Critical care and mission critical operational facilities are among the most important spaces impacting the design, implementation and management of ICT related infrastructure and networking components. Maintaining 99.999% availability of network services is a non-negotiable design criterion for these environments. The potential risk associated with implementing a facility which does not meet the level of availability to support the needs of a functional hospital is extremely great, and creates risk for all parties involved in the process.

By examining various components of the environment, a baseline solution-set including the passive cabling infrastructure, the network equipment requirements, security, and auditing protocols can be clearly defined. These requirements can vary widely based upon the level of availability that the facility as a whole, or various sub-regions within facility deem as necessary. While one can design, integrate and sustain a complete network environment for a waiting room and cafeteria which meets the same redundancy, power backup, and low latency and jitter requirements as an operating room or Neonatal Intensive Care Unit (NICU), it is not fiscally responsible to burden the entire project scope with such systems.

Within this document, we will analyze the current healthcare ICT design best practices and standards from organizations such as Building Industry Consulting Services International (BICSI) and the Telecommunications Industry Association (TIA), evaluate redundancy criteria based on spatial functions and categories, and review the various security and privacy regulations and guidance as outlined in the United States Health and Human Services (HHS) Code of Federal Regulations (CFR). With those considerations in mind, the already well known benefits of a Tellabs® Optical LAN (OLAN) become all the greater with the added flexibility in delivering best of breed services to each business function (on demand instead of via cumbersome infrastructure, communications spaces, and specialized network switches for each traffic type).

Current Standards & Guidelines

When evaluating the criteria to support any facility, let alone a critical care hospital or similar space, it is vital to understand the differences between desired features, best practices and suggested methods, and standards and regulations. While codes and regulations are considered law, standards, best practices and suggested methods are merely guidelines based on past experiences and consensuses of non-profit working groups. The common documents which influence healthcare and critical facilities are those published by the United States Health and Human Services (HHS), the Facility Guidelines Institute (FGI) Guidelines for Design and Construction of Health Care Facilities, along with those outlined under various support organizations such as the Telecommunications Industry Association (TIA).

It also is vitally important to reflect upon the ancillary systems which provide the health operational functions of the facility. These can include the requirements, many times contractual with the healthcare ownership or region including Picture Archiving and Communications System (PACS) and imaging solutions

, patient entertainment and education systems, tele-medicine and tele-health diagnostics systems, patient monitoring, nurse call solutions, and real time location systems (RTLS) among others. Without the proper inclusion of all of these components in addition to standard voice, data and audio/visual systems, an overall map of a facility cannot be put together. In the scenario where all systems are not properly

acknowledged, the proper security, traffic priority, and monitoring of the systems cannot be ensured and the inevitable "finger pointing" of the system designers, vendors, and integrators will ensue during the commissioning of a facility.

The standards for current facility designs are not well documented, and instead follow more of a common sense architecture for hospitals based on the level of redundancy and resiliency that is required by the design team. The common set of design principles for a full service facility include:

- Redundant outside plant and service provider entrance facilities with redundant data-center or equipment room facilities
- Diverse circuit routes from multiple service providers
- Fully redundant core network switching components in each data-center
- Meshed access layer switching components to each of the core nodes (sometimes a distribution layer as well)
- Redundant backbone cabling to all intermediate distribution frame (IDF) or telecommunications rooms (TRs) service the access layer of the network.
- Parallel infrastructure and switching to support nurse call systems
- 802.1x authentication for all devices to adhere with any HIPAA guidelines on information security and protection.
- Physical security safeguards and procedures to not only limit access to both physical and virtual data and to properly be notified of any events or intrusions to the system.

