cloudastructure

Best Practices

For Successful Installs

June 8, 2022
V1.1

INTRODUCTION

This best practices guide has been developed through experience of cabling and network practices common in industry today. This guidance does not cover specialized installation scenarios, such as elevators. Cloudastructure, its affiliates, and partners recommend these best practices. However, nothing in this guide is intended to supersede NEC and local electrical codes or NFA, local fire safety regulations, or any other state, local or jurisdictional regulations. Those codes always supersede these best practices and uncategorically must be followed. This guide is intended to be supplemental and instructional only.

For help by phone, please contact: +1-650-644-4160 and ask for Technical Support

TABLE OF CONTENTS

AUDIENCE

This document is intended for third-party installers, resellers, and customers deploying Cloudastructure systems. It explains the industry best practices that lead to successful installations and robust, secure video surveillance, voice, and access control infrastructure.

GENERAL GUIDANCE FOR ALL INSTALLERS

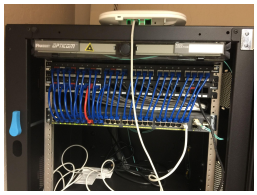
INSTALLERS ARE EXPECTED TO READ, UNDERSTAND AND ABIDE BY THE SPECIFICATIONS OF THIS DOCUMENT FOR THE SCOPE OF THE WORK THAT IS BEING REQUIRED BY THE CLOUDASTRUCTURE (CSI) CUSTOMER.

INSTALLERS ARE RESPONSIBLE TO PROVIDE ALL PATHWAYS (CONDUITS, CABLE BASKET TRAYS, WALL OR FLOOR PENETRATIONS, GROUNDING, AND BONDING) TO ENABLE INSTALLERS TO INSTALL CABLING FOR IP CAMERAS, AND ANY OTHER RELATED CABLING WITHIN THE SCOPE OF THE CONSTRUCTION PROJECT. CSI CAN REVIEW SPECS AND PLANS WITH LOW VOLTAGE INSTALLERS AND CUSTOMERS.

PART 1: GENERAL

1.0 PROJECT SIZING

Not all best practices apply to projects of all sizes. In particular, the head-end electronics space may vary widely based on the number of endpoint devices:



- A small installation of just a few cameras, such as may need only a 6U wall-mounted enclosure to contain RJ45 couplers, UPS, switch, and CVR, located in a shared office space.

- A mid-sized installation supporting dozens of cameras and possibly multiple applications, such as access control, intercom, and WiFI, may warrant a larger wall rack or a free-standing two-post relay rack in a dedicated closet, and hard-wired RJ45 patch panels.

- The largest installations will require multiple racks across several MDFs and IDFs, with a leaf-and-spine network topology, using top-of-rack switches, and possibly a fiber optic backbone.

Small installations generally don't require enterprise-grade structured cabling, although that is still considered a best practice. When structured cabling is not used, a blank keystone panel can be employed in place of a hard-wired RJ45 patch panel, with keystone couplers that interface RJ45-plug distribution cables to Rj45-plug patch cables. Fully-enclosed racks are still recommended in order to protect equipment from tampering and enable clean cable identification and organization.

1.1 EXISTING NETWORK SERVICES REQUIREMENTS

Because CSI systems are typically deployed in existing networking infrastructure, they're designed to work with equipment and services that are already in place. These services are:

1. Firewall or Network Gateway. Every Internet-connected network has at least one firewall device, which serves as a gateway to the public Internet. Most firewalls also serve a security function, providing services such as intrusion detection and prevention, malware filtering, and content control. CSI is a cloud-based system, and thus requires Internet access. The CSI Cloud Video Recorder (CVR) assumes that a firewall is already installed and can be detected automatically (using DHCP, see below).

2. Managed Switches. Any security-related network components should support configuration management, either via a Web interface, command line, or Software Defined Network (SDN) controller. Fortunately managed switches are standard in the industry and need not be expensive. The risks of using unmanaged switches include broadcast storms and bridge loops that can disable the entire network. Managed switches also have built-in diagnostic tools that greatly speed network troubleshooting and cybersecurity forensics.

   At a minimum, switches should support VLAN segmentation, Simple Network Management Protocol (SNMP) statistics reporting and Rapid Spanning Tree Protocol (RSTP).

3. DHCP. Dynamic Host Configuration Protocol, or DHCP, automatically configures network endpoints such as IP cameras with an IP address, and gateway address, subnet mask. Through the use of options, it can also tell endpoints the IP address of a local time server, time zone offset, VoIP gateway, and other application-specific data items.

   Unless special arrangements are made, CSI requires an active DHCP server delivering at least IP address, gateway address, and subnet mask for the CVR to operate. Cameras can either run off the same DHCP services or be statically assigned.

4. DNS. Domain Name System, or DNS, translates domain names into private and public IP addresses so that endpoints can establish communications with a network service by name. CSI requires an active DNS service, which may be local or provided over the Internet, in order for cloud functions to operate.

5. NTP. Network Time Protocol, or NTP, is a widely available service that delivers the current date and time, and nothing else. Despite its simple functionality, NTP is critical to nearly every network element, as an accurate time-of-day and date clock is necessary for encrypted Internet communications. In a security application, timestamps are also essential for accurately logging events such as motion detection or door accesses, and for correlating events from multiple devices to determine their sequence.

   Some enterprise networks have one or more local NTP servers that get the time of day continuously from the Global Positioning System (GPS) satellite network. If a local time source is unavailable, Internet-based time sources can be used, and are published from a rotating pool of publicly available servers at the domain name pool.NTP.org. For public NTP servers geographically located in a specific country, you can add a country-code prefix, e.g., US.pool.ntp.org or FR.pool.ntp.org.

6. For security applications, there is some risk in using Internet-based public NTP servers. For example, NTP is vulnerable to Man-in-the-Middle (MitM) attacks, which allow unauthorized users to alter traffic sent between clients and servers. Given the relatively small number of public NTP servers, this risk is not insignificant.

