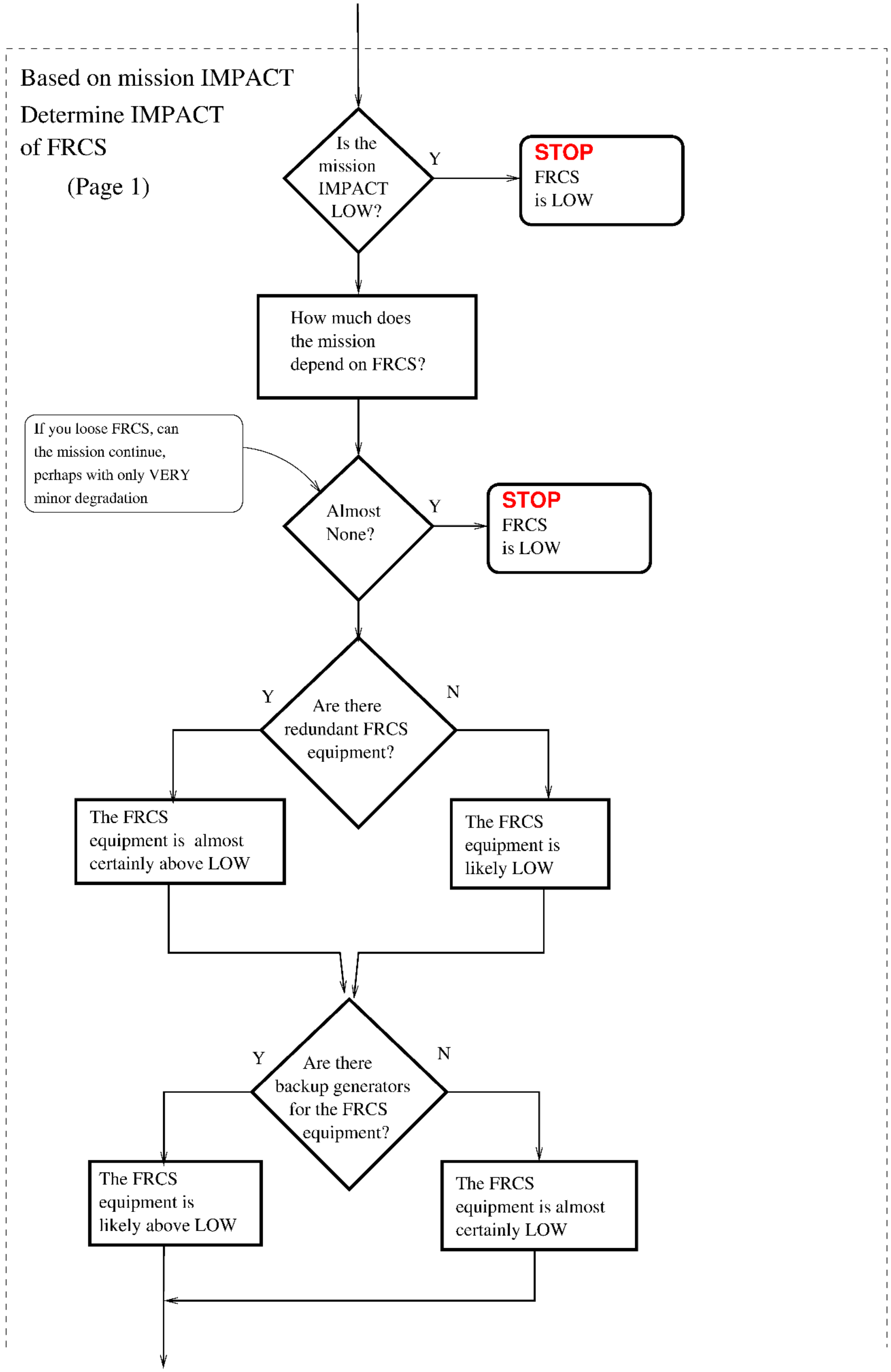
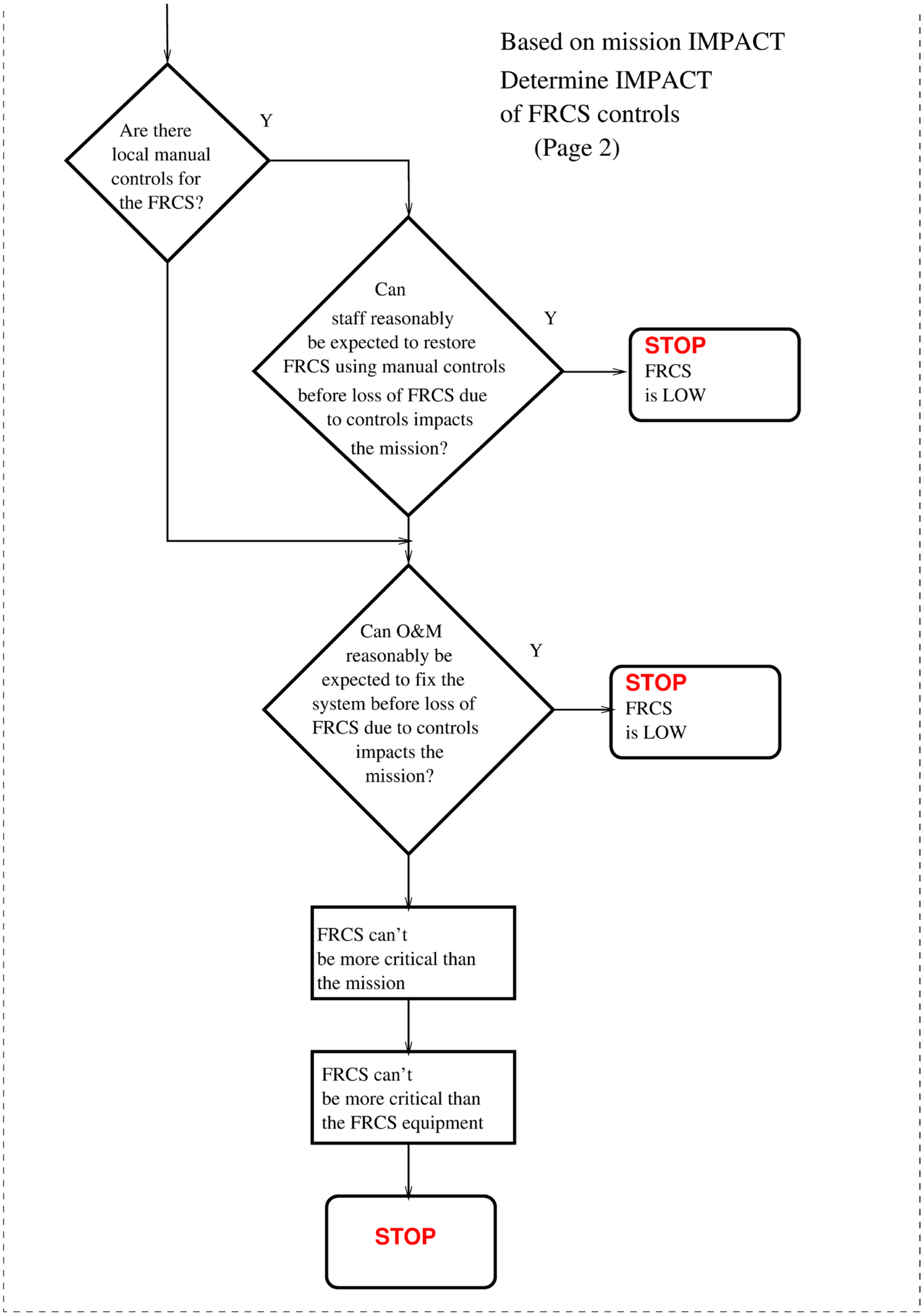

Based on mission IMPACT
Determine IMPACT
of FRCS
(Page 1)
Is the mission IMPACT LOW?
Y
STOP
FRCS is LOW
How much does the mission depend on FRCS?
If you loose FRCS, can the mission continue, perhaps with only VERY minor degradation
Almost None?
Y
STOP
FRCS is LOW
Y
Are there redundant FRCS equipment?
N
The FRCS equipment is almost certainly above LOW
The FRCS equipment is likely LOW
Y
Are there backup generators for the FRCS equipment?
N
The FRCS equipment is likely above LOW
The FRCS equipment is almost certainly LOW

Figure E-3. FRCS impact determination flowchart, part 2b—determining FRCS impact based on mission impact.


Based on mission IMPACT
Determine IMPACT
of FRCS controls
(Page 2)
Are there local manual controls for the FRCS?
Y
Can staff reasonably be expected to restore FRCS using manual controls before loss of FRCS due to controls impacts the mission?
Y
STOP
FRCS
is LOW
Can O&M reasonably be expected to fix the system before loss of FRCS due to controls impacts the mission?
Y
STOP
FRCS
is LOW
FRCS can't be more critical than the mission
FRCS can't be more critical than the FRCS equipment
STOP

E.2.2.2 Addressing the critical control system

Several options for addressing a critical FRCS are suggested by the above drawing:

- Consider if manual controls could possibly be added to compensate for a compromised control system.
- In some critical facilities that are staffed 24/7, consider if a local controls front end might be installed inside the facility and facility staff might be provided sufficient training to make basic adjustments to the system. Another option to consider is the addition of local display panels (limited operator interfaces within the control system) in mechanical rooms, again with the intent of allowing on-site staff the ability to maintain system operation (perhaps in a degraded state, but sufficient to maintain basic mission capabilities).
- Consider if simple, standalone backup systems could possibly be added to compensate for a failed (basewide) control system. For example, for a data center, could a standalone computer room air conditioner (CRAC) unit can be added that would start based on a local thermostat and run independently of the basewide system. Particularly in the case of a critical facility (which likely has redundant HVAC equipment), consider if the primary unit could possibly be connected to the basewide UMCS while the secondary unit might operate in a standalone configuration with purely local controls.
- Some overall noncritical buildings may have a small critical room or facility inside the larger building, consider it may be possible to add a small standalone unit, such as a small direct expansion (DX).

If the standalone system approach is used, this might mean that the standalone system cannot be monitored by the primary systems. Multiple strategies exist to allow for a lower-impact system to monitor a higher-impact system. Some of these strategies are described in UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems* (DoD 2017a).

E.2.3 System categorization based on Facility-Related Control Systems (FRCS) Master List

The Facility-Related Control Systems (FRCS) Master List, available on the Office of the Assistant Secretary of Defense for Sustainment's FRCS cybersecurity website (https://www.acq.osd.mil/eie/IE/FEP_CSC.html), provides preliminary impacts dependent on supported mission criticality. Note that these are preliminary baseline categorizations, and **system criticality is determined by the AO (in coordination with the SO) and is based on input from the designer of the control system.**

The Master List uses three categories of mission criticality into which the facility or mission the system supports will fall. The DoDI 5000.02 defines them as

- Mission Support. Not designated as Mission Essential or critical
- Mission Essential. “is basic and necessary for the accomplishment of the organizational mission (designated by the DoD Component head)”
- Mission Critical. “the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations (designated by the DoD Component head)” (USD [A&S] 2020).

Assuming that the mission is heavily dependent on the FRCS, then the CIA values under the mission criticality for the facility or mission can be used as preliminary CIA values for the FRCS. Table E-1Figure E-1 shows an excerpt of the Master List for UMCS.

Table E-1. UMCS categorization based on mission criticality.

FRCS Type and Description	Preliminary Baseline C-I-A								
	Mission Support			Mission Essential			Mission Critical		
System Name	**C**	**I**	**A**	**C**	**I**	**A**	**C**	**I**	**A**
Utility Monitoring and Control System (UMCS)	L	L	L	L	L	L	L	M	M

* C=confidentiality, I = integrity, A=availability** L=low, M=medium, H-high

Note that the CIA values for Mission Essential or Mission Critical facilities should be lower than shown on the “Master List” if the mission does not depend heavily on the FRCS.

Note also that the Baseline CIA values from the Master List are not policy, rather they are guidance in helping one determine categorization. The focus on determining categorization is in the following instructions on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 (NIST 2008). For example, one may have a physical access control system that does not rise to the suggested CIA impact categorization of MMH (for moderate confidentiality, moderate integrity, and high availability impact) as depicted in the "Master List." Follow the next section and provide a clear concise categorization rationalization.

E.2.4 NIST SP 800-60, Vol. 2, Rev. 1, Information Types

NIST SP 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information System to Security Categories* (NIST 2008) is the authoritative document to help SOs determine the CIA values for the information processing types of their systems.

NIST SP 800-60, Table D-1, "Mission-Based Information Types and Delivery Mechanisms Mission Areas and Information Types" lists information type (NIST 2008, 103).

While many system types are not an ideal match to the systems listed in Table D-1, UMCSs (and HVAC, electrical, and lighting systems) will most likely fall into information systems described in Section D.7, "Energy." The information types in D.7 are

- Energy Supply
- Energy Conservation and Preparedness (common information type for an Army UMCS)
- Energy Resource Management
- Energy Production

NIST SP 800-60, Table D-2 (summarized in Table E-2, below) lists the anticipated CIA categorization for each of the above types. Note that UMCSs fall in the energy conservation and preparedness information type and have a baseline CIA level of low-low-low.

Table E-2. CIA categorization based on information type.

Information Type	Confidentiality	Integrity	Availability
Energy Supply	Low	Moderate	Moderate
Energy Conservation and Preparedness (includes UMCS)	Low	Low	Low
Energy Resource Management (does not include UMCS)	Moderate	Low	Low
Energy Production	Low	Low	Low

This is still not enough information for you to appropriately justify your CIA categorization. Go to NIST SP 800-60 section D.7, “Energy,” and review the definitions of the four types of energy (as listed above) and determine what best fits the system. Select all information types that are applicable to your system. Make sure you look at the definitions of confidentiality, integrity, and availability and any special factors that could elevate the baseline CIA.

E.3 Summary and required categorization rationale

Where applicable, the best approach is likely “compare to similar systems.” If that is not an option, the best approach may be to use the “methodical system review” approach to determine impact level, then select (if there is a plausible fit) the system type from NIST SP 800-60 to defend the decision.

Appendix F: Cyber: Responsible, Accountable, Consulted, and Informed (RACI) Matrix

A powerful yet simple tool that can be used by the UMCS workgroup to support cybersecurity accreditation is a responsible, accountable, consulted, and informed (RACI) matrix that lays out the granular tasks, who the touch points are, and their actions in execution. Additional insights on terms used in this table are provided in Long et al., 2019.

Table F-1. Responsible, accountable, consulted, and informed (RACI) matrix.

