**FACILITY-RELARED CONTROL SYSTEMS**

**IT TELECOMMUNICATIONS AND NETWORKING GUIDELINE**

|  |
| --- |
| **DOCUMENT CONTROL** |
| **VERSION** | **DESCRIPTION** |
| Version 1.0 – 10/31/2016  | Draft |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Contents

[1.1 PURPOSE AND SCOPE 4](#_Toc465667178)

[1.2 BACKGROUND 4](#_Toc465667179)

[1.3 APPLICABLE POLICIES, STANDARDS AND PROCEDURES 4](#_Toc465667180)

[1.4 ROLES AND RESPONSIBILITIES 6](#_Toc465667181)

[1.5 REQUIRED SUBMITTALS 7](#_Toc465667182)

[1.6 APPLICABLE ESTCP TEMPLATES 7](#_Toc465667183)

[1.7 GLOSSARY (PER UFC 3-580-01 01 Jun 2016 Change 1, 01 Jun 2016) 7](#_Toc465667184)

[1.8 REQUIREMENTS FOR SUBJECT MATTER EXPERTS 11](#_Toc465667185)

[1.9 JOINT INFORMATION ENVIRONMENT 11](#_Toc465667186)

[1.10 PUBLIC SAFETY NETWORK (PSNET) 13](#_Toc465667187)

[1.11 NIPRNET AND COMMERICAL CARRIER NETWORKS 13](#_Toc465667188)

[1.12 OPERATIONS CENTER (OC) 13](#_Toc465667189)

[2.1 OPERATIONAL TECHNOLOGIES (OT) 14](#_Toc465667190)

[2.2 WIDE AREA NETWORKS (WAN) 14](#_Toc465667191)

[2.3 LOCAL AREA NETWORKS (LAN) 14](#_Toc465667192)

[2.4 WIRELESS NETWORKS 14](#_Toc465667193)

[2.5 PORTS, PROCTOCOLS AND SERVICES (PPS) 14](#_Toc465667194)

[2.6 TELECOMMUNICATIONS AND NETWORK DESIGN REQUIREMENTS 15](#_Toc465667195)

[3.1 GIGABIT PASSIVE NETWORK (GPON) 16](#_Toc465667196)

[3.2 SPACE REQUIREMENTS 16](#_Toc465667197)

[3.3 PATHWAY REQUIREMENTS 16](#_Toc465667198)

[3.4 ALARMING CARRIER REQUIREMENTS 16](#_Toc465667199)

[3.5 ALARM MONITORING SYSTEM 16](#_Toc465667200)

[3.6 OLT 18](#_Toc465667201)

[3.7 ONT COPPER ETHERNET INTERFACES 19](#_Toc465667202)

[3.8 ONT COPPER ANALOG INTERFACES 19](#_Toc465667203)

[3.9 ONT COPPER COAXIAL INTERFACES 19](#_Toc465667204)

[3.10 ONT REMOTE POWERING 19](#_Toc465667205)

[3.11 ONT REMOTE POWERING 20](#_Toc465667206)

[3.12 CROSS-DOMAIN ENTERPRISE 20](#_Toc465667207)

[4.1 NETWORK SECURITY OPERATIONS CENTER (NOSC) 21](#_Toc465667208)

[4.2 CYBER RANGES 21](#_Toc465667209)

[4.3 MISSION ASSURANCE 21](#_Toc465667210)

[4.4 USCYBERCOM 21](#_Toc465667211)

[4.5 DEPARTMENT OF VETERANS AFFAIRS 21](#_Toc465667212)

CHAPTER 1. INTRODUCTION

1.1 PURPOSE AND SCOPE This document defines the IT Telecommunications and Network Standards for ESTCP Facility-Related Control System (CS) projects. The intention of this document is to provide a general outline and guide to ensure the IT Telecommunications and Network Transport Backbone, cabling, wireless, firewalls, routers, switches and end-point devices are properly installed, configured and tested to meet DoD CIO, DISA and service/agency connectivity requirements.

1.2 BACKGROUND The DoD follows industry and DISA best practices and guidance for designing and operating Telecommunications and Networks. Currently, the DoD is transitioning to the Joint Information Environment (JIE) as defined by Department of Defense Instruction 8530 Cybersecurity Activities Support to DoD Information Network Operations March 2016. DISA, as the lead agency for implementing the JIE, has developed guidance and STIG’s for telecommunications and network components. A second technological objective of DoD is to implement IPv6 and use optical fiber networks to reduce the total cost of ownership of the IT infrastructure. For DOD facilities, this is enables multiple benefits; AMI connections can now support Multi-Protocol Layer Switching (MPLS) for real time demand and supply of electrical power and Microgrids, reduces the number of Telecom Distribution Rooms and associated HVAC cooling, and extends the length of a network segment from feet to miles.