   As a result, many smaller organizations are now installing their own dedicated GPS-based NTP servers, which can be purchased for under $400. Example:

   https://timemachinescorp.com/product/gps-time-server-tm1000a/

1.2 SCOPE

A. The installer generally furnishes and installs all materials for a complete, functional data and voice communications system in accordance with system design provided by CSI.

B. CSI supports any qualified cable (twisted-pair Cat6 copper and/or Single Mode optical fiber), innerduct, interconnect-patching equipment connectors, patch cables, and telecommunications outlets as well as Camera, Access Control, and IP intercom stations. Decisions on media selection should be based on availability, compliance with standards, and price.

C. In addition to material and equipment, installers provide labor (either directly or via an approved subcontractor) and any incidental material required for installation. All copper station cables should be terminated on patch panels at distribution frames and on data communication outlets at the station end, using structured cabling conventions: Ethernet jacks at all terminations, employing patch cables for all interconnects. Some very small installations will forgo this structured cabling in order to reduce costs. If the decision to go without structured cabling is made, then the Customer should be informed that this could present the following risks:
   1. Limits on potential growth
   2. The ease by which the cabling becomes unsightly and difficult to troubleshoot
   3. Lack of ability to support meaningful growth in the number of devices (cameras, doors, AP, or other IoT endpoints).

D. The installer is also responsible to patch all connections in patch panels and station locations to yield a functional, testable system.

E. Upon completion of infrastructure installation, installers should test all copper and fiber links and record the test results, as specified in section 3.7, *before* connecting any active equipment, in order to minimize the chance of damage to PoE interfaces due to miswiring.

F. The work performed under this specification should be of good quality and performed in a workmanlike manner. In this context "good quality" means the work meets industry technical standards and quality of appearance. Work that is not performed correctly should be redone so it meets both aesthetics and performance requirements. Often, aesthetics make troubleshooting easier should something need remediation.

G. The installer may deploy cable pathways (conduit, J-hooks, raceways, etc.) required to meet electrical codes and adequately service CSI's design. In general, J-hooks are most effective, conduits are most secure, and raceways are a good compromise.

1.3 RELATED DOCUMENTS

A. Regulatory References

The following industry standards are the basis for the structured cabling conventions described in this document.

1. American National Standards Institute (ANSI) / Telecommunications Industry Association (TIA)
    - ANSI/TIA-4966 – Telecommunications infrastructure standards for educational facilities.
    - ANSI/TIA-568.0-D – Generic Telecommunications Cabling for Customer Premises or most recent revision at the time of installation
    - ANSI/TIA-568.1-D – Commercial Building Telecommunications Cabling Standards or most recent revision at the time of installation.
    - ANSI/TIA-568-C.2 – Balanced Twisted Pair Communications and Components Standards or most recent revision at the time of installation.
    - ANSI/TIA-568.3-D – Fiber Optic Cable System Components Standards or most recent revision at the time of installation.
    - TIA-569-D – Commercial Building Standard for Telecom Pathways and Spaces or most recent revision at the time of installation.
    - ANSI/TIA-606-C – Administration Standard for the Telecommunications Infrastructure of Commercial Buildings or most recent revision at the time of installation.
    - ANSI-J-STD-607-C – Commercial Building Grounding/Bonding Requirements or most recent revision at the time of installation.
    - ANSI/TIA 1152 – Testing of Copper Links.

2. National Electric Codes
    - National Electrical Safety Code (NESC) (IEEE C 2)
    - National Electrical Code (NEC) (NFPA 70)
      Reference this page for NEC variations by state:
      https://www.nfpa.org/NEC/NEC-adoption-and-use/NEC-adoption-maps

3. ISO/IEC
    - ISO 11801 - Generic Cabling for Customer Premises.

4. OSHA Standards and Regulations – All Applicable.

5. Local Codes and Standards – All Applicable.

If there is a conflict between installation standards, then the more stringent requirement shall apply. All documents listed are believed to be the most current releases of the documents. The installer has the responsibility to determine and adhere to the most recent release when developing the proposal for installation and regulatory jurisdiction.

This document does not replace any building code or regulation, either partially or wholly. The installer should be aware of local codes that may impact this project.

1.4 QUALITY ASSURANCE

The following general quality assurance guidelines should be followed unless waived by written authorization:

1. The installer must possess any valid low voltage license required for the Customer jurisdiction. If the installer has RCDD (Registered Communications Distribution Designer) on staff, that designer should approve all designs and change orders.

2. The installer should be completely familiar with the TIA standards for telecommunications raceway/pathway infrastructure systems and with the telecommunications design practices as defined in the BICSI Telecommunications Distribution Methods Manual.

3. The installer should have worked satisfactorily for a minimum of five years on systems of this type and size within a fifty-mile radius of the center of the Customer location.

4. WARRANTY Installer shall provide a complete system warranty to guarantee end-to-end high-performance cabling systems that meet application requirements. The manufacturer of the telecommunications equipment, devices, and cable should warranty the entire telecommunications structured cable system to be in compliance with applicable codes and standards and to be free from defects in materials and workmanship. The warranty shall apply to all passive structured cabling system components and shall cover the failure of the system to support applications in accordance with the performance levels stipulated in the referenced ANSI/TIA standards.

5. Upon successful completion of the installation and subsequent inspection by the CSI's Customer ("Customer") project manager, the manufacturer of the telecommunications equipment devices and cable shall furnish a numbered registration certificate attesting to cable test results to CSI and Customer.

6. A TIA or ANSI-certified low voltage installer should complete all work described herein. Any subcontractors utilized should be approved in advance in the contract documents. All products specified herein should be installed by the installer(s) represented in the proposal. The installer should have completed standards-based product and installation training. A copy of the Authorized Supplier Installer Registration should be submitted in the proposal.

1.5 GOVERNING CODES AND CONFLICTS

If the requirements of CSI's design document exceed those of the governing codes and regulations, then the requirements of CSI's design document set the minimum requirements. However, nothing in CSI's design document shall be construed to permit work not conforming to all governing codes and regulations.