Roles-Responsibilities Matrix								
Legend	Responsible (R)	[Party responsible for task]						
	Approval (A)	[Final Approval Authority]						
	Consulted (C)	[In coordination with or makes recommendations]						
	Informed (I)	[Be informed of decision or status]	PDT	Contractor	Customer	Customer G6/NEC/DOIM	SCA-V	Notes
Manage Task Order								
		Ensure Contractor provides required deliverables	R	C	C	C	X	
		Modify Task Order when required	R	C	C	C	X	
		Task Manager	R	C	C	C	X	
		Provide funding required to execute tasks	C	X	R	X	X	
System Design								
		Determine if standalone or networked	C	I	R	C, A	X	
		Determine if child under parent ATO or standalone ATO	C	I	C	R, A	X	
		Define network configurations/architecture options available	C	R	C	C, A	X	
		Determine if hard server or virtualized	C	I	C	R, A	X	
		Define network configurations/architecture "allowable"	C	I	C	R, A	X	
		Develop Network Diagram	C	R	I	C, A	X	
		Develop Data Flow Diagram	C	R	I	C, A	X	
Cybersecurity Requirements								
		Register System APMS	C	I	R	C, A	X	
		Register System eMASS	C	I	R	C, A	X	
		Categorize System (Requires Signed AO Approval Memo)	C	I	R	C, A	X	

Select Security Controls								
		Apply CNNSI 1253 to determine System Classification	C	I	R	C, A	X	
		Apply DoD 800-53 Control Set	I	I	R	C, A	X	
		Apply DoD 800-53A Control Set	I	I	R	C, A	X	
		Determine Supplemental Controls	I	I	R	C, A	X	
		Import results from CSET into eMASS	C	C	R	C, A	X	
		Reach Agreed Baseline with customer/system owner	C	C	R	C, A	X	
		Determine all Data Types to be used in system, per RMF Guidance	C	C	R	C, A	X	
		Overlay Application and Selection	C	C	R	C, A	X	
		Import System Diagrams	C	C	R	C, A	X	
		Develop Monitoring Strategy	C	C	R	C, A	X	
		Finalize Control Set	C	C	R	C, A	X	
		Request Reciprocity Agreements from G6	C	C	R	C, A	X	
Implement Security Controls								
		Apply appropriate STIGs to system	C	R	I	C, A	X	
		Obtain Licensing for ACAS Server	C	C	C	R, A	X	
		Install Converged Security Scanning Server into lab environment	C	R	C	C	X	
		Gather existing system documentation from G6	C	C	R	C	X	
		Develop Contingency Plan	C	C	R	C, A	X	
		Develop COOP Plan	C	C	R	C, A	X	
		Develop System Security Plan	C	C	R	C, A	X	
		Scan/Fix Process	C	R	I	I	X	
		Develop Security Assessment Report	C	R	I	I	X	
		Upload system documentation to eMASS	C	C	R	C	X	
Assess Security Controls								
		Develop Security Assessment Plan	C	C	C	C	X	
		Submit Security Assessment Plan for approval	C	R	C	C, A	X	
		Prepare site for Validation team	C	C	R	C	C	
		Host Validation Team	C	C	R	C	C	
		Collaborate with Validation team to receive results from validation scan	C	R	I	C	C	
		Apply any necessary Scan/Fixes resulting from Validation Team	C	R	I	C	C	
		Prepare system POA&M	C	R	I	C	X	
		upload POA&M into eMASS	C	C	R	C	X	
		Prepare any final system documentation	C	R	C	C	X	

		Submit RMF Package to AODR	C	C	R	C	X	
Authorize System								
		Collaboration meeting with AODR	C	I	R	C	X	
		Receive Decision from AO	I	I	R	C, A	X	
Monitor Security Controls								
		Apply Monitoring Strategy to system	I	I	R	C	X	
		Updates and Patching	I	C	R	C	X	
Third Party Validation								
		Documents and Reports Review	I	C	I	C	R	
		Scans & Test	I	C	I	C	R	
		Apply any necessary Scan/Fixes resulting from Validation Team	I	R	I	C	C	
		3rd Party Recommendation to AO	I	I	C	C, A	R	
Authority to Connect (ATC) Process								
		Request ATC	I	I	R	C, A	X	

Appendix G: UMCS Manager—Position Description

G.1 Introduction

This document introduces a UMCS Manager position and includes the recommended relative authority level in the organizational hierarchy and position description duties verbiage.

It is recommended that a new independent UMCS organization, headed by the UMCS Manager, be created directly under the Director of the DPW. Ideally, the UMCS Manager would be at a Division Chief level to facilitate interactions with other Division Chiefs in the DPW; however, staffing levels do not appear to justify a Division Chief position, and the creation of a new branch is recommended. Placing the UMCS Manager directly under the Director of DPW helps ensure that the UMCS Manager can influence the other divisions within the DPW without answering to a particular Division Chief.

If adding a new organization directly under the Director of DPW is not practical, it is recommended that a new UMCS branch headed by the UMCS Manager be created in the Operation and Maintenance (OMD) or Business Operation and Integration Division (BOID). While the Energy Manager (the closest most installations currently have to a UMCS Manager) is often located in the Environmental Division, it is strongly recommended that, due to the extensive interaction between HVAC O&M staff and the UMCS, the UMCS Manager be located in the O&M Division. Many O&M Divisions already have a “Controls Shop” or “UMCS Shop” of some sort, so this location is not without some precedent and will facilitate O&M ownership of the UMCS.

Regardless of the actual implementation of the UMCS Manager, this position must be given responsibility for and authority over the UMCS, including related installation processes (such as O&M and design standards for controls).

It is critical that the UMCS Manager have a position in the organization and requisite authority and responsibility needed to effectively manage the

UMCS. It is recommended that the UMCS Manager be established as a new position and that the UMCS Manager be the head of an independent organization reporting directly to the Director of DPW (such as a branch or division). This helps ensure that the UMCS Manager can influence the other divisions within the DPW without answering to a particular Division Chief.

As the person responsible for the UMCS, the UMCS Manager has authority to accept or reject BCS and UMCS project submittals and other work and should be at a sufficient level to interact directly with decision makers in the NEC.

Because of their responsibility for contract approvals and the ability to commit the Government, as well as their interaction with other DPW and NEC staff, the UMCS Manager must be a Government position.

G.2 Position Description Verbiage

Position Description
UMCS Manager

Draft: 2019-09-27

A. DUTIES:

The UMCS Manager works under the very general supervision of the Director of Public Works, who establishes overall broad outlines of objectives and policy guidance. Incumbent is assigned long-term, continuing responsibility for independently managing the installation's UMCS, consisting of the utility monitoring and control system (UMCS) and building control systems (BCS). This responsibility includes independently planning, designing, and carrying out major projects or studies which impact the performance of the UMCS. Incumbent works with significant independence and freedom from technical control to plan and complete projects and assignments of substantial variety and complexity. Incumbent works with other branches to coordinate overlapping and interrelated technologies. The supervisor sets general priorities and establishes objectives and is consulted on significant work problems or highly controversial matters. Completed work is reviewed in terms of effectiveness of results achieved. UMCS Manager acceptance of work by others (Contractors) is considered as technically authoritative, normally constituting the basis for final approval or endorsement by the installation command group, as applicable.

Work is centered upon the attainment of goals and compliance with agency policies and regulations. Supervisor is kept informed through info0rmal discussions, conferences, and consultations.

B. MAJOR DUTIES:

1. The primary purpose of this position is to manage all aspects of the UMCS and assume responsibility and authority to make local decisions concerning the UMCS, including planning, project prioritization and system operation. This position is the designated office of record for technical files and procurement initiatives and will maintain this designation.
2. Serves as a technical authority on UMCS-related issues and champions the UMCS to garrison leadership to secure funding and support. Serves as the single point of contact for the <GARRISON> UMCS and BCS. Prepares reports and briefings to activity supervisors, commander, and higher headquarters on progress and status of the UMCS. Briefs command group, Office of the Inspector General (IG), and higher headquarters inspection teams on the UMCS.

   Plans and programs for the UMCS. Develops plans for and coordinates implementation of the UMCS. Develops, documents, and maintains the UMCS and UMCS policies and procedures. Stays abreast of, interprets, and implements UMCS-related policy and regulations. Conducts feasibility studies, prepares preliminary design concepts, and develops statements of work (SOW) and serves as Contracting Officer Representative (COR) for these SOWs as needed. Reviews Value Engineering proposals for proposed improvements to the UMCS.

   Works with other divisions within the Directorate of Public Works (DPW) to provide oversight, review, and approval of in-house designs as they pertain to the UMCS. Including working with the

- Engineering Division to ensure UMCS requirements are in design documents (in-house and out of house), project submittals meet UMCS requirements, Quality Assurance (QA) and commissioning procedures are adequately executed to ensure that they meet UMCS requirements
- O&M Division to coordinate UMCS use and maintenance with O&M staff. (This interaction is absolutely critical, and its lack is one of the big stumbling blocks with many UMCS implementations). Coordination is likely needed with the service order process in the O&M division as well.

- Master Planning Division to champion projects that make best use of the UMCS
- Environmental Division to coordinate efforts to meet energy goals
- Network Enterprise Center (NEC) to ensure all coordination necessary to achieve network connectivity

3. Manage and supervise UMCS staff. This staff consists of individuals performing the following roles: UMCS Administrator, Technical Expert, UMCS Operators, System Integrator, Controls Technicians, and Energy Manager. Staff may consist of or include Contractors and therefore the UMCS Manager shall manage contract staff in accordance with Federal Acquisition Regulation (FAR) requirements.
4. Serves as managing authority for the <GARRISON> UMCS. Performs liaison and coordination with the contracting officer, other DPW branches; Headquarters, Installation Management Command; the Department of Army (DA) Center for Public Works; and other Federal agencies. Provides technical advice to the Contracting Officer and Director on UMCS implementation and support matters. Represents <GARRISON> at meetings and conferences concerning UMCS technical matters. Keeps informed on UMCS technology to provide the Director and installation (advisory council) with advice. Stays abreast of and evaluates new developments in UMCS technology to ensure that program planning, approaches, findings, and decisions reflect the lasted thinking. Maintains close contact with research and development laboratories, manufacturers, scientists, other Corps divisions, and other Federal agencies. Anticipates the implications that probable technological change will have for Corps designs. Directs design changes as needed. Ensures compliance with established criteria, sound engineering principles, standard practices, and existing building codes. Detects omissions, discrepancies, inadequacies, and nonconformance with approved criteria. Assures project funding, project management, scheduling, and cost estimates for project features are appropriate and reasonable.
5. Recommends preparation of additional supportive technical documentation to substantiate project design, analysis, value engineering (V-E) studies, and calculations. Evaluates and responds to questions raised by districts as a result of technical engineering review comments. Ensures that designs satisfy the intended project purpose.
   Identifies, defines, and develops specifications, requirements, techniques, methodology, and criteria for UMCS. Supervises development of or devel-

ops architectural-engineering specifications for the UMCS. Performs technical inspections, supervision, or oversight, at his/her discretion, on all aspects of the UMCS design, constructions, and operation. Identifies problems such as improper use, type, or installation of systems; and other inefficient, improper, or ineffective arrangements. Prepares and staffs regulations, policy documents, memoranda of instructions, circulars, standard operating procedures, etc., pertaining to the UMCS. Organizes working groups and chairs meetings with Installation functional activities to maintain and improve UMCS implementation.

6. Develops projects for and justifies, both technically and economically, UMCS projects, and prepares project documentation for project approval and funding, and work orders or contract delivery orders for their accomplishment. Prepares estimates for alteration and modification project, analyzes work to be done, and assigns work in the most efficient manner and sequence. Performs cost-benefit analyses to determine if alteration costs will be recovered in energy conservation projects. Reviews, evaluates, and coordinates with other activities within the DPW on Military Construction Army (MCA), Research Development Test and Evaluation (RDTE), maintenance and repair, and family housing projects, ensuring state-of-the-art conservation techniques are incorporated into the designs, suggesting different energy-efficient methods, and keeping informed of new, innovative ideas.

Appendix H: SOW: UMCS Contractor—System Admin, Control Techs, System Integrator

STATEMENT OF WORK
FOR
UTILITY MONITORING AND CONTROL SYSTEM (UMCS)
System Administrator, Controls Technicians, System Integrator
at [Post Name]

[***Specifier/designer note:*** *This statement of work (SOW) can be used to obtain long-term support of a UMCS and/or building control systems. Several tasks are included, and the SOW must be edited to remove any tasks that are not desired. This sample statement of work (SOW) must be tailored to installation-specific requirements. Refer to the yellow-highlighted, square bracket [ ] items for tailoring options and locations that need to reflect local conditions and requirements.*

In general, this SOW can provide:

1. *A Controls Technician embedded in the maintenance shop to assist with building control systems (paragraph 2.2).*
2. *A UMCS System Administrator to develop and maintain procedures for UMCS operation and the integration of building systems into the UMCS. This System Administrator may also perform the day-to-day tasks required to maintain the UMCS. Note that in many cases, some of this work may be performed by the NEC, but it may not fall within their common level of service agreements and the DPW may choose to independently perform this work (paragraph 2.3).*
3. *Development of a detailed System Integration Methodology describing how to perform integration of building direct digital control (DDC) systems into the UMCS (paragraph 2.4). Note: this task does not include actual System Integration; instead, the goal is to produce a document that will help the installation better define a detailed integration process.*]

1. OBJECTIVE

The Contractor shall provide technical support to **[Post Name] [UMCS System Name]** Utility Monitoring and Control System (UMCS). The Contractor shall:

[Specifier/designer note: The bulleted list includes a selection of tasks that can be covered by this SOW. Include the bullets and corresponding paragraphs for items you want as part of this SOW and remove the others.**]**

- Develop and document a System Operation Methodology
- Provide Operations and Maintenance Department (OMD)-embedded maintenance support
- Develop a UMCS Operation Methodology (paragraph 2.3.1)
- Manage and operate the UMCS according to the Operation Methodology (paragraph 2.3.2)
- Develop and document a System Integration Methodology (paragraph 2.4)

2. REQUIREMENTS

[Post Name] currently has a **[UMCS System Vendor/Model** Utility Monitoring and Control System installed in accordance with the requirements of UFGS 25 10 10. Unless otherwise indicated, all requirements of this Statement of Work pertain to this UMCS. All work performed by the Contractor shall ensure that the system is an open UMCS in accordance with UFGS 25 10 10. In cases where UFGS 25 10 10 allows options, the Contractor shall coordinate these options with **[Post Name]**.

2.1 US Citizenship Requirements

Contractor must ensure that all Contractor Personnel who will work on **[Post Name]** or have access to information that describes the site Utility Monitoring and Control System (UMCS) must be United States citizens. Contractor will be responsible for ensuring that all Subcontractor personnel, at any tier, having access to information about the site UMCS are United States citizens. The Contractor is expected to secure all drawings or other descriptive information concerning the current site UMCS so that access is granted only to those who need the information to perform work under this contract.

2.2 Embedded Maintenance Support

[*Specifier/designer note:* *Indicate the name of the maintenance shop. The bracketed number of hours is for 1 year. Adjust as needed for more or less support.***]**

The Contractor shall provide a Controls Technician embedded in the **[Maintenance Shop]**. The embedded Technical Support Representative (TSR) shall maintain a physical presence in the shops according to a mutually agreed upon work schedule for a total of **[1,800 hours]** under this contract. The Contractor shall assign specific staff to perform the TSR services and shall not rotate staff in and out of the TSR role so that consistency of support staff is maintained. TSRs are not required nor expected to participate in maintenance support activities outside of or beyond the scope of this contract.

The TSR shall

2.2.1. Provide maintenance support services for both new and existing control systems equipment and hardware. Intimate familiarity with the **[UMCS Vendor System]** is required along with a working knowledge of other equipment and hardware, such as other vendor’s DDC and pneumatics. The support requirements apply to all control systems regardless of whether or not the system is connected to the UMCS.

2.2.2. Assist **[Maintenance Shop]** staff with control system problem identification, diagnosis, maintenance, repair, installation, and commissioning. This includes the generation of service orders according to **[Maintenance Shop]** procedures. TSR shall pay particular attention to systems and equipment that are under warranty, the intent being to identify problems prior to warranty expiration and have repairs performed under warranty by the installing Contractor.

2.2.3. Assist with in-house renovation projects, including the development of project requirements; specifications; drawings; scopes of work; cost estimates; bill of materials, installation, and inspection.

2.2.4. Provide scheduled and on-the-job UMCS and DDC training to **[Maintenance Shop]** staff. Scheduled training shall be classroom style at mutually agreed upon periodic intervals. The duration, scheduling, and content of scheduled training shall be mutually agreed upon by the TSR and **[Maintenance Shop]** maintenance staff.

2.2.5. Obtain and maintain a cell phone service and provide cell phone number to **[Maintenance Shop]** staff. TSR shall carry the phone at all times during the agreed upon work schedule and shall use this phone for communicating with **[Maintenance Shop]** staff.