This Guideline covers both the legacy Telecommunications and Networks, and the next generation Gigabit Passive Optical Networks (GPONs). The Unified Facility Criteria 3-580-01 Telecommunications Interior Infrastructure Planning And Design June 2016, provides the primary criteria; this chapter provides supplemental guidance related to cybersecuring the exterior and interior networks that transmit CS data.

If the ESTCP project involves medical facilities, additional requirements may apply. The DoD and the Department of Veterans Affairs have joint responsibilities for military and veteran healthcare and over the next decade plan to construct multiple joint use facilities. The VA Telecommunications and Network Design Guide was updated in 2016 and coordinated with the Defense Health Agency Facilities Division and incorporated into the joint MIL Standard 1691 and Space and Equipment Planning Systems (SEPS) guides.

This Guideline provides specific requirements for Levels 3-5 of the 5 Level Control System Architecture outlined in UFC 4-010-06 Cybersecurity of Facility-Related Control Systems. CS network equipment in these levels includes all of the traditional IT Telecommunications and Network transport backbone, WAN, LAN, firewalls, routers, switches and wireless access points.

1.3 APPLICABLE POLICIES, STANDARDS AND PROCEDURES

* CNSSI 1253, Security Categorization And Control Selection For National Security Systems 2014
* Department of Defense Instruction 8500.01, Cybersecurity, March 2014 (available online at www.dtic.mil)
* Department of Defense Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 2014 (available online at [www.dtic.mil](http://www.dtic.mil))
* Department of Defense Instruction 8140 Cyberspace Workforce Management (available online at <http://www.wbdg.org/pdfs/dod_cyberworkforce.pdf>)
* Department of Defense Instruction 8530 Cybersecurity Activities Support to DoD Information Network Operations March 2016 (available online at <http://www.wbdg.org/pdfs/DODI_853001_2016.pdf>)
* Department of Defense Industrial Control Systems Advanced Tactics, Techniques and Procedures Jan 2016 (available online at <http://www.wbdg.org/pdfs/jbasics_aci_ttp_2016.pdf>)
* Department of Defense Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations (available online at <http://www.wbdg.org/pdfs/ics_handbook.pdf>)
* Defense Information Security Agency
* Federal Information Processing Standard 200 Minimum Security Requirements for Federal Information and Information Systems
* Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
* National Institute of Standards and Technology Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
* National Institute of Standards and Technology Special Publication 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations 2013
* National Institute of Standards and Technology Special Publication 800-82 R2 Guide to Industrial Control Systems (ICS) Security 2015
* National Institute of Standards and Technology Special Publication SP 800-115 Technical Guide to Information Security Testing and Assessment 2008
* Department of Veterans Affairs Mental Health Facilities Design Guide 2010
* Department of Veterans Affairs Office of Information & Technology Design Guide 2011
* Department of Veterans Affairs Telecommunications and Special Telecommunication Design Manual (TDM) 01-2016
* Unified Facility Criteria3-580-01Telecommunications Interior Infrastructure Planning And Design June 2016
* Unified Facility Criteria Design 4-510-01 Military Medical Facilities 2014
* USACE Technical Criteria for the Installation Information Infrastructure Architecture, February 2010
* UFGS 25 10 10, Utility Monitoring And Control System (UMCS) Front End And Integration (available online at www.wbdg.org)
* Government Accounting Office Report 15-6 Federal Facility Cybersecurity 2014
* Building Industry Consulting Service International (BICSI) Telecommunications Distribution Methods Manual (TDMM)
* National Fire Protection Association (NFPA) 101 Life Safety Code 2015
* TIA-1179 Healthcare Facility Telecommunications Cabling 2010
* TIA-942-A Telecommunications Infrastructure Standard For Data Centers 2014
* TIA-569-D Commercial Building Standard For Telecommunications Pathways And Spaces 2015
* TIA-758 Customer-Owned Outside Plant Telecommunications Infrastructure Standard 2012
* TIA-606-B Administration Standard For Commercial Telecommunications Infrastructure 2012
* TIA-568-C.2 Balanced Twisted-Pair Telecommunications Cabling And Components Standard 2009
* TIA-1152 Requirements For Field Test Instruments 2009
* TIA Tsb-155-A Guidelines For The Assessment And Mitigation Of Installed Category 6 Cabling To Support 10gbase-T 2010
* TIA-568-C.4 Broadband Coaxial Cabling And Components Standard 2011
* TIA-604-4-B Focis 4 - Fiber Optic Connector Intermateability Standard, Type Fc And Fc-Apc 2004
* TIA-607-C Telecommunications Grounding (Earthing) And Bonding For Customer Premises 2015
* TIA-568-C.2 Balanced Twisted-Pair Telecommunications Cabling And Components Standard Rev C 2009
* TIA-568-C.3 Optical Fiber Cabling Components Standard Rev C 2008
* TIA-568-C.4 Broadband Coaxial Cabling And Components Standard Rev C 2011
* TIA-568.0-D Generic Telecommunications Cabling For Customer Premises 2015
* TIA-568.1-D Commercial Building Telecommunications Cabling Standard 2015
* TIA-862-B Building Automation Systems Cabling Standard 2016
* UL 60950-1 Information Technology Equipment - Safety - Part 1: General Requirements 2013