1.6 DESIGN DOCUMENT

Prior to installation of any equipment, the Customer shall provide the installer with Customer's Design Document providing the system installation details, which may include a Bill of Materials (BOM) with model numbers, quantities, catalog information, cut sheets, and equipment specification sheets, floor plans with equipment and wire locations, and station locations.

The Design Document will not repeat the general best practices described in this document. It incorporates them automatically by reference. Prior to installation, any product substitutions should be reviewed and verified to functionally meet the specifications provided in the Design Document.

1.7 PROJECT RECORD DRAWINGS

As-built drawings are the final set of drawings produced at the completion of the installation project. They include all the changes that have been made to the original Design Document, including notes, modifications, and any other information that the installer decides should be included. The drawings should be digitally rendered. As-Built drawings should be submitted to the Customer and operator, in digital format and should include:

1. Connectors, nodes, telecom rooms (MDF's/IDF's), and backbone (riser) cable runs.
2. Cross-connect schedules include terminations, main cross-connects, intermediate cross-connects, and horizontal cross-connects.
3. Labeling and administration documentation.
4. Optical fiber power meter/light source test results.
5. Copper certification test results on CD with appropriate viewing software.
6. Warranty documents for equipment.

PART 2: PRODUCTS

2.1 GENERAL

A. All products should be new and brought to the job site in the original manufacturer's packaging. Photographs of external labeling showing serial, purchase order, or invoice numbers should be retained as part of the job record. All received products should be tallied on a receiving inventory record in order to detect and mitigate loss.

B. Electrical components should bear the Underwriter's Laboratories label. All communications cables should bear the manufacturer's label in accordance with NEC 800 based on flammability testing as follows:

1. Category-6 CMR Riser-rated communication cable.
2. Category-6 CMP Plenum-rated communications cable.
3. Category-6 RJ45 patch cables.
4. OM-3 muilti-mode (aqua) or single-mode (yellow) Plenum-rated Optical Fiber Cable.

2.2 HORIZONTAL DISTRIBUTION SUB-SYSTEM

A. Station Outlets

Station outlets should be located near the location of the active equipment they serve. Where possible, station outlets should be hidden from view, using access or ceiling panels for maintenance access. The following general best practices should also be followed:

1. Use Category-6 1-, 2-, 4-, 6-, or 8-port surface mount or flush-mount boxes or patch panels for station terminations of solid-copper riser cables. Boxes should be secured to the nearest surface within a short distance of the equipment to be interconnected.

2. Use Category-6 stranded-copper patch cables to interconnect station outlets and active equipment. Take care to route cables in an aesthetic manner, employing a surface-mount raceway or cable loom where required.

3. Outdoor locations must be weatherproof, enclosing station outlets in sealed junction boxes and routing outside-plant-grade patch cables through weatherproof grommets.

4. Outdoor active devices, such as cameras, access points, and door readers, must also be weatherproof, rated to the external environment based on international standard EN 60529 Ingress Protection (IP) ratings of the form IPxy, where x specifies dust protection and y specifies liquid protection, as follows:

0 No dust protection.
1 Protected against solid objects over 50mm, e.g. accidental touch by hands.
2 Protected against solid objects over 12mm, e.g. fingers.
3 Protected against solid objects over 2.5mm, e.g. tools & wires.
4 Protected against solid objects over 1mm, e.g. wires & nails.
5 Protected against dust-limited ingress, no harmful deposits.
6 Totally protected against dust.

0 No liquid protection.
1 Protected against vertically falling drops of water, e.g. condensation.
2 Protected against direct sprays of water up to 15 degrees from the vertical.
3 Protected against direct sprays of water up to 60 degrees from the vertical.
4 Protected against water splashed from all directions, limited ingress permitted.
5 Protected against low-pressure jets of water from all directions, limited ingress permitted.
6 Protected against strong jets of water, e.g. on ships deck, limited ingress permitted.

B. IP Intercom, Surveillance Camera, and Access Controls

Cabling should be designed to cover strategic locations and sensitive areas of the Customer for comprehensive surveillance and monitoring. All cables should be pulled by the low voltage installer. All Category-6 copper point-to-point runs should be home run to the nearest IT Network closet as indicated in CSI's Design Document, not exceeding 90 meters for riser cables, allowing for 10 meters of patch cables to comply with the 100-meter total distance limitation. In plenum spaces, plenum cables must be used in accordance with local fire codes and the applicable NEC governance.

1. Intercom Cabling

a. For single-unit intercoms, a single Ethernet drop provides both power and VoIP signaling. The intercom unit should be flush mounted where feasible, otherwise securely surface mounted. The Category-6 cable should enter the back of the unit, invisible to the user.

b. For split-unit intercoms, a single Ethernet drop provides both power and VoIP signaling to the main control unit, with a separate low voltage cable (typically 18-gauge stranded copper) connecting to the microphone and speaker assemblies. The intercom unit should be mounted out of sight where feasible, otherwise securely surface mounted. The Category-6 cable should enter the back of the unit, invisible to the user. Microphone and speaker assemblies should be flush mounted where feasible, otherwise securely surface mounted.

c. Outdoor intercoms must be weatherproof for the anticipated environment, following the Ingress Protection standard cited earlier. All connections must be enclosed and protected from environmental forces.

2. Surveillance Camera Cabling

a. For surface-mounted cameras, a single Ethernet drop provides both power and video signaling. The camera should be attached directly to a wall or ceiling surface, with cabling entering the back of the unit, invisible to the user, and secured from tampering.

b. For pole- or pendant-mounted cameras, a single Ethernet drop should be routed through the pole or pendant where feasible, so that wiring is invisible to the user and secured from tampering.

c. Outdoor cameras must be weatherproof for the anticipated environment, following the Ingress Protection standard cited earlier. All connections must be enclosed and protected from environmental forces.