2.2.6. Provide and be responsible for their own transportation vehicle, diagnostic equipment, and hand tools.

2.2.7. Provide monthly activity summary reports. Reports should be brief summaries of activities performed for the month. These reports shall be organized as follows:

a. List of DDC Systems supported (as described in paragraph 2.2.1.
b. Summary of **[Maintenance Shop]** staff assistance provided (as described in paragraph 2.2.1.
   i. problems identified for warranted systems
   ii. commissioning support provided
   iii. other support activities
c. Summary of assistance provides to in-house renovation projects (as described in paragraph 2.2.2.
d. Summary of training provided (as described in 2.2.3. including dates, times, attendance and content of scheduled and on-the-job training sessions

2.3 UMCS Administration, Operation, and Management

2.3.1. UMCS Operation Methodology

The Contractor shall develop and document a UMCS Operation Methodology. As part of this, the Contractor shall coordinate with DPW and **[Maintenance Shop]** staff in the identification and development of processes for operation of the UMCS and shall implement mutually agreed upon processes. The processes shall take into consideration the current and future anticipated needs and uses of the UMCS. These processes include, but are not limited to,

[*Specifier/designer note:* *Include a list of computers that must be able to access the UMCS.***]**

a. DPW and **[Maintenance Shop]** access. **[Installation X]** needs access to the system according to defined procedures and logistics, including, but not limited, to password levels and limits, and access to and training on tools. Coordinate with the installation Network Enterprise Center (NEC) to ensure that the following computers can access the UMCS: **[List of Computers]**.
b. DPW Tools. Describe a methodology for DPW personnel, including O&M shop personnel, to access and use the UMCS and related tools, such as laptops. Methodology must include DPW personnel responsibilities and obligations.
c. Service Calls. Define the process whereby the UMCS support staff responds to requests for information, and diagnostic actions to be taken by the UMCS operator in response to calls from maintenance staff who are troubleshooting DDC systems that are connected to the UMCS.

d. Alarms. Define the process whereby alarms received by the UMCS from DDC systems connected to the UMCS are selected, setup, monitored, routed, and managed. This includes the generation of work orders based on received alarms.
e. Energy Savings. Define the process for reducing energy consumption, tracking energy savings, data archiving, and trending towards meeting LEED goals and standards along with the creation and management of equipment usage and performance reports.
f. UMCS Training. Identify and define training needs and requirements for DPW staff. Note: The Contractor shall provide UMCS training as specified in UFGS 25 10 10.
g. Installation Design Guide (IDG). The Contractor shall provide verbiage for suggested changes to **[Installation X's]** IDG in support of an open basewide Niagara Framework UMCS and in support of its successful management, operation, and maintenance.

2.3.2. UMCS Operation and Management

The Contractor shall manage the UMCS in a manner consistent with the requirements and intent of UFGS 25 05 11, UFGS 25 10 10, UFGS 23 09 00, UFGS 23 09 23.01, UFGS 23 09 23.02, and the following requirements:

a. Systems Integration Log. The Contractor shall develop and maintain an up-to-date log consisting of
   i. Documentation drawings and submittals specified in UFGS 25 10 10 and UFGS 25 05 11 for the UMCS
   ii. Documentation drawings and submittals specified in UFGS 23 09 00, UFGS 23 09 23.01, UFGS 23 09 23.02, and UFGS 25 05 11 for DDC systems connected to the UMCS or those for which future connection is anticipated
   iii. Related documentation as specified in this SOW
   iv. System Administrator and Cybersecurity documents, records, and certification data
   v. Maintenance and repair records
   vi. Meeting minutes

   These items are further described below.

b. Documentation. The Contractor shall compile, manage, store, and maintain UMCS and related DDC system documentation. As part of this, the Contractor shall assist the DPW to identify, locate, and assemble existing UMCS and DDC materials that will facilitate the implementation of the UMCS as a basewide system such as: DDC System Drawings, Contractor Submittals, including software, licenses, and system databases, Points Schedules, technical references, etc.

[*Specifier/designer note:* *Edit the following two items to define which tasks are in this SOW and which are to be performed by NEC or other Contractors.***]**

c. System Administrator. The Contractor shall serve as a System Administrator for the UMCS and UMCS computers and shall obtain all necessary training and certifications and otherwise meet Information Assurance requirements—as described in Exhibit A for the Contractor staff and for the UMCS—as needed to perform System Administrator duties for the UMCS.

d. Maintenance and Repair. The Contractor shall maintain the UMCS as follows:

   i. Maintenance and repair of hardware

   ii. Maintain all UMCS-related software, including Monitoring and Control software, including up-to-date patches, fixes, upgrades.

   iii. Coordinate with **[POC]** to maintain software and hardware for vendor-specific engineering tools, including laptops and controller programing and configuration tools.

   iv. Perform database backups

   v. Maintain user accounts and permissions

   vi. Provide data to other computer systems or personnel as needed

[*Specifier/designer note:* Edit and include the following as applicable.**]**

   vii. **[Update UMCS with applicable data as needed from other computers systems, such as automatic meter reading, electrical distribution, Supervisory Control and Data Acquisition (SCADA), etc.]**

e. DDC Contractor Coordination. The Contractor shall work with DDC Contractors to clarify Open Control Systems and integration requirements and demonstrate the UMCS.

f. Meetings and Reviews. The Contractor shall attend the monthly **[Post Meeting]** UMCS workgroup meetings. The Contractor shall attend design and planning charrettes and shall review UMCS and DDC-related designs for Military Construction and other funded projects. The Contractor shall review DDC system submittals from third-party DDC System

Contractors to determine if the DDC system meets the requirements of the System Integration Methodology. The Contractor may provide recommendations to the Government but will not be permitted nor be responsible for accepting or rejecting other Contractors' work or submittals. The Contractor shall provide minutes for all meetings held with the Government.

2.4 System Integration Methodology

2.4.1. System Integration Methodology. The Contractor shall develop a System Integration Methodology in accordance with the Open Control Systems requirements in this SOW, UFGS 25 10 10, and the applicable integration-related requirements of UFGS 23 09 00, UFGS 23 09 23.01, and UFGS 23 09 23.02. The methodology shall describe the technical approach for accomplishing the integration of DDC systems installed in accordance with UFGS 23 09 00, including those installed by third-party Contractors. The description shall include all elements contained in this SOW, including, but not limited to

a. Government Coordination. Describe the coordination procedures, including those with, at a minimum, the following Government personnel:

- DPW, UMCS Manager: **[name, phone, e-mail. Roles and Responsibilities]**
- DPW, UMCS Administrator: **[name, phone, e-mail. Roles and Responsibilities]**
- DPW, Chief of O&M: **[name, phone, e-mail. Roles and Responsibilities]**
- DPW, Shop Foremen: **[name, phone, e-mail. Roles and Responsibilities]**
- NEC: **[names, phone, e-mail. Roles and Responsibilities]**
- District Office Engineer: **[names, phone, e-mail. Roles and Responsibilities]**
- Area Office Engineer: **[names, phone, e-mail. Roles and Responsibilities]**

b. UMCS Connectivity. Describe the procedure for connecting the DDC system to the UMCS IP network and obtaining the IP connection. Issues to be addressed include the following:
i. Who will coordinate with the NEC for FPOC location and IP addresses?
ii. How will the cybersecurity of the UMCS be maintained during and after the integration process?

c. Niagara Framework Database and Licensing. Describe the procedure for managing the UMCS database(s), including the approach for integration of UFGS 23 09 00 systems. Describe the procedures for maintaining current licenses for the UMCS plus connected buildings. For example, should Installation A purchase and manage all licensing, or should individual building Contractors provide licenses as necessary to **[Installation X]**?

d. UMCS Integration Checklist. Develop a checklist of activities and describe information to be provided by the UMCS Contractor to third-party UFGS 23 09 23 Contractors for them to perform successful integration with the UMCS, such as domain names and addressing. List and describe submittals and technical information needed from third-party Contractors in order to accomplish integration of third-party UFGS 23 09 23 systems.

e. DDC Integration Checklist. Develop a checklist of activities and describe information to be provided by the Building Control System Contractor to the UMCS System Integration Contractor that is needed to perform successful integration with the UMCS. This might consist of Niagara database handling and submission, software licenses, Niagara tool software updates and source code submittals, verifying Points Schedule drawing, verifying override points defined/available, Points Schedule drawing submittal, Riser Diagram drawing submittal, and listing potential or expected recommissioning requirements for field devices (for obtaining field data, not sending it).

f. M&C Software Configuration. Provide a step-by-step description for programming, configuring, and otherwise setting up hardware and software to accomplish Monitoring and Control software functionality specified in UFGS 25 10 10 so as to accomplish integration of third-party Niagara Framework systems (IAW UFGS 23 09 00). This shall include obtaining or developing a Points Schedule drawing for the system to be integrated.

g. Acceptance and Startup Procedures. Describe any inspections or testing to be performed to verify that the interface between the UMCS and the third-party building-level system can be accomplished.

3. DELIVERABLES

Specifier/designer note: *The bracketed due dates for the deliverables assumes this is a 1-year contract. Edit the due date for all deliverables to reflect actual requirements.*

Unless otherwise noted below, each of the below submittals shall be in editable electronic format on CD-ROM (no PDFs unless otherwise approved) and in hardcopy format.

3.1 Embedded Controls Technician Activity Summaries

[Monthly activity summary report for each month due on the 5th day of the following month except that the summary report for the last month of this contract is due on the last day of the performance period.]

3.2 UMCS Operation Methodology

Initial submittal **[3 months after award]**

Final submittal **[2 months prior to contract completion]**

3.3 System Integration Methodology

Initial submittal **[3 months after award]**

Final submittal **[2 months prior to contract completion]**

3.4 Meeting Minutes

Meeting minutes shall be delivered via email within 1 week after each meeting.

4. PERIOD OF PERFORMANCE

Specifier/designer note: *Specify the duration for the project. If you specified a number of hours for a Controls Technician, make sure the completion of the project allows enough time for those hours.*

Completion of this project will be **[_____]**.

5. DISTRIBUTION

Specifier/designer note: *Specify distribution for all deliverables.*

Distribution for all deliverables of this project will be **[____]**.

Exhibit A: Network Access Requirements

Specifier/designer note: *The UMCS System Administrator will need to work on a Government computer system to perform the requirements of this SOW. Coordinate with the installation NEC to identify any requirements that the Contractor must meet in order to access Government networks and computers and include them here. The below text is from a SOW generated by Fort Bragg and is included as an example only.*

Example Network Access Requirements for US Government Contracts

1. Information Assurance (IA). Contractor personnel requiring access to US Government Information Systems to fulfill their duties shall possess the required favorable security investigation, security clearance, formal access approval, and need-to-know prior to being granted access to any Government computer or computer network.
2. IT-I Level of Security Access is required for Contractor personnel in IA Position working with infrastructure devices, Intrusion Detection Systems (IDSs), routers, System Administration or Network Administration, with privileged-level access to control, manage, or configure Information Assurance tools or devices, individual information systems, networks, and enclaves. At a minimum, such Contractor personnel shall require a favorably completed NAC, initiation of SSBI, completion of SF85P, SF86, and Supplemental Questionnaire.
3. IT-II Level of Security Access is required for Contractor personnel in IA positions requiring the work with operating systems administration of common applications or enclaves, or back-up operators, with limited privileged level access to control, manage, or configure information systems or devices. At a minimum, such Contractor personnel shall require a favorable review of local personnel, base or military, medical and other security records as appropriate, initiation of a NACLC, and completion of the SF85P or SF86 and Supplemental Questionnaire.
4. IT-III Level of Security Access is required for Contractor personnel in positions as normal users, a power user on individual systems for configuration with nonprivileged level of access to information systems and devices. At a minimum, such Contractor personnel shall require a favorable review of local personnel, base or military, medical, and other security records as appropriate; initiation of a NAC; and completion of the SF85P and Supplemental Questionnaire.
5. Contractor personnel shall not be granted access to any Government computer systems or networks until proof of compliance to the Information Assurance (IA) clearance requirements.

6. Once Contract personnel have complied with the Information Assurance requirements as reflected above, they will be granted the appropriate Information Technology level of security access.
7. Contractor personnel shall personally pick-up and sign for Government network user identification and password at **[location]**
8. Contractor employee(s) shall be solely responsible for the safeguarding of user passwords and shall immediately report any suspected compromise or loss of password to **[office]**.

Appendix I: SOW: UMCS BCS Integration

STATEMENT OF WORK FOR UTILITY MONITORING AND CONTROL SYSTEM (UMCS) BCS INTEGRATION at [Post Name]

[*Specifier/designer note:* *This SOW can be used to obtain system integration services to integrate a BCS installed under UFGS 23 09 00 into a UMCS front-end server installed in accordance with (IAW) UFGS 25 10 10. For MILCON projects, this SOW can be used by having the district transfer project funds (with a Military Interdepartmental Purchasing Request (MIPR) to a contracting entity to award the integration services.***]**

Version: 2019-09-30

1. **SYNOPSIS** : The Contractor shall provide the materials and labor required to integrate direct digital control (DDC) systems into the **[Post Name]** basewide **[UMCS Manufacturer] [UMCS Model]** Utility Monitoring and Control System (UMCS).

2. **PRICE PROPOSAL** : The Contractor shall provide a firm fixed price proposal for the integration of the DDC systems specified below into the **[Post Name]** UMCS.

[*Specifier/designer note: System integration should be done in accordance with the (System Integration Methodology SIM) if the installation has one. Include the bracketed text if the installation has a SIM and remove it otherwise.***]**

3. **SPECIFIC WORK TO BE ACCOMPLISHED**: The Contractor shall provide materials and labor required to integrate Building Control System (BCS) DDC systems specified into the **[Post Name]** UMCS. All work shall be in accordance with **[the approved [Post Name] System Integration Methodology]**, Unified Facilities Guide Specification (UFGS) 25 10 10, and this SOW. All work performed by the Contractor shall ensure that the system is and remains an open UMCS in accordance with UFGS 25 10 10. In cases where UFGS 25 10 10 allows

options, the Contractor shall coordinate these options with **[Post Name]**.

3.1 The Contractor shall integrate the following building DDC systems:

Specifier/designer note: *Identify all systems to be integrated. If FPOC locations and IP addresses are going to be listed in this SOW (as opposed to on a drawing or requiring coordination—see next specifier note) you may want to put a table here showing this information as well. For example,*

System	**FPOC Location**	**IP Address**
Bldg. 52 West Wing	Bldg. 52, room 215	192.168.2.101
Bldg. 52 East Wing	Bldg. 52, room 215	192.168.2.105
Bldg. 62 AHU 1	Bldg. 62, room 410	192.168.2.108

3.1.1. **[list the DDC systems (including building) or buildings]**

3.2 For each DDC system, the Contractor shall perform all tasks required to fully integrate the system into the UMCS, including, but not limited to the following:

3.2.1. Connect the building IP network to Facility Point of Connection (FPOC) to connect the building DDC system to the UMCS IP backbone.

[*Specifier/designer note:* *Provide FPOC locations by one of the following:*

Include a drawing or other document with these locations with the SOW.
List the locations (building and room number) here.
Refer to the table (see previous specifier note) where they are listed.

Similarly, provide IP addresses for all BCS IP devices. Note that the IP addresses may not be known preaward in which case choose either to *provide them to the Contractor post-award or require that the Contractor obtain them from NEC. If requiring the Contractor to obtain them from NEC, provide a NEC point of contact.*

*Note that this SOW assumes that the FPOC location is the location of the IP drop provided by NEC.***]**

3.2.1.1 FPOC locations are **[shown in the Government furnished documents] [_____]**.

3.2.1.2 DDC hardware IP addresses [**are shown in the Government furnished documents**][**will be provided after contract award**][**shall be obtained from [Post Name] NEC. NEC POC is [_____]] [____]**.

3.2.2. Incorporate each DDC system component into the UMCS database:

[*Specifier/designer note: Include bracketed text referring to the system integration methodology if the installation has one, otherwise remove the bracketed text.*

Select appropriate licensing requirement depending on whether ***[Post Name]*** *provides and manages its own licenses or not.*

If ***[Post Name]*** *has graphics standards in the SIM or IDG, include the bracketed requirement.***]**

3.2.2.1 Add building devices to the UMCS database **[and in accordance with the System Integration Methodology]**.

3.2.2.2 **[Provide additional UMCS front-end licenses as required to complete the integration. License must be assigned to [Post Name] and meet requirements in UFGS 25 10 10.]** Coordinate all licensing with [**Post Name**].

3.2.3. Incorporate each DDC system into the UMCS Monitoring and Control software:

3.2.3.1 Create graphic display pages for each DDC system:

- To the greatest extent possible, graphics for similar systems shall be the same.
- Graphics shall provide monitoring and override points as shown on the Points Schedules.
- **[Graphics shall conform to the Installation Design Guide and System Integration Methodology.]**

3.2.3.2 Configure scheduling, alarming, and trending functionality for the building system as shown on the Points Schedules.

3.2.3.3 Configure supervisory control functions, such as demand limiting, load shedding, or optimum start/stop, if applicable.

3.2.4. Reconfigure any building DDC devices as necessary to restore building functionality that was compromised as part of the integration process.