1.4 ROLES AND RESPONSIBILITIES

*Role*: Government Stakeholders

*Members*: Service Design Manager, Facilities Engineering Acquisition Department (FEAD), Services Civil Engineering Representative (NAVFAC, AFCEC, USACE, DPW, etc.), Integrated Product Team (IPT).

*Responsibilities*: Review ESTCP CS Installation Contractor submittals, test reports, and Commissioning reports.

*Role*: ESTCP CS Installation Contractor

*Members*: Contractor responsible for the installation or modification of a CS network component. Includes the contractor’s Control Systems Cybersecurity Specialist and Integration Specialist.

*Responsibilities*: Responsible for production and submittal of all project Configuration Items (CI’s), project CI inventories, and design/construction/commissioning documentation associated with the installation or modification of CS systems.

*Role*: ESTCP CS Engineer of Record

*Members*: Project mechanical engineer of record, electrical engineer of record, and control system engineer of record (if applicable)

*Responsibilities*: Responsible for modifying the provided UFGS and ESTCP CS Engineering Manual design templates to meet the requirements of the specific project

*Role*: ESTCP CS Service Agreement Contractor

*Members*: Contractor(s) responsible for the operation and maintenance of the installation’s CS network.

*Responsibilities*: Following configuration management procedures during required system modifications, security patches, and firmware upgrades.

*Role*: ESTCP Information Owner/Steward

*Members*: Installation Chief Information Officer (CIO)

*Responsibilities*: Responsible for maintaining the current baseline of Configuration Items, management of the CI repository, and managing and tracking the security state of information systems.

*Role*: Security Control Assessor (SCA)

*Members*: Installation Chief Information Officer (CIO)

1.5 REQUIRED SUBMITTALS

UFGS 251010 UMCS Front End and Integration – Relevant Submittals:

SD-02 Shop Drawings - UMCS Contractor Design Drawings

SD-02 Shop Drawings - Draft As-Built Drawings

SD-02 Shop Drawings - Final As-Built Drawings

SD-03 Product Data - Product Data Sheets

1.6 APPLICABLE ESTCP TEMPLATES

None

1.7 GLOSSARY (PER UFC 3-580-01 01 Jun 2016 Change 1, 01 Jun 2016)

1.7.1 **ACRONYMS**

**Acronym Term**

10G 10-Gigabit Ethernet

10GPON 10-Gigabit Symmetrical Passive Optical Network

AC Alternating Current

ADN Area Distribution Node

AFCESA Air Force Civil Engineering Support Agency

AFH Army Family Housing

AHJ Authority Having Jurisdiction

ANSI American National Standards Institute

APC Angled Physical Contact

A/V Audio Visual

AWG American Wire Gauge

BATB Base Area Transport Boundary

BEQ Bachelor Enlisted Quarters

BET Building Entrance Terminal

BICSI Building Industry Consulting Service, International, Inc.