3. Access Control Cabling

a. For surface-mounted access readers, a single Ethernet drop provides both power and data signaling. The access reader should be attached directly to a wall or ceiling surface, with cabling entering the back of the unit, invisible to the user, and secured from tampering.

b. For pole- or podium-mounted access readers, a single Ethernet drop should be routed through the pole or podium where feasible, so that wiring is invisible to the user and secured from tampering.

c. For door-colocated controllers, a single Ethernet drop provides both power and data signaling to the door control unit, with separate low voltage cable (typically shielded stranded copper) connecting to the access reader, door position switch, request-to-exit device, and door strike units. The door controller should be mounted out of sight where feasible, on the protected side of the door, otherwise securely surface mounted. The Category-6 cable should enter the back of the unit, invisible to the user. All-access reader, door position switch, request-to-exit device, and door strike cables must be securely routed, either within walls or door frames, conduit, or armored surface-mount raceway.

d. No cabling can be accessible from the secure side of the door..

e. Outdoor access readers must be weatherproof for the anticipated environment, following the Ingress Protection standard cited earlier. All connections must be enclosed and protected from environmental forces.

C. Miscellaneous Station Outlets

These may include, but not be limited to console and server stations, fire alarm emergency dialers, fire alarm panels, elevators (e.g., emergency phones and elevator car video surveillance), environmental controls, occupancy sensors, low-voltage lighting, and premise alarm systems. Applicable standards for some or all of these locations may be under multiple regulatory jurisdictions, so the installer should be familiar with any governance requirements for these outlets.

D. Horizontal Station Cabling

Horizontal station cable should be Category 6 unshielded four-pair copper cable (not copper-clad aluminum, often labeled CCA), 23AWG UTP, UL/NEC CMR, or CMP, non-plenum or plenum rated with a PVC jacket as required for the application. All cables should conform to the requirements for communications circuits defined by the National Electrical Code Article 800. Any pathways on the ground level, in or under the slab, or any other potentially wet locations should use the appropriate OSP cable.

2.3 HORIZONTAL CROSS-CONNECT TERMINATION HARDWARE

A. Horizontal Cross-Connections

1. In larger network deployments, all four-pair Category 6 cabling should be terminated with Category–6 patch panels and placed into rack-mount cabinets, either free-standing or wall-mount. Typical designs will call for one station cable per outlet, plus 25% empty ports available for future growth within each rack. Install port blanks on any ports not used within the patch panels.

2. Each 1U of patch panel space should be provided with 1U of horizontal cable management, either above or below the patch panel, but located consistently within all cabinets.

3. Where feasible, cabinets should include an allowance for vertical cable management raceways, preferably on both sides of the cabinet. Note that many standard 19” rail cabinets do not provide this allowance in their standard models. For small cabinets (e.g. 12U and below), this practice can be waived.

4. The horizontal cross-connects will employ stranded-copper RJ45 patch cables from rack-mounted patch panels to the network equipment, as well as each station device.

5. For connections between network switches in MDF/IDF locations employing fiber-optic interconnects, install an appropriate dust-protected rack-mount fiber optic enclosure, preferably one with a slide-out front access drawer for easy cable manipulation. Where available cabinet space precludes this, use a surface-mount fiber optic enclosure and an innerduct path to the cabinet for fiber optic patch cables.

2.4 CABLE MANAGEMENT

A. Distribution Rings

1. All Cables routed on backboards should be supported using die-cast aluminum distribution rings “D-Rings”. Rings should be located within 12” of entering or exiting conduit, 6” prior to any radius bends, and at least 2’ on center. Metal Distribution Rings keep all low voltage cables & wires neat & well-organized, featuring rounded edges that will prevent damage to the wire & cable, allowing for an easier “pull”.

B. Cable Management ties

1. Bundle all communications cables together with Hook & Loop-type tie wraps only. ZIP TIES ARE PROHIBITED as they have been known to kink and cut into the cabling.

2.5 COMMUNICATIONS CLOSETS CONFIGURATION

In large installations employing the Main Distribution Frame (MDF) the MDF should be at least 10’x16’ to allow maintenance access and meet ADA requirements. When sizing the MDF closet, consult all local and state ADA regulatory requirements.

A. Communication Backboard

Data/Voice terminal backboards should be 3/4” thick plywood painted with two (2) coats of White, fire retardant paint, APA exterior grade Douglas Fir A-C and fire retardant with flame spread rating not more than 25 when tested according to ASTM E-84. Refer to drawing for locations, quantities, and mounting arrangement. The installer must ensure that requirements for demonstrating fire rating compliance are met (e.g. masking of fire coating stamp printed on plywood, or paint label).

B. Equipment Cabinets

1. General Guidance for all Equipment Cabinets: Provide enough cabinet space to facilitate the CSI design, leaving a minimum of 25% room for growth within each closet, cabinet, and patch panel.

2. Wall-mounted Cabinets: Wall-mounted cabinets can be used where a typical 2-post floor mount rack is impractical or unnecessary.

3. Vertical Wire Management: The Cable Management System should be used to provide a neat and efficient means for routing and protecting fiber and copper cables and patch cords on telecommunication racks and enclosures. The system should protect network investment by maintaining system performance, controlling cable bend radius and providing cable strain relief. Use 6” wide managers on either side of the rack rails unless cabinets are mounted side by side in a row. In that case place 8” managers between the cabinets with 6” managers on each end. All center-mounted vertical cable managers should be bolted to both cabinets.

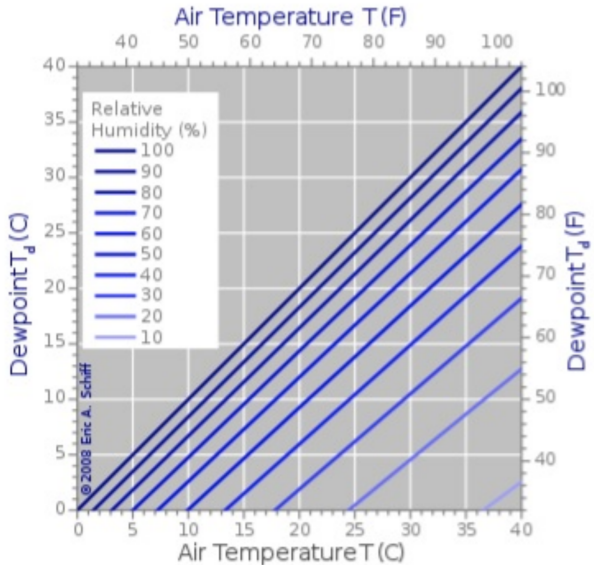
4. Where feasible, provide 4RU of separation space between systems, where different systems exist within the same cabinet. Coordinate exact layout with Customer’s project manager, prior to rough-in.