3.3 Contractor shall demonstrate completed integration to the Government. This demonstration shall show all work performed and shall be sufficient to familiarize the Government with the interface to the integrated systems. **GOVERNMENT FURNISHED INFORMATION**

[*Specifier/designer note:* *Include all drawings and documentation required to document the building system for integration. The following list contains some suggested drawings, not all of which may be needed. For example, the ductwork layout drawing may not be needed by the Integrator if user displays do not include ductwork information.***]**

4.1 Control system drawings, notably including the Points Schedule drawing(s)

4.2 [Floor plan drawings]

4.3 [Ductwork layout drawings]

4.4 [Mechanical drawings]

4.5 [Electrical drawings]

4.6 [Other drawings as indicated by UFGS 25 10 10, [Post Name], or the System Integration Methodology]

[*Specifier/designer note:* *The Integrator may be required to update UMCS front-end licensing. This may require them to purchase additional* *licensing and require knowledge of the existing site licensing. Provide documentation of the existing site licensing so that the Integrator can determine the cost and effort involved in meeting this requirement.***]**

4.7 [UMCS front-end licensing information, including licensed components, revision, and license status]

5. DELIVERABLES:

5.1 Summary listing of all M&C software edits, changes, and updates accomplished as part of system integration. Format shall be hardcopy and MS-Word or PDF on CD-ROM.

5.2 Product data, including product data sheets and computer software supplied under this contract as specified in UFGS 25 10 10. Format shall be hardcopy and MS-Word or PDF on CD-ROM of all data sheets, plus computer software on CD-ROM.

5.3 Licensing information for all software provided or modified as under this contract as specified in UFGS 25 10 10. Format shall be hardcopy and electronic file on CD-ROM.

5.4 Final As-Built Drawings as specified in UFGS 25 10 10. Format shall be 11 × 17 inch hardcopy and MS-Excel on CD-ROM.

[Specifier/designer note: *Provide the notification time, which must be given for the demonstration of the integration, and who must be notified.****]***

6. SCHEDULE

The performance period shall be from **[expected date of DDC system completion or acceptance]** until **[two months from start or period of performance]**. Notice of demonstration of completed integration shall be given to **[point of contact]** no less than **[one week]** before demonstration. Schedule impacts, for any cause, will be brought to the attention of **[the Contracting Officer Representative (COR)]** and the Contracting Officer immediately. The Contractor shall provide a proposed resolution and basis for delay.

Appendix J: Microgrid And Other UCS

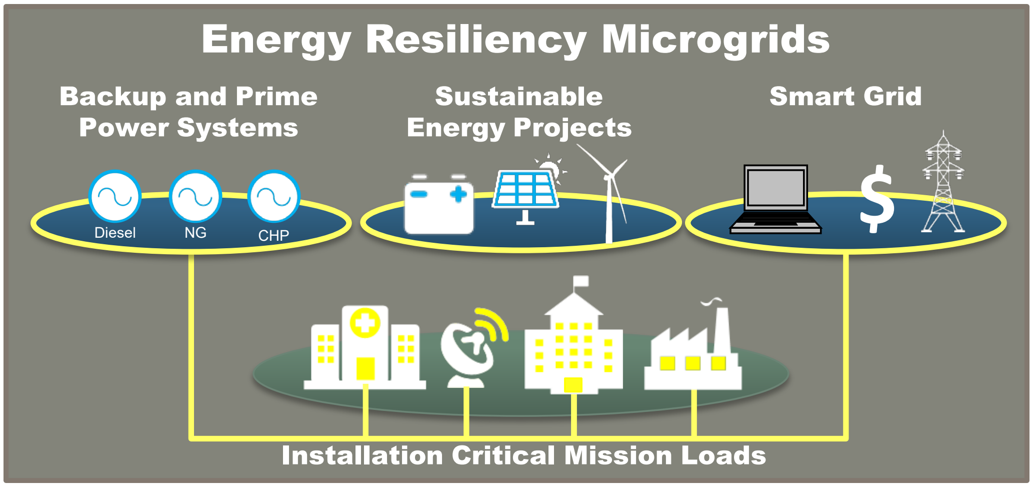
J.1 UMCS integration with microgrid control systems vision

As the Army pursues improved energy resiliency and expands smart infrastructure at installations, installations will experience increasing interconnection between control systems. Integration between microgrid control systems and UMCSs offers new capabilities and efficiencies that will improve how the installation uses electrical energy.

J.2 Microgrids—functions and operation

DoD installations with a high need for electric power resiliency may implement microgrids to serve critical electric loads with highly reliable power. Microgrids enable the installation distribution system to disconnect, or "island," from the commercial power grid when utility service is not available or unreliable. When islanded, the microgrid serves connected loads from multiple local power sources, such as a central utility plant, backup power generators, renewable power sources, and energy storage systems. Figure J-1 illustrates this concept, where multiple generation sources support installation critical loads.

Figure J-1. Microgrid concept.


Energy Resiliency Microgrids
Backup and Prime Power Systems
Sustainable Energy Projects
Smart Grid
Diesel
NG
CHP
Installation Critical Mission Loads

Microgrids may also operate in a grid-connected mode to manage renewable energy production and energy storage units, but their primary purpose is to provide the installation with electricity during an extended power outage. During islanded operation, the microgrid must balance power production from generation resources with demand from connected loads such that power supplied equals power demand. In a microgrid with sufficient generation capacity, the control system will optimize and select generation resources to supply the loads to maximize fuel efficiency, reliability, emissions, or other criteria. However, if a microgrid does not have enough generation sources to meet load demand, it must selectively shed (turn off) noncritical loads.

Most existing microgrids rely primarily on building- or feeder-level load shedding and careful generation management to achieve system balancing. When the microgrid enters islanded mode, the microgrid control system opens predefined switches throughout the distribution system to take noncritical loads offline. The control system then turns on generation resources and restores electric service to critical loads in a predefined sequence or set priority. As the loads fluctuate, the microgrid control system maintains some additional capacity, or spinning reserve, on connected generation to accommodate increases in load. As load increases, the microgrid starts additional generation to serve loads and maintain spinning reserves at a defined set point. In some microgrids, additional load shedding during operation may occur but usually at the whole-building or whole-feeder level.

J.3 Integration between microgrids and UMCS

Integration between a microgrid control system and a UMCS offers an opportunity to improve the performance of the microgrid system and the UMCS during islanded operation. Interaction between these two systems will allow the installation to shed noncritical loads with higher granularity and without expensive modifications to the electrical distribution system. Integration will also enable higher fuel efficiency in the microgrid by reducing spinning reserve requirements during islanded operation.

With tight integration between the microgrid control system and the UMCS, the concept of operation would be substantially different. When entering islanded operation, the microgrid control system would still operate distribution system switches to do some building- and feeder-level load shedding and then bring on generation and loads in a defined sequence to start the microgrid. However, the microgrid control system could further reduce startup load using the UMCS to curtail building loads such as

HVAC systems, lighting, plug loads, and others. Lower startup loads are easier to manage and support from a system stability standpoint.

During microgrid operation, the two systems would exchange commands and requests. If system generation sources are constrained, the microgrid system could command the UMCS to curtail building loads, allowing the UMCS to activate preprogrammed curtailment strategies, such as raising HVAC temperature set points, reducing lighting levels, or limiting plug loads. This interaction reduces the need for building- or feeder-level load shedding and instead offers a fine-grained load shedding approach that operators can fine tune based on building operations and priorities.

Conversely, the UMCS can make requests to the microgrid control system. When a large load needs to start, the UMCS would notify the microgrid system of the size and location of the large load. This would allow the microgrid system to make adjustments to system operation before the load comes online. Adjustments may include turning on additional generation sources or reconfiguring distribution connections to meet the large load's requirements. Once the adjustments are made, the microgrid control system would then alert the UMCS that it has permission to start the requested large load. This interaction would improve system stability by allowing the microgrid to prepare for large increases in load and improve fuel efficiency by allowing the microgrid to operate with reduced spinning reserves.

J.4 Integration challenges

Integration between microgrid control systems and a UMCS is not without challenges. Connections between these two systems will result in more complicated cybersecurity approaches and will require careful management and monitoring of the interface between them. While policies and approaches to control system cybersecurity, information assurance, and RMF accreditation are still evolving, this will remain a substantial challenge to developing an interface between microgrid control systems and UMCS.

At many installations, the electrical distribution system is owned and operated by a Utilities Privatization Contractor (UP). The UP is responsible for all operation and maintenance of the distribution system, including any information networks that support the system. Consequently, many microgrid projects overlaid on privatized distribution systems use the Contractor-owned-and-operated information network to transport controls communication. This may pose a problem for integration between microgrids and UMCSs that operate on Government networks. Interfaces between these networks will require thorough consideration in information assurance policy, as no specific guidance for Contractor networks for control systems currently exists.

Appendix K: UMCS Master Plan Example

Note: this is an actual master plan that has been redacted to obscure location and vendor information. Some language was edited for clarification.

EXECUTIVE SUMMARY

Part 1. SAMPLE INSTALLATION NAME

1.01 BACKGROUND

A. Installation [*A*] contracted Contractor *B* to support an upgrade/modernization program for the Utility Monitoring and Control System (UMCS) at INSTALLATION A. INSTALLATION A had identified 300 buildings that they wanted to be considered as part of a basewide master plan. Their stated vision for the UMCS is integration of all applicable buildings into a basewide UMCS based on Version 4 of the Niagara Framework.

B. The new UMCS must provide a single login per user to the entire integrated group of buildings; provide a common graphical user interface, including scheduling, alarming, and trending to the integrated systems; function on a UMCS-specific VLAN within the INSTALLATION A installation campus area network (ICAN,) and meet DoD Risk Management Framework (RMF) cybersecurity requirements.

1.02 SUMMARY OF SCOPING ACTIVITIES

A. CONTRACTOR B performed a site scoping survey of over 300 buildings, identified buildings or locations that qualify for the UMCS Integration Plan (and some that do not), and prioritized their integration in groups as Low, Medium, and High. Of the qualifying locations, 15% were prioritized Low, 18% prioritized Medium, and 67% prioritized High.

B. CONTRACTOR B investigated Niagara V4 technical requirements in order to determine potential upgrade paths for INSTALLATION A Niagara builds.

C. CONTRACTOR B investigated networking and staffing options for a basewide UMCS.

1.03 RECOMMENDATIONS

A. Buildings where integration is justified should be integrated into a new unified Niagara Version 4 basewide UMCS. Prior to integrating individual buildings or locations, a new server system and support software will need to be installed. As the conversion process proceeds, each location will be backed up and removed from the existing system, converted to the new system, commissioned, then brought online under the new server.

B. Locations should be integrated in groups moving from High to Low priority. As part of the plan development and coordination with INSTALLATION A, these groups may be adjusted. The integration at each location will vary based on the existing control system. Most locations will require the installation of a new NIAGARA FRAMEWORK SUPERVISORY GATEWAY to communicate with the building's existing controllers and the new front end. Integration for some locations will be more difficult than others, and there will be a period of no communications with the building during the transition.

SAMPLE MASTER PLAN CONTENTS

PART 2. ACRONYMS AND ABBREVIATIONS

AF	Air Force
AO	Authorizing Official
AR	Army Reserve
ATO	Authority To Operate
AX	NFSG model ‘AX’; previous generation technology
BACnet	Building Automation and Control Networking Protocol (ASHRAE 135)
BAS	Building Automation System
CNSSI	Committee on National Security Systems Instruction
CONUS	Continental United States
CPU	Central Processing Unit
CRAC	Computer Room Air Conditioner
DDC	Direct Digital Control
DoD	Department Of Defense
DPW	Directorate of Public Works
FPOC	Facility Point of Connection
HVAC	Heating, Ventilation, and Air Conditioning
ICAN	Installation Campus Area Network
IT	Information Technology
LonWorks	Local Operating Network (ANSI 709.1)
MACOM	Major Army Command
MSF	Million Square Feet
N4	NFSG model 'N4'; current generation technology (Niagara version 4)
NAF	Nonappropriated Funds
NEC	Network Enterprise Center
NFSG	Niagara Framework Supervisory Gateway (nonproprietary term for a NIAGARA FRAMEWORK SUPERVISORY GATEWAY)
O&M	Operations and Maintenance
OEM	Original Equipment Manufacturer
PM	Project Manager
R2	NFSG model 'R2'; obsolete technology
RMF	Risk Management Framework
SCADA	Supervisory Control and Data Acquisition
SMA	Software Maintenance Agreement
SO	System Owner
TLS	Transport Layer Security
UFC	Unified Facilities Criteria
UFGS	Unified Facilities Guide Specifications
UMCS	Utility Monitoring and Control System
VLAN	Virtual Local Area Network
Wi-Fi	trademarked term meaning IEEE 802.11x wireless communication standard

PART 3. BACKGROUND

INSTALLATION A

3.01 BACKGROUND

A. Installation A is a base in State C, which has a wide variety of building control systems ranging from simple pneumatic, electric, first generation DDC (all obsolete) to a number of modern DDC systems. Overall, their most prevalent systems (excluding pneumatics) are those based on the Niagara Framework, with approximately 260 based on the AX version, and another 90 or so based on the obsolete R2 version.

B. INSTALLATION A contracted Contractor B to support a conversion and integration program for Utility Monitoring and Control System (UMCS) at INSTALLATION A. INSTALLATION A identified *300* buildings to be considered as part of a basewide master plan. Their stated vision for the UMCS is to integrate applicable buildings into a basewide UMCS based on Version 4 of the Niagara Framework.

C. The new UMCS must provide a single login per user to the entire integrated group of buildings; provide a common graphical user interface including scheduling, alarming, and trending to the integrated systems; function on a UMCS-specific VLAN within the INSTALLATION A ICAN; and meet DOD RMF cybersecurity requirements.

3.02 KEY CONCEPTS

A. The UMCS Integration Plan includes an outline of steps to convert (or repair) and integrate building controls systems, including several existing UMCSs into a new UMCS, meeting INSTALLATION A's operational and security requirements. The initial base scoping survey has been completed and has been incorporated into the UMCS Integration Plan. Several recommendations are presented as part of the Plan development for consideration by the INSTALLATION A UMCS Plan team.

B. INSTALLATION A staff provided a list of key desires for incorporation and development within the UMCS Plan:

1. Maximize the reuse of existing Tridium systems; replace proprietary and obsolete systems.
2. Provide single log-on capability with role-based access control for all authorized users. Include the following features:
   a) One screen access to each building UMCS with ability to manage all UMCS alarms
   b) An audit log that will store activity for each user

c) Access to as-built control drawings and sequences for each building UMCS

d) Log-on from any authorized workstation with no change in user capabilities

3. Provide remote management of all Niagara Framework Supervisory Gateways.

3.03 PLAN PRIORITIES AND GROUPS

A. CONTRACTOR B performed a site scoping survey of 300 buildings, identified buildings or locations that qualify for the UMCS Integration Plan, and prioritized them in groups as Low, Medium, and High. Of the qualifying locations, 15% are prioritized Low, 18% prioritized Medium, and 67% prioritized High.

3.04 REPAIR AND CONVERSION PROCESS STEPS

A. Prior to integrating individual buildings or locations, a new server system and support software will need to be installed. As the conversion process proceeds, each location will be backed up and removed from the existing system, converted to the new system, commissioned, then brought online under the new server.

B. The integration at each location will vary based on the existing control system. Most locations will require the installation of a new NIAGARA FRAMEWORK SUPERVISORY GATEWAY to communicate with the building's existing control modules and the new server system. Integration at some locations will be more difficult, and there will be a period of no communications with the building during the transition.

PART 4. INTEGRATION OBJECTIVES

4.01 NEW UMCS FRONT END SELECTION

A. Background: The current UMCSs are spread across multiple platforms and workstations. There is no common means of connection to every control system, with some capable of remote IP connections and others requiring a local workstation. There is no common log-on or security protocol for these systems. There is currently no single workstation capable of viewing all the active control systems remotely or locally.

B. Primary objectives for the new UMCS front end include the following:

1. Integrate all building DDCs under a single system.
2. Provide a single unique log-on for each user that manages user access and logs activity.
3. Provide a common graphical user interface for all building DDCs to manage all alarm events and trend logs.
4. Connect all building DDCs onto a dedicated INSTALLATION A UMCS VLAN.

C. The Tridium Niagara Framework system represents over 60% of the control system installations at INSTALLATION A qualified for integration with the planned UMCS. Tridium's current product line, Niagara 4 (N4), can integrate most of the existing systems under a single log-on from one screen. The current revision of the N4 system (v4.6) also provides additional security options, user management, and a common graphic interface with management of all alarms and trend logs that meets INSTALLATION A requirements through a single interface. The Tridium N4 platform will be used as the central integrating system for the INSTALLATION A UMCS.