BOQ Bachelor Officers Quarters

CATV Community Antenna or Cable Television

CCB Construction Criteria Base

CCTV Closed-Circuit Television

CP Consolidation Point

CTTA Certified TEMPEST Technical Authority

DAA Designated Accreditation Authority

dBmV Decibel (reference to millivolt)

DC Direct Current

DCO Dial/Digital Central Office

DDC Direct Digital Controller

DOIM Directorate of Information Management

DOIM Directorate of Information Management

DoD Department of Defense

DODISS Department of Defense Index of Specifications and Standards

DPW Directorate of Public Works

EES Earth Electrode Subsystem

EF Entrance Facility

EMT Electrical Metallic Tubing

ER Equipment Room

EUB End User Building

FO Fiber Optic

FOCIS Fiber Optic Connector Intermateability Standard

FOPP Fiber Optic Patch Panel

FOUO For Official Use Only

Gbe Gigabit Ethernet

GE Grounding Equalizer

GHz Gigahertz

GPON Gigabit Passive Optical Network

HVAC Heating, Ventilation and Air Conditioning

I3A Installation Information Infrastructure Architecture

ICDS Installation Communications Distribution System(s)

IDF Intermediate Distribution Frame

IMA Information Mission Area

IS Information System

ISP Inside Plant Wiring

ITS Information Transport System

ITU International Telecommunications Union

LAN Local Area Network

LATB Local Area Transport Boundary(s)

LC Lucent Connector

MCEN Marine Corps Enterprise Network

MCN Main Core Node

MDF Main Distribution Frame

MHz Megahertz

MILCON Military Construction

MRI Magnetic Resonance Imaging

MTBF Mean Time Between Failures

MUTOA Multi-User Telecommunication Outlet Assembly

NAVFAC Naval Facilities Engineering Command

NCTAMS Naval Computer and Telecommunications Area Master Station

NEC National Electrical Code

NESC National Electrical Safety Code

NFPA National Fire Protection Association, Inc.

NGEN Next Generation Enterprise Network

NMCI Navy and Marine Corps Intranet

NSI National Security Information

ODN Optical Distribution Network

OLT Optical Line Terminal

ONT Optical Network Terminal

OSP Outside Plant

PDS Protected Distribution System

PET Protected Entrance Terminal (sometimes referred to as BET)

POL Passive Optical LAN

PON Passive Optical Network

POTS Plain Old Telephone Service

RCDD Registered Communications Distribution Designer

RU Rack Unit

SEBQ Senior Enlisted Bachelor Quarters

SFP Small Form Pluggable

SIPRNET Secret Internet Protocol Router Network

SMF Single Mode Fiber

TBB Telecommunications Bonding Backbone

TDMM BICSI Telecommunications Distribution Methods Manual (Latest Edition)

TE Telecommunications Enclosure

TEF Telecommunications Entrance Facility

TGB Telecommunications Grounding Busbar

TIA Telecommunications Industry Association

TMGB Telecommunications Main Grounding Busbar

TR Telecommunications Room

UCR Unified Capabilities Requirements (Latest Edition)

UFC Unified Facilities Criteria

UL Underwriters Laboratory, Inc.

UPC Ultra Physical Contact

USACE United States Army Corps of Engineers

UTP Unshielded Twisted Pair

VTC Video Teleconference

WAO Work Area Outlet

WAP Wireless Access Point

**Terms**

**Intra-Building Backbone** – Connectivity for the voice, video, and data networks between the entrance facility or equipment room, to a telecommunications room.

**Inter-Building Backbone** - Connectivity between buildings, also referred to as part of Outside Plant (OSP) and will be defined in UFC 3-580-02

1.8 REQUIREMENTS FOR SUBJECT MATTER EXPERTS The CS Telecommunications and Network shall be designed and engineered by qualified Control System Cybersecurity, Information and Communication Technology, and System Integration specialists complying with the requirements listed below.

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

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

1.8.3 System Integration Specialist: The System Integration specialist shall have a minimum of five years’ experience in BAS control system network and MEP design and shall maintain current certification as a Certified System Integrator (CSI) for the products they are integrating (Tridium, Johnson Controls, Wonderware, Schneider, Schweitzer Engineering Laboratories, Rockwell, etc.) and/or be Control System Integrators Association (CISA) Certified. The System Integrator specialist must have demonstrated knowledge and experience applying IT and OT security strategies such as the application of the NIST security controls, BAS design and installation, project management, quality assurance and commissioning. The résumé of the specialist must be submitted to the ESTCP Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

1.9 JOINT INFORMATION ENVIRONMENTThe JIE vision is “a robust and resilient enterprise that delivers faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location.”