C. Environmental Requirements

The IT environmental classifications for CSI equipment cabinets is Human Occupancy: the environment should not exceed normal temperature and humidity values for comfortable human occupancy. Where feasible, all active equipment should be located in human-occupiable space. Cabinets consisting only of cross-connects and patch panels, with no active equipment, are typically classified as Natural Environment, where temperatures and humidity do not exceed those of shaded open air environments.

The most environmentally-critical component in a CIS deployment is the Cloud Video Recorder (CVR), which has the following specific minimum and maximum operating values:

Temperature (main board): minimum 0C, maximum 50C
Temperature (system): minimum 0C, maximum 35C[1]
Humidity: below dew point (e.g. non-condensing), using the following chart:



2.6 BACKBONE CABLING

Backbone cables should be installed separately from horizontal distribution cables. Where backbone cables and distribution cables are installed in a cable tray, backbone cables should be installed first and bundled separately from the horizontal distribution cables.

A. Copper Backbone

1. Plenum dry locations require a plenum-rated cable or non-plenum-rated cable enclosed in EMT conduit.
2. Plenum wet locations require a plenum-rated liquid-tight flexible conduit.
3. Non-Plenum dry locations do not require conduit, but EMT conduit vertical runs are recommended to facilitate future expansion and reduce RFI interference.
4. Non-Plenum wet locations require a non-plenum-rated liquid-tight flexible conduit.

[1] https://www.intel.com/content/dam/support/us/en/documents/intel-nuc/NUC10i357FN_TechProdSpec.pdf (page 42)

B. Optical Fiber

1. Optical Fiber Cable: Data communications backbone should be installed from the MDF to each of the IDF locations where distance and/or bandwidth requirements dictate. Typically this will be specified in the CIS Design Document.

2. Dust-protected Fiber Optic enclosures should be used for all MDF/IDF fiber optic runs.

3. Fiber optic enclosure bulkheads must terminate each fiber strand. No fibers may be left unterminated. Any unused bulkhead bays and ports must be covered by blanks to maintain dust protection.

4. Generally LC-type connectors should be used throughout the fiber optic plant to maximize port density.

2.7 ACTIVE COMPONENTS

1. Cloudastructure Video Recorder (CVR): This device should be sized to the expected number of cameras, and camera activity level. This is what is used to capture video footage, and then upload it to cloud storage once Internet connectivity becomes available. A CSI sales engineer will assist in selecting A CVR based on performance and environmental requirements.

2. Network switch(es): These switches are essential to connect the CVR to the security cameras and/or video encoders (for legacy analog cameras). Power Over Ethernet (PoE) switches are used to provide power to cameras over the same network cabling used for network connectivity. In the event that the switch is non-PoE or provides insufficient power, PoE injectors are used in their place. Recommend to use managed switches to assist with per-interface troubleshooting and diagnostics of underperforming or offline cameras and other security devices.

3. Video Encoder: For legacy analog cameras that use coax cabling, along with separate power supplies, these units allow the re-use and integration of analog cameras into a network video recording system. Typically video encoders will not be used at sites with new IP Cameras.

4. Power supplies/power injectors: For analog cameras, the cameras will have separate connections for signal (coax cabling) and power (separate DC power leads). For PoE injectors, most are for single cameras, but there are some mid-span multi-link PoE injectors on the market. PoE injectors are used in situations where there is no PoE switch or the power from the PoE switch is insufficient for the application. The suitability of these solutions is beyond the scope of this document.

5. Line Drivers/Line Extenders: There are several offerings for overcoming circumstances where there are distance limitations for traditional twisted-pair between a network switch and IP Camera, and circumstances where replacing legacy coax cable plant would either be costly or impractical. The suitability of these solutions is beyond the scope of this document.

6. Internet connection: This connection/circuit should be sized according to the expected network load for both recording and uploading in addition to any “live views” from a device on the local (Customer) networks. In the event of a shared Internet connection, this should be sized to support the high water mark of all Internet connections for that site circuit.

7. Router/firewall: This is what allows for the CVR to reach the Internet and to separate cameras/access control traffic from other networks at the site. This is needed in the event that the Internet is shared and “mixed-use” and to limit the access of cameras from other networks.

8. Uninterruptible Power Supply (UPS): This provides power in the event of substandard or interrupted power. Recommend that UPS units are used for backup power to CVR, cameras, encoders, network switches, routers/firewalls, all the way up to the point where the Internet enters the building/campus (the carrier/network demarcation point). Due to the weight of these devices, they are typically placed on the floor/ground and fed into an in-rack/in-cabinet Power Distribution Unit (PDU). In the event that the UPS units are installed in-cabinet, careful consideration needs to be applied to the additional weight the UPS adds to the rack/cabinet.

9. Power Distribution Unit (PDU): While lacking in surge suppression, these consolidate the power connections to in-rack distribution. This helps reduce clutter caused by power cords for the rest of the active hardware. Because they lack surge suppression, they are often used in conjunction with UPS units because surge suppression can cause bigger issues with UPS units when used downstream from the UPS. Upstream surge suppression is redundant as the UPS incorporates these functions, lightning suppression (in the electrical main or sub-panel) is entirely another matter.

PART 3: EXECUTIONS

3.1 RECEIVING INSPECTIONS

The installer should inspect all bulk cable prior to installation to verify that it is identified properly on the reel identification label that it is of the proper gauge, contains the correct number of pairs, and is the material ordered. Any physical damage to the cable and wire should be noted: non-uniform jacket thickness and jacket tightness should also be identified. Note any buckling of the jacket, which would indicate possible problems.

Similarly, all infrastructure components – cabinets, patch panels, connectors, jacks, and patch cables – should be inspected prior to installation to verify the applicable Design Document specifications are met.