4.02 BUILDING DDC PLAN

A. Background: The INSTALLATION A site scoping survey identified thirteen unique control vendors within the UMCS plan scope. The technology, connectivity, and applicability to the UMCS Integration Plan goals varies broadly across these systems. Some systems are obsolete with limited to no support and others have current generation hardware with web-based interfaces but operate standalone without centralized security. Maintaining thirteen widely different control systems creates an unnecessary resource strain on DPW, particularly for those systems with no remote access (over 50%).

B. Primary objectives for building DDC systems are as follows:

1. Provide an IP Facility Point of Connection (FPOC) for all building DDC systems
2. Reduce the number of unique control system installations as efficiently as possible

3. Replace obsolete systems with current N4 compliant controls
4. Integrate AX installations to N4 for centralized control and security
5. Provide guidance for the implementation of UFGSs to standardize building DDC configurations and communication protocols

C. Buildings without an FPOC (typically a NEC-supported IP drop) for DDC typically have two options:

1. Integrate the remote DDC into a nearby building that does have an FPOC
2. Install a new FPOC at the remote building through coordination of the Building Automation System (BAS) Contractor and NEC.

Integrating with a nearby building will require establishing a DDC field-level network cable between the two building NIAGARA FRAMEWORK SUPERVISORY GATEWAYs. If there is no existing cable between the buildings that can be reassigned for this purpose, a new cable would have to be pulled. This is not the most desired solution, unless the remote building has a small footprint with a minor controls installation. If a new cable would have to be pulled, there is more value in pulling an IP connection to the remote building rather than a special use cable and establishing an FPOC for the remote building. Any work involving extension of the base IP will require close coordination with the NEC.

D. INSTALLATION A buildings within the scope of this plan have been placed into high, medium, and low priority groups. Details of the grouping process can be found in the INSTALLATION A UMCS Survey Report—Appendix E. While most of the systems within these groups are already based on Tridium, there are obsolete Tridium variants (R2) within the group, and even modern variants (AX) with hardware that does not have the capacity to convert to the current version (N4). As of this writing, there are no Tridium N4 installations at INSTALLATION A.

As part of this plan, all qualified building DDC systems will be converted to an N4 capable system. This will result in the replacement of at least six of the thirteen systems currently installed, reducing overall DPW resource requirements.

E. All existing DDCs based on AX with N4 compatible NIAGARA FRAMEWORK SUPERVISORY GATEWAY hardware will be scheduled for a software conversion to N4. All obsolete or noncompliant systems will be scheduled for repair and replacement (see Part 4—“Vendor-Specific Niagara Framework Supervisory Gateway Upgrades”). Some vendors are in the early phase of developing N4 solutions with connections to their existing legacy DDC (obsolete). As of this plan, none of these early developments are viable for the UMCS integration Plan.

F. For all systems that require replacement under this plan, a set of UFGSs will need to be applied to ensure the new system is in line with the UMCS's goals. Recommendations regarding LON or BACnet protocols are provided below in Part 6.06—"Integration Path." These specifications shall become the master guideline for all future DDC installations at INSTALLATION A.

4.03 ADDITIONAL FUTURE OBJECTIVES

A. Background: The initial requested scope of this plan primarily addressed significant issues with UMCS communications, security, and accessibility. There will be additional benefits with the implementation of this plan that should be considered for application going forward.

B. Additional future objectives for the UMCS are as follows:

1. Standardization of common system sequences for post-upgrade systems
2. Standardization of point configurations for common systems
3. Future connection to existing energy metering systems for energy demand reduction sequencing of HVAC systems

C. This plan recommends laying the groundwork for development of standard sequences of operation across the INSTALLATION A UMCS. These standard sequences would apply to all future DDC installations. They would include standard direction for air handling unit economizer operation, modes of occupied and unoccupied operation, demand-controlled ventilation, and other items where standardization would assist with energy management and maintenance of the systems.

D. Requirements from UFC 3-410-02, Appendix E "Point Naming Convention" should be stringently enforced. This will prevent communications conflicts and aid in point identification when configuring schedules and trends. This should be in place as systems are merged under the common UMCS. A master point naming convention will require engineering to uniquely identify each DDC object across the entire INSTALLATION A UMCS, not just within each building.

E. Another post-installation potential future objective for consideration is to interface the UMCS with the energy metering system to collect utility data for use by the UMCS. This data could be applied to on-demand sequence adjustment of HVAC equipment to add another level of energy management. This is a long-term goal that would require completion and stabilization of the UMCS integration prior to implementation.

PART 5. UMCS CENTRAL SERVER

5.01 EXISTING WORKSTATIONS OR SERVERS

A. The UMCS integration process will be measured in months and years, which will require the existing systems to remain in place and operable during the conversion. To that end, additional space will need to be allocated for the new server and workstation until replacement work begins. As buildings are upgraded and the existing systems are decommissioned, the existing workstations and servers dedicated to those will be decommissioned and removed from the operator's space.

B. Prior to the Contractor beginning any conversion work, INSTALLATION A should backup all existing workstations and NIAGARA FRAMEWORK SUPERVISORY GATEWAYs. The Contractor will not be allowed to directly modify existing workstations or NIAGARA FRAMEWORK SUPERVISORY GATEWAYs during the repair and conversion. They must run their own backup, and the backup files will be used to perform the station conversion. Any graphics or software located solely in an existing NIAGARA FRAMEWORK SUPERVISORY GATEWAY must be backed up and integrated into the new station or server and tested prior to converting. Graphics will primarily reside at the new server[30] and also at the NIAGARA FRAMEWORK SUPERVISORY GATEWAY, which will require a model with sufficient capacity for N4 compliance and graphic storage.

5.02 NEW WORKSTATION OR SERVER

A. The new server software will be the latest version of Niagara 4.x (N4). Current Niagara requirements for the server are as follows:

1. Processor: Intel Xeon CPU E5-2640 x64 (or better)
2. Operating System: Windows 10, 64-bit Windows 8.1 Enterprise, 2012 R2 Standard
3. Memory: 8 GB minimum

Acquisition of the server hardware should be coordinated with NEC.

B. UFGS 25 10 10, *Utility Monitoring and Control System (UMCS) Front End and Integration* contains requirements for the Niagara software; these can be selected through use of the "Niagara Framework" tailoring tag in *SpecsIntact*. While a default N4 installation will meet most of these requirements, UFGS 25 10 10 should be used to ensure that all of the necessary Government requirements are met. In particular, UFGS 25 10 10 has very specific licensing re-

[30] Cybersecurity requirements discourage placing both user interface (web pages) and control functionality in the same device; the default approach should be to have graphics at the front-end server, not in the NIAGARA FRAMEWORK SUPERVISORY GATEWAY.

quirements, including the Niagara Compatibility Statement to allow interoperability with Niagara Framework components from multiple vendors.

C. Research with Tridium indicates a single, properly configured server can handle connectivity to all INSTALLATION A buildings included in the UMCS plan. Appropriate Device and Point packs will need to be purchased by the UMCS Contractor (see Part 6.08 Tridium N4 Software Environment and Licensing) to accommodate the total number of required connections. These can be purchased and added as needed for each building integrated with the N4 server.

D. The new UMCS server will communicate with sites through the existing basewide, NEC-provided VLAN. Connectivity and configuration of the new server will be coordinated with NEC. Initially, workstations will also be on the UMCS VLAN, but it is desirable in the future to allow workstations to access the server from elsewhere on the INSTALLATION A ICAN, possibly to include NEC-provided Wi-Fi.

E. CONTRACTOR B recommends locating the server in a NEC server farm and that NEC provide basic support for the server, including backups and software updates (not including UMCS application-specific software). Software updates will need to be coordinated with DPW to ensure that updates (such as Windows patches) do not disrupt key UMCS server functionality. The DPW will need to coordinate with NEC to provide support to the Niagara software on the server. Some software, such as underlying database or web server software may be supported by either DPW or NEC; this will depend on the specific software support provided by the UMCS-server Contractor.

5.03 CYBERSECURITY FOR THE SERVER

A. Contractor cybersecurity requirements for the front-end server (as well as the building control systems) are covered in UFGS 25 05 11, *Cybersecurity for Facility-Related Control Systems*. In addition to requiring submittals documenting the configuration of the server, this UFGS covers server requirements related to the following:

1. Access Control for user accounts and login procedures
2. Identification and Authentication of users
3. Auditing of events, both in the control system and at the server
4. Other cybersecurity requirements

B. Most (but not necessarily all) of the above requirements will be met by configuring the N4 server as described in the Tridium *Niagara 4 Hardening Guide*. This includes the following:

1. Passwords
   a) Use the password strength feature.

b) Enable the account lockout feature.
c) Expire passwords.
d) Use the password history.
e) Use the password reset feature.
f) Keep the "Remember These Credentials" box unchecked.

2. System Passphrase
a) Change the default system passphrase.
b) Use Transport Layer Security (TLS) to set the system passphrase.
c) Choose a strong system passphrase.
d) Protect the system passphrase.

3. Platform Account Management
a) Use a different account for each platform user.
b) Protect all platform credentials.

4. Station Account Management
a) Use a different account for each station user.
b) Disable commonly known default accounts when possible.
c) Set temporary accounts to expire automatically.
d) Disallow concurrent user sessions.

5. Role and Permission Management
a) Configure roles with minimum required permissions.
b) Assign minimum required roles to users.
c) Use the minimum possible number of super users.
d) Require super user permissions for program objects.

6. Authentication
a) Use an authentication scheme appropriate for the account type.
b) Remove unnecessary authentication schemes as entry points.

7. TLS and Certificate Management
a) Enable TLS for all connections where feasible.

PART 6. CONTROL SYSTEM CONVERSION AND INTEGRATION

6.01 OVERVIEW

A. Building systems fall into the following categories:

1. **Niagara systems with an AX version NIAGARA FRAMEWORK SUPERVISORY GATEWAY that can be directly converted to N4**. These buildings will only require a software conversion in the NIAGARA FRAMEWORK SUPERVISORY GATEWAY followed by integration to the UMCS server. Note that some systems may appear to be directly convertible, but resource limits will force a NIAGARA FRAMEWORK SUPERVISORY GATEWAY replacement (i.e., graphics

installed in NIAGARA FRAMEWORK SUPERVISORY GATEWAY, high trend storage, and alarm buffering). The UMCS Plan (Concept Phase) originally included all NIAGARA FRAMEWORK SUPERVISORY GATEWAY host models that supported conversion to N4. With the Intermediate Plan, the NIAGARA FRAMEWORK SUPERVISORY GATEWAY-3e, NIAGARA FRAMEWORK SUPERVISORY GATEWAY-6, and NIAGARA FRAMEWORK SUPERVISORY GATEWAY-6e models have been dropped since information from the manufacturer states these models do not support all N4 capabilities after conversion and may lack the resource requirements to perform the conversion. Unfortunately, the resource capability cannot be determined without attempting the conversion. INSTALLATION A also explained these NIAGARA FRAMEWORK SUPERVISORY GATEWAY models have been problematic for them operating in the AX environment. This phase of the UMCS Plan will only consider NIAGARA FRAMEWORK SUPERVISORY GATEWAY-7 and higher installed models and recently installed current revision models as qualified for the conversion to N4.

2. **Niagara systems with an AX version NIAGARA FRAMEWORK SUPERVISORY GATEWAY that cannot be directly converted to N4**. These systems are technically obsolete and will require an AX software conversion with capacity limits or hardware replacement of the failed NIAGARA FRAMEWORK SUPERVISORY GATEWAY followed by a DDC hardware change to N4. Again, some systems may have resource limits and require a new NIAGARA FRAMEWORK SUPERVISORY GATEWAY. After the conversion, these systems will be integrated to the UMCS server. The following NIAGARA FRAMEWORK SUPERVISORY GATEWAY models are marked obsolete as part of the UMCS Plan and will be replaced with NIAGARA FRAMEWORK SUPERVISORY GATEWAY-8000 models: NIAGARA FRAMEWORK SUPERVISORY GATEWAY-NXS, -NXT, -545, -403, -2, -2e, -3e, -6, -602, -603, -645, and NIAGARA FRAMEWORK SUPERVISORY GATEWAY-6e.

3. **Niagara systems with the R2 version of Niagara**. These buildings are technically obsolete and will require a new NIAGARA FRAMEWORK SUPERVISORY GATEWAY and considerable effort to reintegrate the building into the new NIAGARA FRAMEWORK SUPERVISORY GATEWAY. These buildings should not require replacement of the building controls other than the NIAGARA FRAMEWORK SUPERVISORY GATEWAY and associated expansion modules. Once an N4 Niagara Framework Supervisory Gateway is installed, it can be integrated to the UMCS server. Note that this process will be easier

if data on the existing building control system can be extracted from the R2 Niagara Framework Supervisory Gateway before the conversion begins, and therefore, consideration should be given to making familiarity with the R2 version of Niagara a required Contractor qualification for those buildings.

4. A few existing systems (see Vendor-Specific Niagara Framework Supervisory Gateway Integrations below) can be integrated without replacement of the underlying building controls via installation of an N4-compatible Niagara gateway. Once the building is N4 compatible, it can be integrated into the UMCS server.
5. Several remaining buildings have control systems that are technically obsolete and incompatible with N4 Niagara and will require a complete controls repair or replacement project with the installation of new Niagara compatible building controls. Once they have been installed, along with an N4 Niagara Framework Supervisory Gateway, the building can be integrated into the N4 UMCS server.

B. Capital improvement plans for all buildings should be reviewed as this plan progresses. Buildings scheduled for major renovation should be noted in the plan and tracked. The Project Managers for that work should be contacted and made aware of this plan and the UMCS scope to incorporate those initiatives as soon as possible.

6.02 EXISTING CONTROL SYSTEMS

A. Within the building plan scope, Tridium-based control systems account for ~64% of the installed DDCs at INSTALLATION A. SYSTEM Ds are second with ~16% of the DDC installations. The third largest installations are buildings with pneumatic or nonDDC controls at ~8%. The remaining eleven systems comprise ~12% of the DDC installations combined.

B. Out of those eleven systems, six are marked for complete replacement of the existing DDC. These systems are technically obsolete and do not meet INSTALLATION A's current requirements for an acceptable DDC, are no longer supported by the manufacturer, or have no means for integration into the Tridium network while retaining the required capabilities of this upgrade project.

C. Existing control systems with a path to Tridium N4 integration will be retained. Their existing gateway or Niagara Framework Supervisory Gateway will be converted or replaced as necessary to achieve the required level of integration.

Existing System Distribution and Integration Path

Existing DDC System	Base %	Path Forward
SYSTEM A	0.19	Obsolete; replace all existing DDC with N4 system.
SYSTEM B	0.19	Obsolete; replace all existing DDC with N4 system.
SYSTEM C	0.19	Obsolete; replace all existing DDC with N4 system.
SYSTEM D	15.61	Replace obsolete DDC with N4 system. Repair AX 3.8 or greater installation with N4 conversion.
SYSTEM E	0.74	Obsolete; replace all existing DDC with N4 system.
SYSTEM F	0.19	Obsolete; replace all existing DDC with N4 system.
SYSTEM G	0.19	Obsolete; replace all existing DDC with N4 system.
SYSTEM H	1.49	Install EC-BOS-8 series Niagara Framework Supervisory Gateway and integrate system.
SYSTEM I	6.32	Install WEB-8000 series Niagara Framework Supervisory Gateway and integrate system.
SYSTEM J	0.19	Retain VRF controls; add hardware for N4 integration.
SYSTEM K	1.49	Obsolete; replace all existing DDC with N4 system.
SYSTEM L	1.30	Replace or Repair hardware to N4 and integrate.
SYSTEM M	48.14	Replace or Convert hardware and integrate with N4.
SYSTEM N	15.80	Obsolete; replace hardware and integrate with N4.
Non-DDC	7.99	Obsolete; Install new N4 DDC system (Niagara Framework Supervisory Gateway and building level controls) and integrate.

6.03 HIGH-PRIORITY CONTROL SYSTEMS

A. The High-Priority existing control systems include SYSTEM M (68.89%), SYSTEM N (15.56%), SYSTEM D (6.94%), SYSTEM I (2.78%), SYSTEM H (1.11%), SYSTEM L (0.56%), SYSTEM E (0.28%), and SYSTEM K (0.28%). This group also includes some buildings with pneumatic or other non-DDC systems (3.33%) that will be entirely replaced with a new Niagara Framework Supervisory Gateway and DDC system or an extended DDC from an adjacent building control system.