“JIE is comprised of IT capabilities, operations and defense of those capabilities, and overall governance. The overall vision for the future DoD computing environment is the ability to deliver a standardized, agile, and ubiquitous set of computing capabilities available to all authorized users as part of a services-based Information Enterprise (IE). Computing and storage services will be delivered through a set of consolidated and interconnected Core Data Centers, Installation Processing Nodes, Special Purpose Processing Nodes, Tactical/Mobile Processing Nodes, and end-user devices that deliver cloud-based, on demand services while also continuing to support existing/legacy services and applications. The high-level goals are:

* Significantly reduce the number of DoD data centers in support of the Federal Data Center Consolidation Initiative and the DoD IT Enterprise Strategy & Roadmap.
* Reduce excess hardware infrastructure in data centers by adopting virtualization technology and reducing the number of instances of multiple applications
* Reduce software redundancy and rationalize the software infrastructure through the implementation of standardized software platforms (including cloud platforms) that are continuously monitored and respond to emerging threats
* Make common applications and services (e.g., email, collaboration) available to all DoD users that are secure, highly scalable, and can be rapidly configured and deployed
* Ability to provide on-demand capacity and self-provisioned services that can scale, as required, to user needs
* A federation of “franchised” CDCs, IPNs, SPPNs, and TPNs with robust interconnectivity and global accessibility delivering services to all authorized users in all locations
* Authorized users can access needed information from anywhere from any authorized device. Data is visible, accessible and understandable based on security privileges
* Improved security posture and agility (ability to recover from unplanned events) of the computing infrastructure
* Ability to more readily adopt emerging commercial technologies, platforms and services

1.9.1 Installation Processing Nodes A fixed DoD data center serving a single DoD installation with local services that cannot be (technically or economically) provided from a CDC. There will only be one IPN per DoD installation but each IPN may have multiple enclaves to accommodate unique installation needs (e.g., Joint Bases).

**NOTE:** The DoDIN Demarc to the installation/site is a IPN in the JIE.

1.9.2 Special Purpose Processing Nodes A fixed data center or data servers in a fixed facility supporting special purpose functions that cannot or should not be supported by Core DCs or IPNs due to its association with mission specific infrastructure or equipment (e.g., Meteorology, Medical, Modeling & Simulation, Test Ranges, Classrooms, RDT&E, etc.).

**NOTE:** The PE Operations Center is a SPPN in the JIE.

1.9.3 Tactical Processing Nodes Tactical/Mobile Processing Nodes of the target state will provide services very similar to those of fixed Core DCs but are optimized for the tactical environment or deployable computing needs. TPNs will connect to the JIE network whether in garrison or deployed, but may do so in different ways (e.g., terrestrial fiber vs. satellite connectivity).

**NOTE:** Tactical Operational Energy Assets (Generators, Microgrids, Vehicles, Energy Storage Flywheels/ Fuel Cells/Batteries) can now be incorporated into the fixed ashore installation energy production services; a building UMCS could have a direct connection plugin for a Tactical Asset to provide backup or primary power. These would be a TPN in the JIE.

1.10 PUBLIC SAFETY NETWORK (PSNET)If the ESTCP Project will be on a Navy installation, the Navy master architecture is PSNet which provides the national, regional, and installation level backbone transport and is owned and managed by NAVFAC.

1.11 NIPRNET AND COMMERICAL CARRIER NETWORKSOn Joint base, off-site commercial lease space, or VA facilities, the transport backbone could be the NIPRNET or commercial carriers. The PE Operations Center (OC) Inherits all of the security controls provided by NIPRNET or the commercial carrier. The OC is responsible for the CS network and supporting LANS.

1.12 OPERATIONS CENTER (OC)The is the central point for all monitoring, controlling, programming, and service for all CS systems. The OC and CS HMI operators console provides the Continuous Monitoring capability, and is divided into the Production System, and the Test and Development Environment. All patches, requests for configuration changes, and verification of SCAP/ACAS scans are completed in the TDE before deploying to the Production system.

CHAPTER 2. OPERATIONAL TECHNOLOGIES, WAN, LAN, WIRELESS

2.1 OPERATIONAL TECHNOLOGIES (OT)Throughout industry, and informally within DoD, the term Operational Technology (OT) is used to differentiate control systems from traditional information systems (IS). Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. (Gartner OT <http://www.gartner.com/itglossary/operational-technology-ot/>). Other emerging terms related to control systems include Hybrid/Converged Systems, Cyber Physical Systems, the Internet of Things, and the Industrial Internet of Things.