3.2 CABLE TRAY AND RACEWAY INSTALLATION

A. Cable Tray Systems Installers

1. The cable tray systems should be rigid, prefabricated structures that support telecommunications cables and cabling and installed to meet applicable building codes. If any cable tray is to be shared by another installer telecommunication, cables should be separated by a nonconductive or grounded metallic barrier.

2. Cable trays and raceways should be sized to allow for future growth, with 25% of the total capacity unused.

3. Pathways that require slots and/or sleeves to penetrate through a wall must meet applicable fire code regulations, and provide 25% additional cable occupancy capacity for future growth.

4. Sleeves and slots must not be left open after cable installation. All sleeves and slots should be fire-stopped in accordance with the applicable building codes.

5. Cable trays and raceways, and all transitions, should be installed below all mechanical components for access during installation and for future cabling needs as it is routed to each of the MDF/IDF locations.

B. Supporting Cable Trays and Raceways

1. Cable trays should be supported by installing:

    a. Cantilever brackets anchored to vertical walls and partitions.

b. Trapeze supports with threaded rod ceiling anchors.

c. Where code permits, braided stainless steel suspension wires.

2. Supports should be spaced according to the cable load and span, as specified for the cable tray or raceway's type and class by the manufacturer and applicable codes. Supports should be placed so that connections between sections of the cable tray are between the support point and the quarter section of the span. Support must also be placed within (2') on each side of any connection to a fitting, per NEC requirements.

3. Cable trays and raceways should never be used as walkways, ladders, or support for personnel. Cable trays can only be used as a mechanical support for cables. For heavily loaded pathways, supports may need to be designed by the structural engineer or professional engineer.

C. Bonding Cable Trays

All metallic cable trays must be grounded and all sections including conduits bonded in accordance with listing requirements for the particular type of system. All cable trays and grounding conductors should be clearly marked in accordance with the manufacturer's instructions, applicable codes, standards, and regulations.

3.3 CABLE INSTALLATION – GENERAL

A. Workmanship

The installer should ensure that the communications cable is installed with care, using techniques that prevent kinking, sharp bends, scraping, cutting, deforming of the jacket or other damage. During inspection evidence of such damage will result in the material being declared unacceptable. The installer should replace unacceptable cabling.

B. Conduit and Cable Tray Usage

Installers should install all Cable trays and conduits for communication cable. All conduits should be routed in the ceiling space and not in the concrete slab whenever possible. All conduits should be run from the station located in one complete and continuous path to the cable tray and bonded to the cable tray as per ANSI/TIA Standards and the NEC. Conduits should not have more than a 180° bend radius in the entire span of the conduit from end to end. If more bend radius is required, install a pull point or pull box after the first 180° of bend radius and continue with this practice through the entire span of the conduit until the path is installed completely.

Each conduit installed should service only one location each. Each conduit will have a 200-lb pull string, and where required by electrical codes,
grounding bushing and ground wire no smaller than 6 AWG, also installed by installers.

C. Spanning of Cable

Spanning of cable is not allowed in any span longer than 36” from cable tray to conduit. No cable run should exceed 90 meters or 300 feet from station locations to the nearest MDF/IDF and not to exceed 100 meters with service loop and patch cables.

D. Cable Draping

The cable should not be draped on, tied, or otherwise secured to electrical conduit, plumbing, ventilation ductwork, or any other equipment. The cable should be secured to building supports or hangers specifically installed for this purpose. All wiring is to be installed in a neat and inconspicuous manner, per local code requirements. Data cables are to be bundled separately and routed parallel to one another in the cable tray from other cables.

E. Allowable Cable Bend Radius and Pull Tension

In general, communications cable cannot tolerate shaper bends or excessive pull tension during installation. The minimum radius bend should be ten (10) times the cable outer diameter with no tensile load applied and twenty (20) times the cable outer diameter with a maximum tensile load of 25 ft/lbs. is applied during installation.

F. Cable Lubricants

Lubricants specifically designed for installing communications cable may be used to reduce pulling tension as necessary when pulling cable into conduit. After installation, exposed cable and other surfaces should be cleaned of lubricant residue.

G. Conduit and Raceway Fill

The communication raceway should not be filled beyond 40% capacity.

H. Backboard and Rack Cable Supports

Clamps, “D-Rings” and Velcro tie-wraps are all acceptable ways to support cable. However, installation of these supports should be done with care so as not to cause crushing or distortion of the cable, nor cause tighter bends than the minimum radius permitted for each type of cable.

3.4 DATA STATION CABLING

A. Service Loops

Provide 10' of service loop using adequate support structures (ladder rack) on all cables routed with each MDF/IDF. Provide 10' of service slack in the ceiling secured neatly to the side of each drop respective conduit to accommodate future cabling system changes for the telecommunications outlets and at a serviceable height of no more than 18" above T-grid.

B. Terminations

In addition, each cable type should be terminated in accordance with the recommendations made in the ANSI/TIA telecommunications standards, manufacturer's recommendations, and/or best industry practices.

C. Grid or Lighting Support Wires

All cable hooks and raceways should be supported to the hard ceiling with their own dedicated support wires or threaded rod. DO NOT reuse the T-bar grid or light fixture support wires to carry the cable.

D. Support Around Moveable Devices

The installation of cables around movable devices, instruments, sub-panels, etc., should be provided with adequate support, length, protection, and flexibility so that the cable is not damaged in the event of equipment being moved.

E. Separation from AC Power Pathways

Every attempt should be made to avoid running telecommunications close to (less than 24") and parallel to power raceway and wiring, or close to light fixtures.

3.5 CABLE LABELING

A. Labeling Cable Ends

All cables should be labeled at each end with the same numbering scheme as approved by CSI and should conform to ANSI/TIA-607 standards.

B. Label Agreement with As-Built Drawings

All labeling information should be recorded on the as-built drawings and all test documents should reflect the appropriate labeling scheme.