B. There is an existing network connection in 94% of the High-Priority buildings; 6% of the buildings will need an FPOC installed or network connectivity extended from an adjacent building. The Contractor will be responsible for coordinating installation with the NEC for a new FPOC or extension of an existing network connection.

C. These control system integrations will primarily consist of software conversions of the SYSTEM Database and Niagara Framework Supervisory Gateway hardware. Hardware replacement is expected to be lowest in the high priority group.

6.04 MEDIUM-PRIORITY CONTROL SYSTEMS

A. The Medium-Priority existing control systems include SYSTEM D (34.69%), SYSTEM N (28.57%), SYSTEM M (11.22%), SYSTEM I (7.14%), SYSTEM K (4.08%), SYSTEM H (3.06%), SYSTEM L (2.04%), SYSTEM A (1.02%), SYSTEM C (1.02%), and SYSTEM E (1.02%). This group also includes some buildings with pneumatic or other non-DDC systems (5.10%) that will be entirely replaced with a new Niagara Framework Supervisory Gateway and DDC system or an extended DDC from an adjacent building control system.

B. There is an existing network connection in 76% of the Medium-Priority buildings; 24% of the buildings will need an FPOC installed or network connectivity extended from an adjacent building. The Contractor will be responsible for coordinating installation with the NEC for a new FPOC or extension of an existing network connection.

C. The Medium-Priority group includes several systems that will be partially software convertible; this will require some of the Niagara Framework Supervisory Gateway hardware to be replaced to reach N4 status. There are also legacy systems in this group where the N4 upgrade path is pending a vendor solution. As of the final plan, the vendor solutions have not left the beta stage and are not appropriate for consideration in the UMCS plan. Vendors without a proven path to integrate legacy DDC to N4 will have to replace obsolete systems.

6.05 LOW-PRIORITY CONTROL SYSTEMS

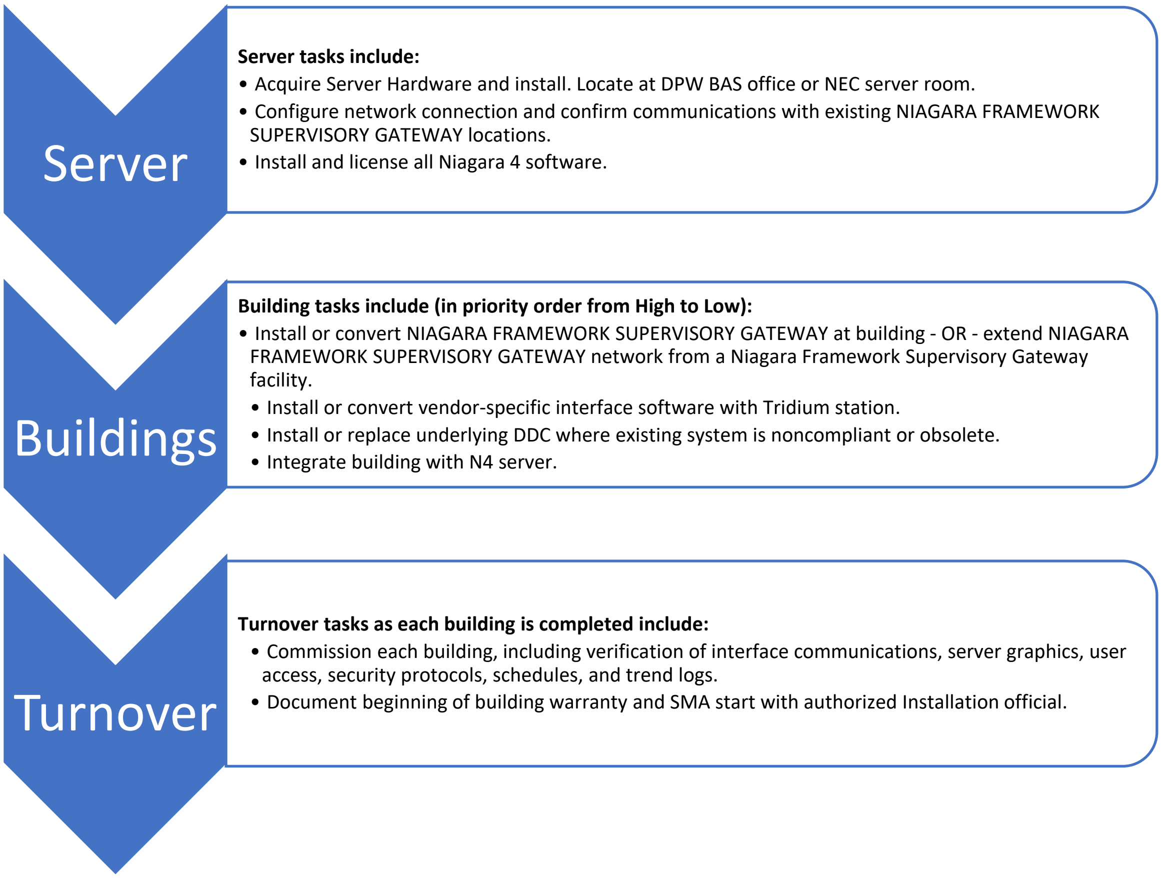
A. The Low-Priority existing control systems include SYSTEM D (31.25%), SYSTEM I (21.25%), SYSTEM K (3.75%), SYSTEM L (3.75%), SYSTEM E (2.5%), SYSTEM B (1.25%), SYSTEM H (1.25%), SYSTEM J (1.25%), and SYSTEM N (1.25%). This group also includes some buildings with pneumatic or other non-DDC systems (32.5%) that will be entirely replaced with a new Niagara Framework Supervisory Gateway and DDC system or an extended DDC from an adjacent building control system.

B. There is an existing network connection in 45% of the Low-Priority buildings; 55% of the buildings will need an FPOC installed or network connectivity extended from an adjacent building. The Contractor will be responsible for coordinating installation with the NEC for a new FPOC or extension of an existing network connection.

C. Most of the Low-Priority systems will require complete replacement with new N4. This will be a significant task; however, installing an FPOC to each Low-Priority building may consume as much time as replacing the systems.

6.06 INTEGRATION PATH

A. Some of the existing building control systems do not have an avenue to convert to Tridium N4 (see Vendor-Specific Niagara Framework Supervisory Gateway Integrations below). Depending on plan funding, there are three options for these buildings: 1) Replace all controls in the building and install a new N4 Niagara Framework Supervisory Gateway and N4 compatible DDC (recommended), 2) Install a new N4 Niagara Framework Supervisory Gateway at the building to establish an N4 footprint and leave the existing building control system in place until funding is available to replace, 3) Install a new N4 Niagara Framework Supervisory Gateway at the building and, where possible, integrate the existing control system using third-party software and devices (not recommended). Adding third-party software and devices increases the points of failure for the system.



Server

Server tasks include:

- Acquire Server Hardware and install. Locate at DPW BAS office or NEC server room.
- Configure network connection and confirm communications with existing NIAGARA FRAMEWORK SUPERVISORY GATEWAY locations.
- Install and license all Niagara 4 software.

Buildings

Building tasks include (in priority order from High to Low):

- Install or convert NIAGARA FRAMEWORK SUPERVISORY GATEWAY at building - OR - extend NIAGARA FRAMEWORK SUPERVISORY GATEWAY network from a Niagara Framework Supervisory Gateway facility.
- Install or convert vendor-specific interface software with Tridium station.
- Install or replace underlying DDC where existing system is noncompliant or obsolete.
- Integrate building with N4 server.

Turnover

Turnover tasks as each building is completed include:

- Commission each building, including verification of interface communications, server graphics, user access, security protocols, schedules, and trend logs.
- Document beginning of building warranty and SMA start with authorized Installation official.

Tasks for Servers, Buildings and System Turnover

B. Building control systems shall be installed in accordance with UFGS 23 09 00, *Instrumentation and Control for HVAC*. This specification includes a number of subspecifications by reference, including the following:

1. UFGS 23 09 13, *Instrumentation and Control Devices for HVAC*
2. UFGS 23 09 23.01, *Lonworks Direct Digital Control for HVAC and Other Building Control Systems*
3. UFGS 23 09 23.02, *BACnet Direct Digital Control for HVAC and Other Building Control Systems*
4. UFGS 23 09 93, *Sequences of Operation for HVAC Control*

C. UFGS 23 09 00 contains several tailoring options for selecting the building control system protocol; since INSTALLATION A is installing a Niagara Framework system, either Niagara BACnet or Niagara LonWorks should be selected:

1. Niagara BACnet will require the inclusion of UFGS 23 09 23.02 (using the Niagara Framework tailoring option in that UFGS) to provide specifications for a BACnet building with a Niagara Framework Supervisory Gateway.

2. Niagara LonWorks will require the inclusion of UFGS 23 09 23.01 (using the Niagara Framework tailoring option to provide specifications for a LonWorks building with a Niagara Framework Supervisory Gateway.
3. The following issues should be considered before selection of either LonWorks or BACnet:
    a) While in theory, some building control systems could be installed with LonWorks and some with BACnet and all be integrated to a common Niagara front end, this needlessly multiplies the number of independent systems that the DPW staff must learn and manage.
    b) INSTALLATION A has a good relationship with their existing Niagara/LonWorks Contractor; this argues for continuing with this approach and the use of UFGS 23 09 23.01, *Lonworks Direct Digital Control for HVAC and Other Building Control Systems*.
    a) Almost all CONUS HVAC vendors offer a BACnet product; very few vendors offer a LonWorks product. This casts doubt on the long-term support for a LonWorks solution and suggests that at some point INSTALLATION A may wish to begin to install BACnet buildings using UFGS 23 09 23.02, *BACnet Direct Digital Control for HVAC and Other Building Control Systems*.

D. Building control system repairs and conversions must also meet the following requirements:

1. All existing Niagara Framework Supervisory Gateways must be converted to full Niagara 4 Framework, not just Niagara 4 compatible. If the existing Niagara Framework Supervisory Gateway lacks capacity for an N4 software conversion, a new N4 Niagara Framework Supervisory Gateway must be provided and installed.
2. N4 drivers must be identified for all Niagara Framework Supervisory Gateways that can be software converted to N4 prior to the integration. If there are existing original equipment manufacturer (OEM) or third-party drivers without an N4 alternate available, a replacement must be engineered prior to beginning the conversion.
3. All Niagara Framework Supervisory Gateway licenses must remain open in accordance with the Tridium open NiCS licensing as detailed in UFGS 23 09 00.
4. The controls vendor must provide a minimum of three (3) years Software Maintenance Agreement (SMA) support for each Niagara Framework Supervisory Gateway converted or installed on the project in addition to their software and hardware warranty.

6.07 INTEGRATION TO THE UMCS SERVER

A. Once buildings have a converted Niagara Framework Supervisory Gateway running N4 software and the underlying building control system is resident in the Niagara Framework Supervisory Gateway, the building can be integrated into the basewide UMCS.[31] Integration requirements are covered in UFGS 25 10 10 *Utility Monitoring and Control System (UMCS) Front End and Integration* and include generic requirements for configuring alarms, trends, schedules, etc. as well as very basic requirements for graphics. Again, the “Niagara Framework” tailoring option should be used to select appropriate requirements. This specifically includes the controls vendor being responsible for engineering and installing all graphics and project-specific software onto the INSTALLATION A Niagara 4 server.

6.08 TRIDIUM N4 SOFTWARE ENVIRONMENT AND LICENSING

A. UMCS Server:

1. Niagara 4.x Supervisor—open (provided by one qualified vendor):

a) This will be the software running on the server as defined by the UMCS Plan. This software provides centralized system management for a network of multiple Niagara-based Niagara Framework Supervisory Gateway controllers.

b) The server vendor must provide an ***open*** N4 Supervisor capable of receiving stations from multiple vendors. All vendor stations must work within the standard Tridium N4 driver environment.

c) The server vendor must provide the initial Niagara 4 Supervisor license (SUP-UNL-SMA-INIT) with unlimited network connections and minimum 18-month Software Maintenance Agreement (SMA). The SMA must be maintained for the life of the system to ensure all software and drivers are kept current.

B. Workbench and Engineering tools:

1. Conceptually, Workbench (the engineering tools) must be separated out into two components:

a) The first component is the tool used to program and configure the Niagara Framework Supervisory Gateway. This should have an ***open license*** such that any vendor’s

[31] Although it may seem unusual to speak of mapping objects into the NIAGARA FRAMEWORK SUPERVISORY GATEWAY as a separate task from mapping them into the front-end server, this distinction is important because those tasks are specified using different UFGS. In practice, it is expected that integration to the front end will follow as a natural result of mapping the building systems into the building NIAGARA FRAMEWORK SUPERVISORY GATEWAY.

Workbench can be used on any vendor's Niagara Framework Supervisory Gateway—with the possible exception of proprietary drivers/components within a specific vendor's Niagara Framework Supervisory Gateway. The gateway programming and configuration tool should not be installed on the server—due to the risk of server compromise—but, instead, should be installed on a laptop (ideally with a docking station so that it has the convenience of a desktop) in the DPW UMCS shop.

b) The second component are the tools used to program the controllers ***below*** the Niagara Framework Supervisory Gateway. Each vendor typically has their own controller line, and these tools are largely proprietary, including any proprietary drivers and components in individual Niagara Framework Supervisory Gateways. Since many vendors have integrated these tools into their version of Workbench, this means that INSTALLATION A will likely require multiple (proprietary) versions of Workbench to accommodate all the different vendors' controllers beneath the Niagara Framework Supervisory Gateways. If there are additional copies of Workbench required to support specific vendor product lines (for controllers below the Niagara Framework Supervisory Gateway), these should be installed on dedicated computers, likely laptops, which can be carried into the field as necessary.

c) In the case where a specific vendor has not integrated their proprietary tools into their version of Workbench, vendors will need to install those tools on dedicated computers, likely laptops, which can be carried into the field as necessary.

d) These proprietary controllers below the Niagara Framework Supervisory Gateway mean that INSTALLATION A will not be able to program or configure these controllers with standard tools but will instead need to use vendor-specific tools. This is a fundamental limitation of the Niagara Framework and cannot easily be avoided.

e) Use of standard protocols (Lon in accordance with UFGS 23 09 23.01, or BACnet in accordance UFGS 23 09 23.02) should reduce, but not necessarily eliminate the need for vendor-specific components (usually in the form of proprietary JAR files) within individual Niagara Framework Supervisory Gateways. By and large, any programming or configuration within the Niagara Framework Supervisory Gateway should work from a vendor-neutral version of Workbench with an ***open*** license.

C. Niagara Framework Supervisory Gateway:

1. Any vendor preparing to connect a Niagara Framework Supervisory Gateway to the server will engineer their N4 Station offline using their own Workbench software with standard Tridium N4 drivers. If an engineering workstation does not already exist at INSTALLATION A DPW for the vendor's Workbench software, the vendor will provide one. The Workbench software will not be installed on the N4 server. When the station is complete and tested, it will be copied onto the N4 Server Supervisor. The vendor will connect (bind) the server to the Niagara Framework Supervisory Gateway and verify all points, graphics, trends, schedules, and user privileges are operating correctly before indicating the integration is complete.
2. For installations that require replacement of an obsolete or inoperable Niagara Framework Supervisory Gateway, a new 8000 series (optimized for Niagara 4) Niagara Framework Supervisory Gateway will be installed by the vendor. The vendor is responsible for providing the Niagara Framework Supervisory Gateway-8000-xx-xxxx with a license encompassing all devices and points necessary for all controllers and points that will reside under the new Niagara Framework Supervisory Gateway. The vendor will be responsible for commissioning the station and verifying the connection as described above.
3. For installations where the existing AX Niagara Framework Supervisory Gateway can be converted to N4, the vendor will be responsible for converting the AX station to N4. This includes maintenance or licensing fees associated with the conversion, commissioning the station, and verifying the connection as described above.

6.09 COMMISSIONING GUIDELINE

A. The UMCS Plan provides recommendations for repair and consolidation of the existing systems with varying levels of modification to the existing building control systems. Some will require full repair or replacement of obsolete controls and others will only need their central gateway brought up to the current communication and security standards for INSTALLATION A's UMCS. Regardless of the scope of the physical modifications, it is recommended that the Contractor provide commissioning services.