DoD and the Department of Veterans Affairs provide healthcare services through a combination of on-site installation/campus and off-site clinics and Medical Office Buildings (MOB’s). The DoD and VA are also building joint use medical facilities. The connectivity between the facilities typically uses commercial telecommunications carriers (AT&T, Verizon, Sprint, etc.)

2.2 WIDE AREA NETWORKS (WAN)DISA provides the WAN backbone circuits for the Army and Air Force. PSNet is the WAN used across the Navy for national, regional and installation backbone transport. For joint use, off-site commercial lease space, and VA facilities, NIPRNET or commercial carriers provide the WAN. In general, the ESTCP Project Team/System Integrator will only need to contact and coordinate with the PE for connection from the LAN to the appropriate WAN.

2.3 LOCAL AREA NETWORKS (LAN)The local engineering function is responsible for CS LANs and other associated stand-alone networks. For ESTCP projects that require use of the DoDIN, the Project Team/System Integrator should ensure that the CS cross-domain connections are secured; most CS are cross-connected to other facility or building control systems such as the Fire Alarm, Fire Suppression, and HVAC fire dampers; Stairwell and Elevator safe haven and Smoke Purge systems; Patient Comfort; and Weather systems, etc..

2.4 WIRELESS NETWORKSWithin the DoD and Navy PSNet master architecture, wireless networks and Land Mobile Radios are part of the approved backbone transport. Industry is also rapidly adopting wireless technologies to include 802.XX, Bluetooth, Zigbee, and HART. All wireless networks used within a CS must be FIPS 140-2 compliant.

2.5 PORTS, PROCTOCOLS AND SERVICES (PPS)DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), establishes PPSM support requirements for configuration management and continuous monitoring. This includes discovery and analysis of PPS to support near real time command and control of the DOD Information Network (DODIN) and Joint Information Environment (JIE), and coordination with the local network and communications community to ensure they add control system PPS. Examples of CS PPS include:

* Modbus: Master/Slave – Port 502
* BACnet: Master/Slave – Port 47808
* LonWorks/LonTalk: Peer to Peer – Ports 1628, 1629
* DNP3: Master/Slave – Port 20000
* Zigbee: Peer to Peer 2.4 GHz
* Bluetooth: Master/Slave 2.4 GHz

2.6 TELECOMMUNICATIONS AND NETWORK DESIGN REQUIREMENTS

Refer to UFC 3-580-01 01 Jun 2016 Change 1, 01 Jun 2016 and the VA Telecommunications Design Manual 2016 for Telecommunications and Network Design requirements.

CHAPTER 3. PASSIVE OPTICAL NETWORKS

3.1 GIGABIT PASSIVE NETWORK (GPON)For ESTCP projects that will become part of the larger DoDIN and next generation networks, the project must demonstrate the capability to integrate into a gigabit passive optical network. This chapter describes the GPON and general operational charateristics.

A passive optical network (PON) is a point-to-multipoint network architecture in which unpowered optical splitters are used to enable a single optical fiber strand to serve multiple end-points. Passive optical LANs are an implementation of PON technology for the enterprise LAN (e.g., large Layer 2 Ethernet networks). The solution reduces physical cabling infrastructure, minimizes the telecommunications space requirements through the use of passive optical splitters, and reduces the typical energy requirements to support traditional Ethernet deployments.

The maximum supported distance of a GPON varies from -20 km (12.5 mi) to -60 km (37 mi), depending primarily upon the loss budget of the PON type. The maximum channel attenuations for the common types of PON technologies are listed in the table below:

|  |  |  |
| --- | --- | --- |
| PON Standard | Max Channel Attenuation | Max Support Distance |
| ITU G.984 GPON (B+ Optics) | 28 dB | 12.5 mi |
| ITU G.984 GPON (C+ Optics) | 32 dB | 37 mi |
| ITU G.987 10GPON | 31 dB | 25 mi |

3.2 SPACE REQUIREMENTSPON typically requires no active equipment in the telecommunications facilities where traditional access layer devices are typically located. The mechanical and electrical systems needed to support a PON deployment must be coordinated closely with the system equipment manufacturer during the planning phases of projects to determine the overall HVAC and power requirements required to support the IT transport system.