C. Label Ink and Substrate

All label printing will be machine-generated using indelible ink ribbons or cartridges. Self-laminating labels will be used on cable jackets, appropriately sized to the outside diameter of the cable and placed within view at the termination point on each end. Nylon conformal labels should be used to wrap cables.

D. Station Drop Cable Labels

Each station outlet terminal should be identified and marked on the patch panel with the outlet number as specified in the Design Plan.

1. Station Labels: Station Labels should contain the fewest alphanumeric characters as necessary for a logical, consistent, and user-friendly identification system. With the exception of Wireless Access Points (see Part 2.2.A.6), all outlet labels should be produced with a labeling machine producing black on white 9mm adhesive Mylar tape labels using 18pt font.

2. Camera locations should be labeled with black on white 9mm adhesive Mylar tape. Labels should be no less than 18mm with a font of no less than 24pt. and will be placed on the ceiling grid track next to the camera cable termination.
3. Intercom locations should be labeled with black on white 9mm adhesive Mylar tape labels. Labels should be no less than 18mm with a font of no less than 24pt. and will be placed on a ceiling grid track directly below the termination location.

4. Label all patch panel jacks in an identical fashion.

5. The numbering system should be Closet, Rack, Patch Panel, and Port (Example, A-1-1-48).

3.6 GROUNDING AND BONDING

A. Cable Tray Bonding

Installers should ground/bond all cabinets, cable trays, raceways, and conduits installed for communication cables with no less than #6 AWG. All conduits must be installed per current NEC and be terminated into a box or bushing prior to cabling. Implementation of telecommunications grounding and bonding as per TIA-607-C and ISO/IEC 30129: Install a Telecommunications Bonding Conductor.

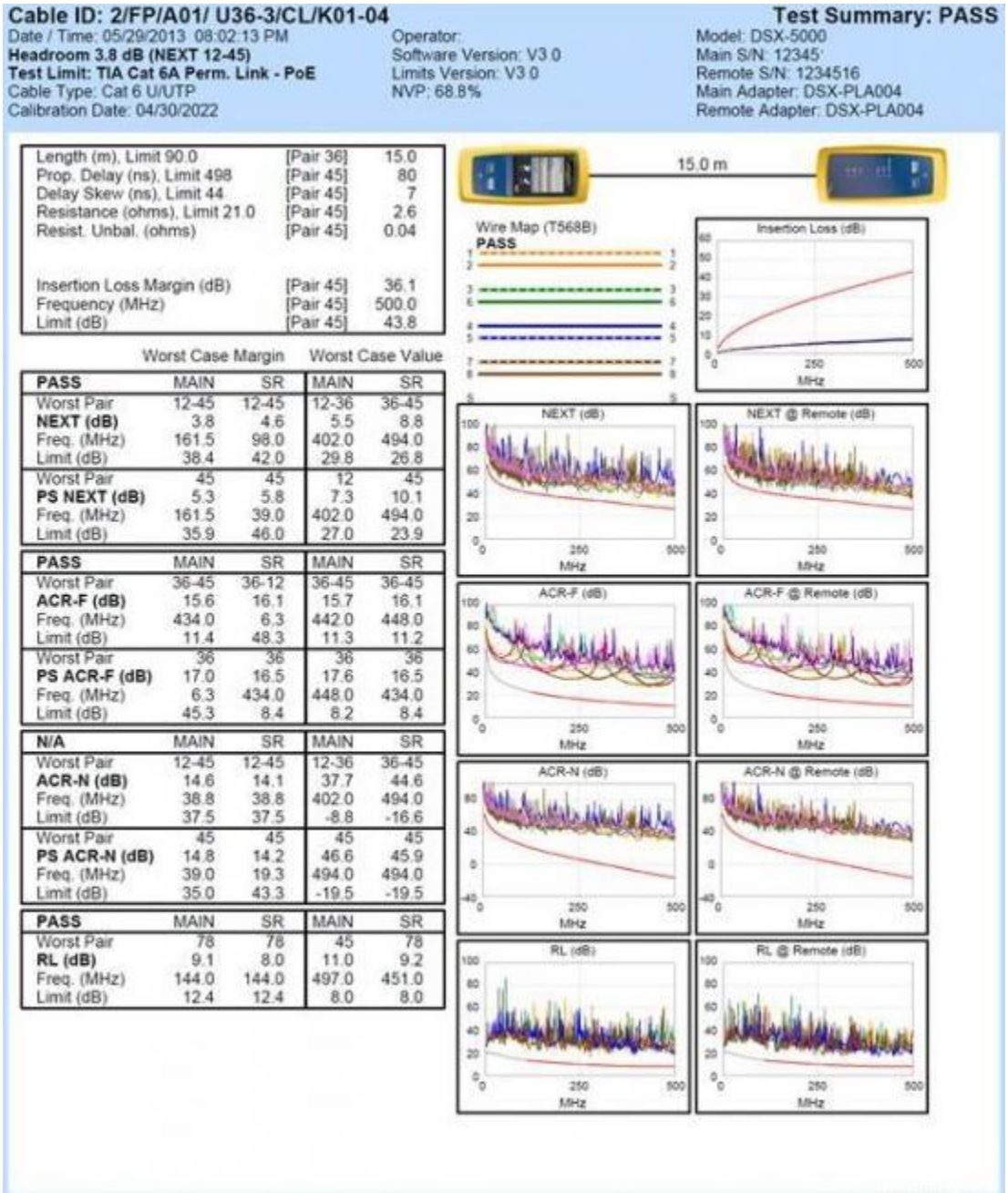
3.7 TESTING

A. Testing UTP Cables and Links

1. The performance tests and their procedures have been defined in the ANSI/TIA/EIA-568-C.2 standard and the ISO/IEC 11801 standard. The TIA standard defines performance in categories (Cat 6) and the ISO defines classes (Class C, D, E, and F). These standards define the procedure to certify that an installation meets performance criteria in a given category or class. Certifications should include the following parameters for each pair of each cablesinstalled:

   a. Wire map (pin-to-pin connectivity)
   b. Length (in feet)
   c. Attenuation
   d. Near-End Crosstalk (NEXT)
   e. Far End Crosstalk (FEXT)
   f. Equal Level Far End Crosstalk (ELFEXT)
   g. Attenuation/Crosstalk Ratio (ACR)
   h. Return Loss
   i. Propagation Delay
   j. Delay Skew