B. For buildings that will undergo a complete control system replacement, commissioning of all work is highly recommended. A complete control system replacement will include all existing DDC controllers, devices, and sensors, and all pneumatic receiver-controllers. Pneumatic device replacement will vary based on the age of the equipment being controlled. Equipment that is obsolete or has been designated for replacement may retain existing control devices rather than be installed with new devices. The Contractor will be required to compile preconstruction documentation of all existing systems and operating parameters. Once the repair or replacement is complete, the Contractor will commission all devices and sequences and provide documentation of the successful completion of the same. A final commissioning report will be completed noting any changes in sequencing or operating parameters between the preconstruction documentation and final commissioning.

C. Buildings where the core HVAC control system can meet the new communications and security requirements for INSTALLATION A's UMCS also have commissioning recommendations. It is recommend to retrocommission any building where preventive maintenance is not regularly performed on the HVAC building automation system, the control devices have not had their calibration verified within the last 18 months, or the control sequences or operation have not been verified in over 24 months.

D. Retrocommissioning includes verifying sensor data and operation of all control devices: existing or new. Sequences of operation will be documented for any buildings without an as-built record. Those with as-built sequence of operations records will be verified. The final retrocommissioning report should include schematic diagrams, points lists, sequences of operations, and device lists for all systems operating on the building HVAC control system.

E. This commissioning guideline defines a path where the Controls Contractor performs and documents all commissioning work. It is recommended that INSTALLATION A dedicate resources from the departments that will be responsible for the building's controls after completion to participate in the commissioning process. For some of the larger and more complex buildings it may be prudent for INSTALLATION A to add another layer of verification by employing a third-party commissioning authority to oversee and manage the commissioning process.

6.10 CYBERSECURITY FOR BUILDING CONTROL SYSTEMS

A. Contractor cybersecurity requirements are covered in UFGS 25 05 11, *Cybersecurity for Facility-Related Control Systems*. In addition to requiring submittals documenting the building control systems, this UFGS will place a number of requirements on the Niagara Framework Supervisory Gateway related to the following:

1. Access Control for user accounts and login procedures
2. Identification and Authentication of users
3. Auditing of events, both in the control system and at the server
4. Other cybersecurity requirements

In addition, there may be some requirements placed on the underlying building control systems.

B. See Appendix C—"Critical Building UMCS Cybersecurity" for special considerations for critical buildings.

6.11 PLAN SCHEDULE

A. The buildings included in the INSTALLATION A integration compose approximately *X* SF± (square feet) of building space. Based on the site scoping survey, 22% of that space requires a major installation, conversion, or replacement of the current DDC to comply with the goals of this plan. The remaining 78% only require a relatively minor integration of network infrastructure and control modules or Niagara Framework Supervisory Gateway conversions to achieve compliance. Under ideal conditions, if all work was completed simultaneously, the conversion and integration would finish in under two years. The actual schedule will require phasing the work: server installation and configuration, High-Priority building conversions, Medium-Priority building conversions, and Low-Priority building conversions. Physical access requirements and coordination with the Contractor between all INSTALLATION A groups impacted by the conversion on a per building basis will significantly impact overall schedule.

B. The High-, Medium-, and Low-Priority buildings represent a broad distribution across INSTALLATION A (see Appendix A). As described earlier in the plan these priorities take into account several factors for building placement. For estimate purposes, the priority groups have been further refined into strictly technical groups. This plan recommends that system conversions and replacements be performed in order from Group "A" to Group "M." Within each group, the replacement order will be from High Priority to Low Priority.

C. The first plan phase will be acquisition, configuration, licensing, and initial testing of the Niagara 4 server. This is expected to take three to four months. Once the server is online, the building conversion phase would begin. Converting High-Priority buildings will be the first part of this phase. Ideally, converting buildings with minor requirements and those with major requirements would occur simultaneously, utilizing multiple Contractor teams. Medium-Priority and Low-Priority conversions would follow in the same fashion.

D. GROUP A

1. Current AX Niagara Framework Supervisory Gateway with N4 Conversion Capability (*X* SF±): This group consists of all Low-, Medium-, and High-Priority SYSTEM M installations with current Niagara Framework Supervisory Gateway models capable of conversion to N4. These systems will be software converted to AX 3.8 then to N4. These control system conversions should be the fastest to completion. No hardware replacements should be necessary.

E. GROUP B

1. Obsolete AX Niagara Framework Supervisory Gateway Replacement—High Priority I (*Y* SF±): This group consists of High-Priority SYSTEM M installations with obsolete Niagara Framework Supervisory Gateway models that will be replaced prior to converting the station to N4. A new N4 compatible Niagara Framework Supervisory Gateway will be installed, and any incompatible Niagara Framework Supervisory Gateway expansion modules will be replaced.

F. GROUP C

1. Obsolete AX Niagara Framework Supervisory Gateway Replacement—High Priority II (*Z* SF±): This group consists of High-Priority SYSTEM M installations with obsolete Niagara Framework Supervisory Gateway models that will be replaced prior to converting the station to N4. A new N4 compatible Niagara Framework Supervisory Gateway will be installed, and any incompatible Niagara Framework Supervisory Gateway expansion modules will be replaced.

G. GROUP D

1. Obsolete AX Niagara Framework Supervisory Gateway Replacement—Low/Med Priority (α SF±): This group consists of Low and Medium-Priority SYSTEM M installations with obsolete Niagara Framework Supervisory Gateway models that will be replaced prior to converting the station to N4. A new N4 compatible Niagara Framework Supervisory Gateway will be installed, and any incompatible Niagara Framework Supervisory Gateway expansion modules will be replaced.

H. GROUP E

1. Obsolete R2 System Replacement—High Priority (β SF±): This group consists of High-Priority SYSTEM N installations that cannot be converted to N4. A new N4 compatible Niagara Framework Supervisory Gateway will be installed, and any incompatible Niagara Framework Supervisory Gateway expansion modules will be replaced. A new N4 station will be engineered from the existing R2 station.

I. GROUP F

1. Obsolete R2 System Replacement—Low/Med Priority (γ SF±): This group consists of Low- and Medium-Priority SYSTEM N installations that cannot be converted to N4. A new N4 compatible Niagara Framework Supervisory Gateway will be installed, and any incompatible Niagara Framework Supervisory Gateway expansion modules will be replaced. A new N4 station will be engineered from the existing R2 station.

J. GROUP G

1. Obsolete DDC System with FPOC Replacement—High/Med Priority (δ SF±): This group consists of High- and Medium-Priority DDC installations that cannot be converted to N4. A new

N4 compatible Niagara Framework Supervisory Gateway and DDC system will be installed.

K. GROUP H

1. Obsolete DDC System with FPOC Replacement—Low Priority (ε SF±): This group consists of Low-Priority DDC installations that cannot be converted to N4. A new N4 compatible Niagara Framework Supervisory Gateway and DDC system will be installed.

L. GROUP J

1. Obsolete Control System with no FPOC Replacement—High Priority (ζ SF±): This group consists of High-Priority control installations that cannot be converted to N4 and do not have a dedicated network connection. An FPOC will be installed. A new N4 compatible Niagara Framework Supervisory Gateway and DDC system will be installed. Some of the existing control systems in this group are non-DDC pneumatic and may require additional control device replacement.

M. GROUP K

1. Obsolete Control System with no FPOC Replacement—Med Priority (η SF±): This group consists of Medium-Priority control installations that cannot be converted to N4 and do not have a dedicated network connection. An FPOC will be installed. A new N4 compatible Niagara Framework Supervisory Gateway and DDC system will be installed. Some of the existing control systems in this group are non-DDC pneumatic and may require additional control device replacement.

N. GROUP L

1. Obsolete Control System with no FPOC Replacement—Low Priority (θ SF±): This group consists of Low-Priority control installations that cannot be converted to N4 and do not have a dedicated network connection. An FPOC will be installed. A new N4 compatible Niagara Framework Supervisory Gateway and DDC system will be installed. Some of the existing control systems in this group are non-DDC pneumatic and may require additional control device replacement.

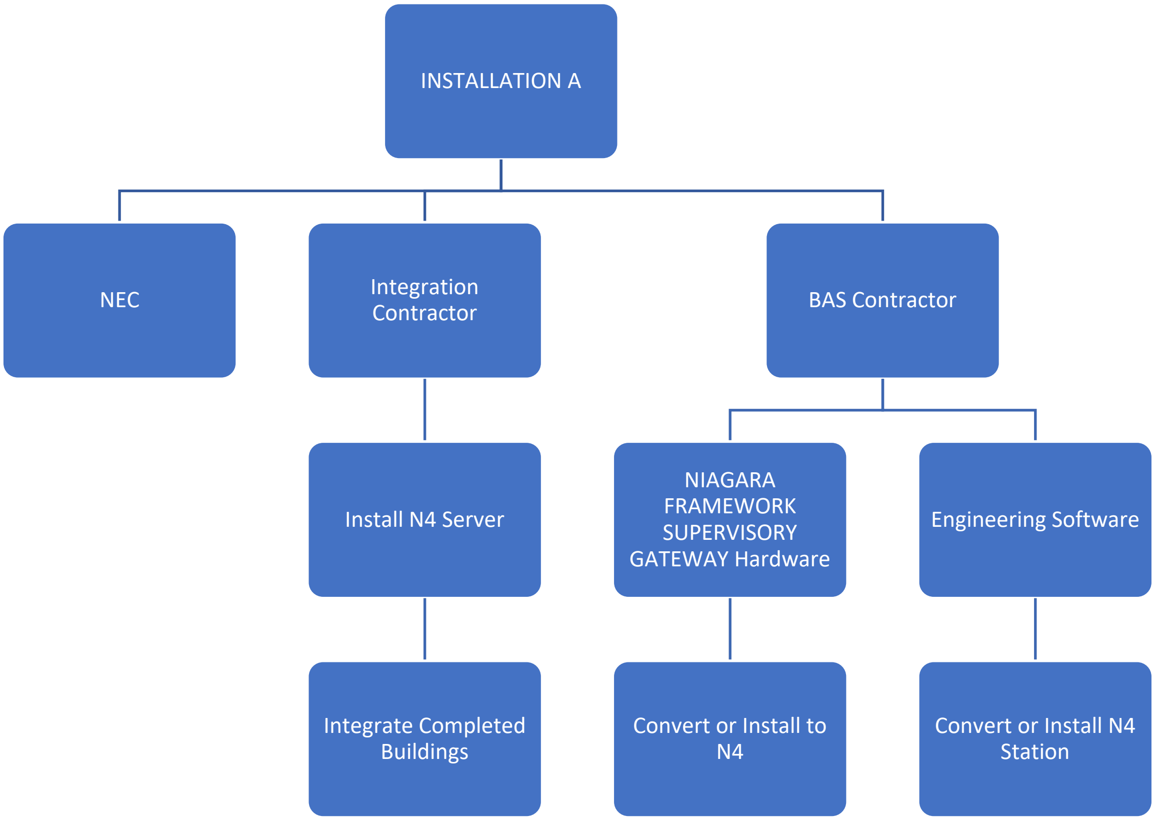
6.12 ROLES

A. During and after the UMCS conversion, several roles will need to be filled for management, maintenance, and operation. Some of these INSTALLATION A roles may already exist, and others may be combined to a single person. Proper staffing is key to realizing the full potential of the UMCS, and consideration needs to be given to any roles that are not currently covered. This plan is structured to keep the INSTALLATION A DPW in a position to manage all aspects of the UMCS internally rather than heavily rely on Contractors.

B. IMPLEMENTATION

Implementation of this plan requires the following roles to be filled:

1. INSTALLATION A Project Manager(s): On-base representative(s) monitoring progress, assisting with building access, coordinating INSTALLATION A departments as necessary, and assisting with project close-out. The project PM(s) will also assist with turning over completed portions of the UMCS to the operational support staff. This will include commissioning of each integration to confirm all software, graphics, licensing, and specification requirements have been met prior to acceptance by the operations team.
2. INSTALLATION A NEC Representative: On-base representative responsible for being familiar with the NEC scope of the project, assisting with server connectivity, hardware and networking requirements, and FPOC installation and activation
3. System Integrator (Contractor): Contractor responsible for installing, configuring, and licensing the N4 server; integrating each building to the server as it is converted; and coordinating network and security protocols with INSTALLATION A NEC
4. DDC Conversion Contractor: Where possible, converts Niagara Framework Supervisory Gateway to N4, otherwise provides new N4 Niagara Framework Supervisory Gateway. Works with Integrator to add Niagara Framework Supervisory Gateway and underlying DDC to new N4 server. Provides engineering and installation of a new DDC where required (long-term plan)



C. SUSTAINMENT

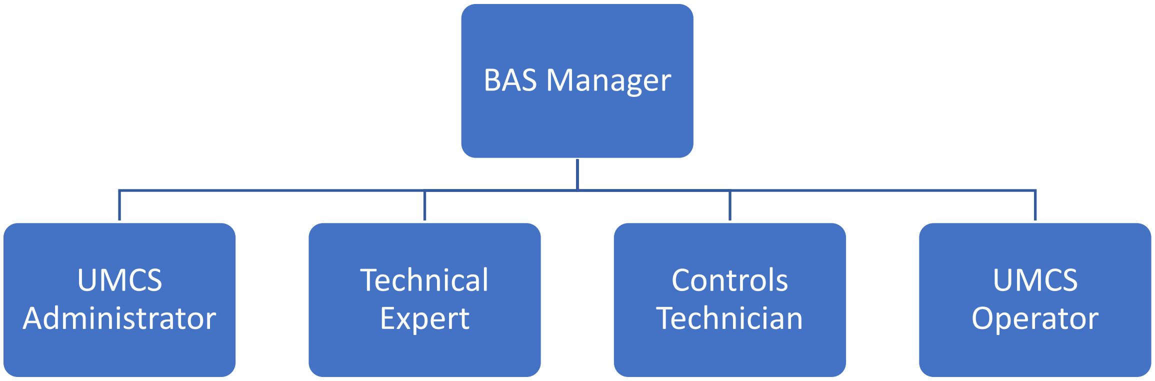
Achieving the full potential of the new UMCS will require a significant investment in staffing at the DPW. Prior to the new UMCS being turned over, this plan requires the following roles to be filled:

1. BAS Manager: This role provides the individual at the garrison with the responsibility and authority to make local decisions concerning the BAS, including planning, project prioritization, and system operation.
2. UMCS Administrator: This role provides the necessary IT expertise to the DPW in support of the UMCS, performs IT management for the UMCS, and coordinates UMCS IT issues with NEC.
3. Technical Expert: This role provides expertise on the BAS technology (Niagara Framework and, to a lesser degree, the underlying control systems). The key responsibilities for this role are the review of project submittals (designs, as-built drawings, etc.) and participation in control system acceptance.
4. Controls Technician: This role provides control system maintenance expertise and support to DPW O&M staff. An approach that has worked at other installations is to start with contract personnel in the form of dedicated Controls Technicians who provide direct O&M support along with on-the-job

training to the DPW. This role should transition to O&M staff as they become trained. Note that this role will scale with the size of the UMCS; ultimately, INSTALLATION A will require several full-time-equivalent employees.

5. UMCS Operator: The purpose of this role is to use the UMCS to monitor and control the connected BCSs. The UMCS Operator provides remote troubleshooting and diagnostic support. The Operator can also adjust schedules, set up trending, configure demand limiting, and to otherwise take advantage of the power and capabilities of the BAS in support of the garrison. Again, this role scales with the size of the UMCS, and INSTALLATION A will require several full-time-equivalent employees.

Note that these requirements are significant but are necessary to maintain the UMCS and take full advantage of the energy management and system performance capabilities of the UMCS.



6.13 VENDOR-SPECIFIC NIAGARA FRAMEWORK SUPERVISORY GATEWAY INTEGRATIONS

A. Several of the existing control vendors have OEM Tridium Niagara Framework Supervisory Gateway devices installed or available for installation. Most indicate their Niagara Framework Supervisory Gateway is currently capable of being converted to Niagara N4 compatibility or there is a conversion to N4 in development. As the UMCS Plan nears completion, recommendations regarding the vendor options will be finalized based on vendor progress.