3.3 PATHWAY REQUIREMENTSThe CS requires an alarmed-carrier pathway system capable of real-time detection of physical breaches. The system must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation. Air-jetted, micro-duct pathways require much less area, maximizing the fiber density capabilities and setting the stage for fiber-on-demand, allowing a defrayed cost scenario for maximum network implementation and utilization. The high-density pathway bundles make it cost effective to have extremely high fiber density capabilities well beyond the current conventional fill capacities.

The pathways must be air-jetted providing a complete, flexible, re-usable pathway for campus, building and floor distribution of telecommunications services throughout the complex. Flexibility is required to accommodate the need for maintenance, movement, changes and expansion as easy as possible. The layout and capacity of the pathway system shall be thoroughly documented in the site and floor plans.

3.4 ALARMING CARRIER REQUIREMENTSAlarm points are required to protect and monitor the entire pathway distribution. The alarm points will be located in the controlled spaces. The alarm point devices shall be provided with the latest firmware/software version and any licenses required.

3.5 ALARM MONITORING SYSTEM The application monitoring software must provide alarm monitoring, performance monitoring, Access panels, Zone Distribution boxes and Maintenance holes on the CS networks. The System must be equipped with pro-active application monitoring and management tools to distribute notifications of alert across a variety of protocols and endpoints. The alarm monitoring software and hardware must be listed on the DISA Unified Capabilities Approved Products List (UC APL) approved for use on DoD Information Networks (DoDIN). The Installing Activity shall purchase and install all components of the system with the latest approved hardware, firmware and software versions certified for net-worthiness on DoDIN to provide a fully functional system.



**Figure 5.2 – PON Campus Deployment Example**



**Figure 5.3 – End to End PON Schema**

3.6 OLT Optical Line Terminals (OLTs) provided for support of each enclave, specific technical specifications for the OLT shall support:

1. Class B+ optics (28 dB optical loss budget) as defined in the ITU standards.
2. Field replaceable GPON SFP modules to minimize downtime.
3. Redundant OLT Processor.
4. Redundant OLT Processor and Timing modules.
5. A fully redundant backplane for all communications from the switching units to the GPON cards with a minimum of 640Gbps backplane with current cards, and capability for a 2.5Tbps overall redundant backplane.
6. Layer-2 bridging functionality.
7. Up to 40 Gigabit aggregate of uplink capacity composed of four (4) 10 Gigabit Ethernet interfaces to facilitate high bandwidth ether-channels for uplink for larger chassis based platforms supporting greater than 512 ONTs.
8. Concurrent use of 10 Gigabit and 1 Gigabit Ethernet uplinks.
9. Full Link Aggregation configuration of uplink interfaces.
10. Rapid Spanning Tree Protocol (RSTP) for redundancy on 1G and 10G network uplinks
11. Multiple Spanning Tree Protocol (MSTP) for redundancy on 1G and 10G network uplinks
12. Ethernet Link Aggregation Group (LAG), Rapid Spanning Tree Protocol (RSTP), Virtual Router Redundancy Protocol (VRRP) for Dual Homing, and Link Aggregation Control Protocol (LACP).
13. Multiple Spanning Tree Protocol (MSTP) for multiple concurrent Dual Homing paths from the OLT.
14. Multiple VLAN per end user Ethernet interface including VLAN translation, trunking, and termination.
15. Concurrent IPv4 and IPv6 with IEEE 802.1q Priority Tag and IEEE 802.1p Q-Tag.
16. VLAN Group provisioning (multiple end-user interface/service into a common VLAN Group) and provisioning of Ethernet Bridging and Private VLAN on a per port basis.
17. Quality of Service (QoS) for each service VLAN using 802.1p and DSCP markings for both upstream and downstream traffic through a combination of ingress policing, queue management, scheduling and shaping at the user service level traffic prioritization support combination of Round Robin (RR), and Strict Priority (SP) queuing. Multiple QoS on each end user Ethernet interface.
18. RSTP loop detection and redundancy on the ONT end user network ports.
19. ITU G.984.x compliant “Type-B PON Protection” schemas, allowing for a 2-input PON splitter to be dual homed to geographically diverse OLT locations without requiring the ONTs to be re-provisioned or any services lost. PON Protection shall provide capability for sub 5-second of system restoration.
20. Layer2 (Ethernet), Layer 3 (IP), Layer 4 (TCP/UDP) Access Control Lists (ACL).
21. Multiple ACL filter profiles attached to each end user interface and service.
22. Sticky MAC address for port security function, 802.1x authentication for port control.
23. Network Access Control (NAC) integration for automatic ONT user port configuration based upon Active Directory/LDAP, 802.1x or CAC/smart card credentials.
24. Link Layer Data Protocol (LLDP) for automatic provisioning of VoIP phones, E911, and MED/Inventory services as well as power negotiations.
25. RADIUS interface on OLT.
26. SYSLOG integration and monitoring.
27. ONT Range Locking to prohibit tampering with the ONTs.
28. POL Threshold Crossing Alarms to provide full PON utilization statistics and alarming based on certain percent utilization of a PON link and SNMP alarm notification.