Each cable test should be documented with a certification report similar to the following:



Cable ID: 2/FP/A01/ U36-3/CL/K01-04 — **Test Summary: PASS**

Date / Time: 05/29/2013 08:02:13 PM
Headroom 3.8 dB (NEXT 12-45)
Test Limit: TIA Cat 6A Perm. Link - PoE
Cable Type: Cat 6 U/UTP
Calibration Date: 04/30/2022

Operator:
Software Version: V3.0
Limits Version: V3.0
NVP: 68.8%

Model: DSX-5000
Main S/N: 12345
Remote S/N: 1234516
Main Adapter: DSX-PLA004
Remote Adapter: DSX-PLA004

Length (m), Limit 90.0	[Pair 36]	15.0
Prop. Delay (ns), Limit 498	[Pair 45]	80
Delay Skew (ns), Limit 44	[Pair 45]	7
Resistance (ohms), Limit 21.0	[Pair 45]	2.6
Resist. Unbal. (ohms)	[Pair 45]	0.04
Insertion Loss Margin (dB)	[Pair 45]	36.1
Frequency (MHz)	[Pair 45]	500.0
Limit (dB)	[Pair 45]	43.8

	Worst Case Margin		Worst Case Value	
PASS	MAIN	SR	MAIN	SR
Worst Pair	12-45	12-45	12-36	36-45
NEXT (dB)	3.8	4.6	5.5	8.8
Freq. (MHz)	161.5	98.0	402.0	494.0
Limit (dB)	38.4	42.0	29.8	26.8
Worst Pair	45	45	12	45
PS NEXT (dB)	5.3	5.8	7.3	10.1
Freq. (MHz)	161.5	39.0	402.0	494.0
Limit (dB)	35.9	46.0	27.0	23.9
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-12	36-45	36-45
ACR-F (dB)	15.6	16.1	15.7	16.1
Freq. (MHz)	434.0	6.3	442.0	448.0
Limit (dB)	11.4	48.3	11.3	11.2
Worst Pair	36	36	36	36
PS ACR-F (dB)	17.0	16.5	17.6	16.5
Freq. (MHz)	6.3	434.0	448.0	434.0
Limit (dB)	45.3	8.4	8.2	8.4
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-45	12-45	12-36	36-45
ACR-N (dB)	14.6	14.1	37.7	44.6
Freq. (MHz)	38.8	38.8	402.0	494.0
Limit (dB)	37.5	37.5	-8.8	-16.6
Worst Pair	45	45	45	45
PS ACR-N (dB)	14.8	14.2	46.6	45.9
Freq. (MHz)	39.0	19.3	494.0	494.0
Limit (dB)	35.0	43.3	-19.5	-19.5
PASS	MAIN	SR	MAIN	SR
Worst Pair	78	78	45	78
RL (dB)	9.1	8.0	11.0	9.2
Freq. (MHz)	144.0	144.0	497.0	451.0
Limit (dB)	12.4	12.4	8.0	8.0

2. Test equipment should provide an electronic and printed record of these tests.

3. CSI recommends 100% testing for a warranty, not sample testing, with no marginal passes accepted. This provides performance headroom equal to the measurement accuracy tolerance defined in the testing standards. All applications defined by the standards to be supported by the relevant cabling channel system will be covered by the Authorized Supplier Company warranty for the duration of the warranty.

B. Testing Fiber Optic Cable

1. Testing of Fiber Optic Cable should adhere to the ANSI/TIA-568.3-D standard. Testing fiber optics with a light source and power meter-utilizing the One Reference Jumper method (TIA- 526-14-C method B). If loss test results are outside the acceptable range, test cable with an Optical Time Domain Reflectometer (OTDR) to determine the cause of variation. Correct improper terminations and replace damaged cables before final system acceptance.

2. Fiber should be tested at 850nm and 1300nm for multimode. If more than 1% bad strands are found, remove and replace the entire feed.

3. Testing will be performed with the most recent version of the software as required by The Authorized Supplier to ensure warranty compliance.

4. Each fiber test should be documented with a certification report similar to the following:

Circuit Detail Report

Link ID:	FS1	Page:	1
Company Name:		Meter Type:	FIBER LOSS
Telephone Number:		Serial Number:	SN:FO43199
		Software Version:	V4.71
Report Date:	5/23/2022		

Circuit ID:	FBR:001	Date of test:	4/24/2019
Calibration Date:	3/18/2019	Temperature:	84.0 F

Circuit Characteristics

Fiber Length (in kilometers):	4.38
Number of Connector Pairs:	2
Number of Splices:	2
Cable Type:	OUTDOOR SM
Standard:	ANSI/EIA/TIA568B.3

Circuit Test Results

	1310nm
Passive Cable System Attenuation	
Light Source Reference Power	-10.21dBm
Fiber Loss	2.19dB
Connector Loss	1.50dB
Splice Loss	0.60dB
Total Allowable System Loss	4.29dB
Minimum Required Power	-14.50dBm
Measured Power	-12.52dBm
Optical Loss	2.31 dB
System Overhead	1.98dB
Operating Margin %	34.27%
Pass/Fail	Pass

Installer/Tester: _____ Date: _____

Customer: _____ Date: _____

C. Final System Testing

To provide the most reliable and secure system, the final system test should include validation of the following:

1. Initial active device inventory
2 NIST Cyber Security Framework (CSF) vulnerability assessment (VA)
3. NDAA compliance verification
4. Firmware version tracking, and baseline performance metrics
5. Latency tracking to the CSI cloud
6. VLAN segment IP address violations
7. DHCP and multicast broadcasts

An SNMP network management system (NMS) module provides the ability to continuously track switch and camera port performance, to detect broadcast storms and oversubscribed connections.

In all deployments care should be taken to always adhere to local and national safety codes.