B. **SYSTEM A**: SYSTEM A carries several different control product lines for various applications. They have marked their XYZ Controller (Niagara AX Framework based) as obsolete. There is only one building identified in the INSTALLATION A survey with SYSTEM A controls. It would not be cost effective to try and maintain a Niagara interface with this single instance of SYSTEM A. This building will require a new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC.

C. **SYSTEM B**: Vendor A carries multiple control products including SYSTEM B for HVAC control. The INSTALLATION A survey identified only one building with a SYSTEM B installation at INSTALLATION A. This does not warrant connecting the existing SYSTEM B to the new Niagara Framework. This building will require a new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC.

D. **System C**: Vendor B is in the process of replacing their SYSTEM C control system workstation software with ABC. The INSTALLATION A survey identified two buildings with SYSTEM C installed. One of these is a recent installation with no Niagara Framework connectivity and no DPW ownership. The other installation is an Air National Guard building slated for turn over to INSTALLATION A. This building will be converted by replacing the SYSTEM C and installing a new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC.

E. **SYSTEM D**: SYSTEM D represent one of the larger installations at INSTALLATION A (15% of qualifying buildings). SYSTEM D offers a JSYSTEM DC-8000 Niagara Framework Supervisory Gateway that is Niagara 4 compliant. However, as of this writing (January 2019), there is no interface between legacy SYSTEM D DDC and N4. For all SYSTEM M 3.8 or higher SYSTEM D installations, the existing system will be integrated with the new N4 system. For older SYSTEM D installations, a new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC will be installed.

F. **SYSTEM E**: The INSTALLATION A survey identified four buildings with SYSTEM E controls installed. These controls are obsolete and will be replaced as part of the UMCS Integration Plan. A new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC will be installed.

G. **SYSTEM F**: There is a small installation of SYSTEM F at INSTALLATION A. The INSTALLATION A survey identified SYSTEM F still active in one building, which also contained a SYSTEM D used for metering only. The HVAC SYSTEM F will be replaced with a new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC.

H. **SYSTEM G**: The INSTALLATION A survey identified five SYSTEM G installations. The newer installations in four out-of-scope buildings will remain as installed. There is one older installation that will be replaced with a new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC.

I. **SYSTEM H**: The INSTALLATION A survey identified eight buildings with SYSTEM H that qualify for the UMCS conversion. Most of these SYSTEM H installations are already Niagara Framework compliant, with one already N4 capable. The AX- and N4-capable Niagara Framework Supervisory Gateways will be converted to full N4 compliance. Older SYSTEM H installations will be converted with the SYSTEM H EC-BOS series Niagara Framework Supervisory Gateway and migrated to N4.

J. **SYSTEM I**: The SYSTEM I installations at INSTALLATION A include several generations of SYSTEM I from some of the oldest systems, including some with pneumatics, to the latest Niagara AX Framework-compliant systems. Obsolete SYSTEM I will be replaced with the SYSTEM I WEB-8000 Niagara Framework Supervisory Gateway controller and an N4-compliant DDC. SYSTEM I WEB-###-AX installations will be converted to N4 where possible or replaced with the WEB-8000 Niagara Framework Supervisory Gateway and have their stations converted from AX to N4.

K. **SYSTEM J VRF**: There are two SYSTEM J VRF installations identified in the INSTALLATION A survey UMCS plan. These installations only control and monitor equipment specific to the VRF and are not connected to the UMCS. However, SYSTEM J carries a Tridium OEM Niagara Framework Supervisory Gateway (PBAC-NBTR0A) in their product line that can communicate in BACnet, LonWorks, or using Niagara Framework. This Niagara Framework Supervisory Gateway is only intended to allow SYSTEM J control systems to integrate with third-party building management systems. We recommend keeping the SYSTEM J controls in place for managing the VRF. However, another DDC should be installed at the building to handle other HVAC control and monitoring needs and to integrate with the SYSTEM J Niagara Framework Supervisory Gateway. The new DDC will integrate the SYSTEM J VRF and additional systems with the new N4 server.

L. **SYSTEM K:** There are eight buildings marked by the INSTALLATION A survey for conversion in the UMCS plan. Unfortunately, the System K products at INSTALLATION A were not designed to interface with a Tridium server. There are products available through third parties to create an interface with SYSTEM K to N4; however, this is not a recommended path. The SYSTEM K HVAC installations will be replaced with a new N4 Niagara Framework Supervisory Gateway and N4-compliant DDC.

M. **SYSTEM L**: The INSTALLATION A survey identified seven buildings with SYSTEM L Talon controls. Most of these controls are already Niagara AX Framework compliant. However, the TNM-2 Niagara Framework Supervisory Gateways are obsolete and not compatible with N4, and in some cases, the TNM-6 Niagara Framework Supervisory Gateways lack the necessary capacity to convert to N4. Talon Niagara Framework Supervisory Gateways with the capacity will be converted to N4 along with their Station software. Incompatible Niagara Framework Supervisory Gateways will be replaced with a new TNM-8000 and the underlying DDC will be converted to be N4 compliant.

N. **SYSTEM M**: The SYSTEM M installations at INSTALLATION A were identified as the largest of the DDC installations (48%) by the INSTALLATION A survey. Most of the SYSTEM M installations with a Niagara Framework Supervisory Gateway model 7 or higher should be able to perform a software conversion to N4. The conversion is performed in multiple steps: the Station is converted from AX to N4, the Niagara Framework Supervisory Gateway is then converted from AX x.x to AX 3.8 to N4. Previous projects, some model 6e Niagara Framework Supervisory Gateways lack the capacity to run N4 software after the conversion. This is not an issue that can be identified in advance using the Tridium conversion tool. Because of this, we recommend all 6e and lower model Niagara Framework Supervisory Gateways be replaced with the new Niagara Framework Supervisory Gateway-8000 series and a converted N4 Station.

O. **SYSTEM N**: The SYSTEM N installations are only second to the SYSTEM M installations in size at INSTALLATION A per the survey. Unfortunately, these are obsolete systems, and there is no automatic conversion path from SYSTEM N to N4. The existing R2 database configuration, programming, all operating parameters, and all information necessary for re-creating the control system must be retrieved from the R2 system prior to decommissioning. Per Tridium, all SYSTEM N systems will require reengineering to convert. The R2 Stations will have to be manually reengineered into an N4 Station as there is no conversion tool. A new Niagara Framework Supervisory Gateway-8000 series controller will be installed, and the underlying R2 controllers will have to be converted as well to meet N4 requirements.

APPENDIX A

INSTALLATION A MAP WITH HIGHLIGHTED PRIORITIES

MAP HIGHLIGHTS KEY

GREEN AREA HIGHLIGHT—HIGH PRIORITY

YELLOW AREA HIGHLIGHT—MEDIUM PRIORITY

RED AREA HIGHLIGHT—LOW PRIORITY

APPENDIX B

INSTALLATION A NETWORK PLAN

APPENDIX C

CRITICAL BUILDING UMCS CYBERSECURITY

APPENDIX D

FINAL PHASE ROM ESTIMATE

APPENDIX E

INSTALLATION A SURVEY REPORT

SURVEY CONTENT:

1. Building Number
2. Priority
3. Duplicate
4. Integration Path
5. Building Name
6. Alternate Name
7. Map
8. Location
9. Area (SF)
10. Units
11. Controls
12. Control System Version
13. NFSG Model
14. N4 Readiness
15. GATEWAY/GUI Location
16. GUI
17. Gateway
18. Meter

19. Network Connection
20. IP Address
21. Survey
22. Non-DDC Zones
23. NFSG Count
24. Primary Control Count
25. Secondary Control Count
26. Zones
27. Notes
28. Priority
29. Questions
30. Mechanical Systems

Abbreviations

Acronym	Term
ACAS	Assured Compliance Assessment Solution
AF	Air Force
AHU	Air Handling Unit
AMP	Army Metering Program
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
APMS	Army Portfolio Management System
AR	Army Reserve
ASA (IE&E)	Assistant Secretary of the Army (Installations, Energy and Environment)
ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
ATC	Authority to Connect
ATO	Authority to Operate
AX	NFSG model 'AX'; previous generation technology
BACnet	Building Automation Control Network
BACS	Building Automation and Control Systems
BAS	Building Automation System (earlier name for UMCS, now UMCS is sanctioned by DoD Unified Criteria and Guide Specifications
BASEOPS	Base Operations
B-AWS	BACnet Advanced Workstation
BCN	Building Control Network
BCS	Building Control System
BEMS	Building Energy Management System
BMS	Building Management System
BOC	Building Operations Center
BOID	Business Operation and Integration Division
BOS	Base Operations and Support
BTL	BACnet Testing Labs
CA	Condition Assessment
CEWE	Comprehensive Energy and Water Evaluation
CIA	Confidentiality, Integrity, and Availability
CLD	Control Logic Diagram
CMMS	Computerized Maintenance Management System
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COE	Corps of Engineers (US Army)
CONUS	Continental United States

Acronym	Term
COOP	Continuity of Operation Plan
COR	Contracting Officer Representative
CPU	Central Processing Unit
CRAC	Computer Room Air Conditioner
Cx	Commissioning
DA	Department of the Army
DCS	Deputy Chief of Staff
DCS	Distributed Control System
DDC	Direct Digital Control
DNP	Distributed Network Protocol
DoD	Department of Defense
DPW	Directorate of Public Works
DX	Direct Expansion
ECM	Energy Conservations Measure
EEDRS	Enterprise Energy Data Reporting System
EISA	Energy Independence and Security Act
eMASS	Enterprise Mission Assurance Support Service
EMCS	Energy Monitoring and Control System (deprecated, see UMCS)
EMUCS	Energy Management and Utility Control System
ERCIP	Energy Resilience and Conservation Investment Program
ERDC-CERL	Engineer Research Development Center-Construction Engineering Research Laboratory
ESCO	Energy Service Company
ESEP	Engineer Senior Executive Panel
ESPC	Energy Savings Performance Contract
ESS	Electronic Security System
ESTCP	Environmental Security Technology Certification Program
EUB	End Use Building Switch
FAR	Federal Acquisition Regulation
FCN	Field Control Network
FCU	Fan Coil Unit
FE	Front End
FEMP	Federal Energy Management Program
FIG	Facility Investment Guidance
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FMS	Facility Management System
FPOC	Facility Point of Connection
FRCS	Facility-Related Control System
GUI	Graphical User Interface
HNC	Huntsville Engineering and Support Center (Huntsville Division)

Acronym	Term
HOA	Hand-Off-Auto
HVAC	Heating, Ventilating, and Air-Conditioning
IA	Information Assurance
IAP	Information Assurance Professional
IASO	Information Assurance Security Officer
IAW	In Accordance With
ICAN	Installation Campus Area Network
ICS	Industrial Control System
IDG	Installation Design Guide
IDIQ	Indefinite Delivery Indefinite Quantity
IDS	Intrusion Detection System
IG	Inspector General
IMCOM	Installation Management Command
IP	Internet Protocol
IS	Information Systems
IS-Cx	Installation Support Center of Expertise
IT	Information Technology
JOC	Job Order Contract
KSA	Knowledge, Skills and Abilities
LAN	Local Area Network
LCCA	Life-Cycle Cost Analysis
LNS	LonWorks Network Service
Lon	Local Operating Network
MACOMS	Major Commands
MATOC	Multiple Award Task Order
M&C	Monitoring and Control (Software)
MCA	Military Construction Army
MCX	Mandatory Center of Expertise
MDMS	Meter Data Management System
MICC	Mission Installation Contracting Command
MILCON	Military Construction
MIPR	Military Interdepartmental Purchase Request
MS	Microsoft
M&S	Maintenance and Services
MSF	Million Square Feet
MS/TP	Master Slave Token Passing
N4	NFSG model 'N4'; current generation technology (Niagara version 4)
NAF	Nonappropriated Funds
NDAA	National Defense Authorization Act
NEC	Network Enterprise Center

Acronym	Term
NiCS	Niagara Compatibility Statement
NIST	National Institute of Standards and Technology
NSFG	Niagara Framework Supervisory Gateway (nonproprietary term for a NIAGARA FRAMEWORK SUPERVISORY GATEWAY)
OEM	Original Equipment Manufacturer
O&M	Operation and Maintenance
OMD	Operation and Maintenance Division/Department
OPC	Open Platform Communications
OT	Operational Technology
PII	Personally Identifiable Information
PIT	Platform Information Technology
PLC	Programmable Logic Controllers
PM	Preventive Maintenance
PM	Project Manager
POAM	Plan of Action and Milestones
POC	Point of Contact
POM	Program Objective Memorandum
PVT	Performance Verification Testing
QA	Quality Assurance
QC	Quality Control
R2	NFSG model 'R2'; obsolete technology
RACI	Responsible, Accountable, Consulted, and Informed
Re	Regarding
RCx	Retro or Re-commissioning
RDTE	Research Development Test and Evaluation
RFP	Request for Proposal
RMF	Risk Management Framework
SA	Service Agreements
SATOC	Single Award Task Order
SBMS	Smart Building Management Systems
SCADA	Supervisory Control and Data Acquisition
SI	System Integrator
SIM	System Integration Methodology
SMA	Software Maintenance Agreement
SME	Subject matter expert
SO	System Owner
SOW	Statement of Work
SP	Special Publication
SRM	Sustainment, Restoration and Modernization
STIGs	Security Technical Implementation Guides

Acronym	Term
TAB	Testing, Adjusting, and Balancing
techs	technicians
TLS	Transport Layer Security
TR	Technical Report
TSR	Technical Support Representative
UCS	Utility Control System
UESC	Utility Energy Savings Contract
UFC	Unified Facilities Criteria
UFGS	Unified Facilities Guide Specification
UMCS	Utility Monitoring and Control System
UP	Utilities Privatization
UPS	Uninterruptable Power Supplies
USACE	United States Army Corps of Engineers
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
VAV	Variable Air Volume
V-E	Value Engineering
VLAN	Virtual Local Area Network

Index

This page intentionally left blank

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)
August 2022

2. REPORT TYPE
Final

3. DATES COVERED (From - To)

4. TITLE AND SUBTITLE
Installation Utility Monitoring and Control System Technical Guide

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT

6. AUTHOR(S)
Joseph Bush, Eileen Westervelt, Brian Clark, David Schwenk, Stephen Briggs, Daniel Shepard, M. Cary Long, Tapan Patel, Melanie Johnson, and Eric Lynch

5d. PROJECT NUMBER
Project 19A01

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army Engineer Research and Development Center (ERDC)
Construction Engineering Research Laboratory (CERL)
PO Box 9005
Champaign, IL 61826-9005

8. PERFORMING ORGANIZATION REPORT NUMBER
ERDC/CERL SR-22-1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Headquarters, US Army Corps of Engineers
Standards and Criteria Program
Washington, DC 20314-1000
And
Headquarters, Department of the Army, Deputy Chief of Staff Army G-9
Army Installation Technology Transition Program (ITTP)
Washington, DC

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
MIPR 11268080

14. ABSTRACT

Army policy calls for each installation to install a building automation system (aka utility monitoring and control system [UMCS]) to provide for centralized monitoring of buildings and utilities to reduce energy and water commodity and maintenance costs.

Typically, the UMCS, including building control systems (BCS), is in-stalled and expanded in piecemeal fashion resulting in intersystem in-compatibilities. The integration of multivendor BCSs into a single base-wide UMCS, and subsequent UMCS operation, can present technical and administrative challenges due to its complexity and cybersecurity requirements.

Open Control Systems technology and open communications protocols, including BACnet, LonWorks, and Niagara Framework, help overcome technical incompatibilities. Additional practical considerations include funding, control systems commissioning, staffing, training, and the need for a commitment to proper operation, use, and sustainment of the UMCS.

This document provides guidance to Army installations to help achieve a successful basewide UMCS through its full life cycle based on DoD criteria and technical requirements for Open Control Systems and cybersecurity. It includes institutional knowledge on technical solutions and busi-ness processes amassed from decades of collaboration with Army installations and learned from and with their staff. Detailed activities spanning both implementation and sustainment include planning, procurement, installation, integration, cybersecurity authorization, and ongoing management.

15. SUBJECT TERMS

Military—Facilities; Military—Buildings; Utilities—Energy--Management—Automation; Electric utilities; Water utilities; Conservation; Open Control System; Heating, Ventilating, and Air-Conditioning (HVAC), Utility Monitoring Control System (UMCS), building controls, Building Automation System (BAS)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	SAR	243	**19b. TELEPHONE NUMBER (include area code)**