3.7 ONT COPPER ETHERNET INTERFACESProvide ONTs equipped with a minimum of four 10/100/1000 RJ-45 Ethernet interfaces conforming to IEEE 802.3 standards. A quantity of four 1000 Base-T interfaces is required. 10/100 Base-T interfaces and those not supporting PoE or PoE+ are not permissible.

3.8 ONT COPPER ANALOG INTERFACESONTs equipped with analog POTS provide various quantities (2, 4, or 24 depending on the model) of RJ-11 or RJ-21 telephone jacks for connection of analog devices (telephones, Faxes, modems, etc.). These interfaces may provide 600 or 900 Ohm terminations and adhere to typical analog voice wire length specifications.

3.9 ONT COPPER COAXIAL INTERFACESONTs equipped with RF video interfaces can provide broadcast television service or any RF frequency up to 1 GHz. The coaxial outlet/connector integrated within the ONT is a standard, male 75-Ohm “F” type connector. The designer must coordinate with the cable service provider where franchise agreements are in place and additional head end components such as an RF combiner, laser modulator and fiber amplifier (EDFA) will be required for POL distribution of RF services.

3.10 ONT REMOTE POWERINGRemote powering of the ONT must be achieved through the combination of singlemode optical fiber and balanced twisted-pair cabling. An alternative to using the composite cable method is to run a parallel balanced twisted-pair cabling channel alongside the singlemode optical fiber cabling channel. The power is introduced to the balanced twisted-pair cabling in telecommunications spaces. The ONTs require direct current (dc) power input, transitioning from ac to dc at a consolidated location (zone box), the power supply must have a primary and backup power source.

3.11 ONT REMOTE POWERINGONTs shall be provided with integrated lithium ion batteries that can allow for a short runtime (e.g., 5-30 minutes) based on the services being provided and the actual power draw of any PoE devices at the end-point device.

3.12 CROSS-DOMAIN ENTERPRISEThe CS may be part of a Cross-Domain and interconnect with other Facility-Related Control Systems. The other CS can be segmented but still have secure data communication with the CS.



**Figure 5.4 – Cross-Domain Networks and Connections**

CHAPTER 4. COORDINATION WITH TELECOMMUNICATION AND OTHER SYSTEMS

The CS design, construction, systems integrator, and operations teams will also need to collaborate and coordinate closely with the CIO, CYBERCOM, and Mission Assurance to ensure control systems have end-to-end cybersecurity across the domain (both internet connected and standalone systems) and the DoD Information Network (DODIN). As stated in DoDI 8530:

“The DoDIN includes DoD information (IT) (e.g., DoD-owned or DoD-controlled information systems (ISs), platform information technology (PIT) systems, IT products and services) as defined in DoDI 8500.01 (Reference (h)) and control systems and industrial control systems (ICSs) as defined in National Institute (NIST) Special Publication (SP) 800-82 (Reference (i)) that are owned or operated by or on behalf of DoD Components.”

4.1 NETWORK SECURITY OPERATIONS CENTER (NOSC) The term NOSC will be used generically in this document for the various types and names used for network operations and security centers organized by joint or DoD Components to direct and manage operations and cybersecurity activities to protect the are owned or operated by or on behalf of DoD Components.”

4.2 CYBER RANGESare incorporating control systems into the matrix of training and exercises as a combination of both physical and virtual environments.

4.3 MISSION ASSURANCEconducts on-site assessments of the installation control systems using the Joint Mission Assurance Benchmarks.

4.4 USCYBERCOMprovides both defensive and offensive response capabilities.

4.5 DEPARTMENT OF VETERANS AFFAIRSand DoD operate joint use facilities and share a number of common facilities services, in particular the CS. Coordinate new and major modernization projects with the VA Construction and Facilities Management (CFM) Office and the local VISN. For small or minor projects, coordinate with the VISN.