While the ANSI/TIA-1179 Healthcare Infrastructure Standard outlines the suggested design of various spaces within a hospital, it acts purely as a guideline. When reviewing recent designs and implementations of new, large hospitals, most are not installing the numbers of individual cables and outlets per room as would be suggested by the standard. One reason for this is the rapid convergence of systems into fewer infrastructures in modern facilities as security, authentication, and technologies such as Passive Optical LAN can provide streamlined delivery and operations of many different service over a single medium. As an example, patient rooms typically are no longer installing greater than 14 Category 6 or 6a cables and more commonly are providing two (2) to four (4) cables in a room to provide patient monitoring services, and another two (2) to four (4) cables to provide patient entertainment and education services, Wi-Fi, and Voice over IP (VoIP) functional services.

That TIA-1179 standard also asserts that an IDF/TR should be larger than a normal space and be no less than 12 m^2or 130 ft^2. This increase is size is a direct result of many individual network types requiring their own rack space, cabling infrastructure, switching architecture, power systems, and that IDF/TRs server upwards of 50,000SF in a hospital. Convergence over a logical Optical LAN solution permits for a dramatic reduction of these devices into a few rack units of fiber optic patch panels and Optical Network Terminal (ONT) powering units which can commonly be placed into a small wall rack. The result is additional floor space that may be turned into revenue generating purposes such as more beds in the facility. Figure #1 illustrates the current TIA-1179 suggested design standards for cable counts, large pathways and IDF/TR spaces. In contrast, Figure #2 illustrate the logical reduction in passive infrastructure cabling, pathway requirements, and physical IDF/TR spaces with a Tellabs Optical LAN and converged network design.

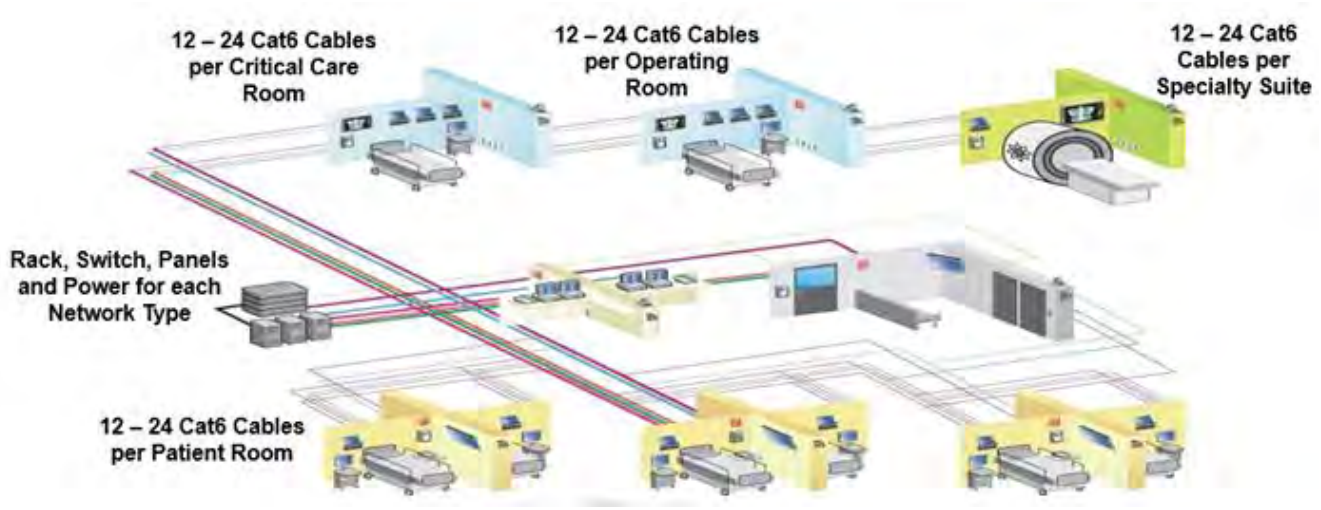

Figure #1: Legacy copper and disparate network switching architecture

Figure #2: Fiber based Tellabs Optical LAN and converged network architecture

The HHS CFR acts as a guideline for system operations and policy with regards to the methods that an overall network is implemented and, even more so, how access and data is restricted and alarmed. It is a common misconception that HIPAA (US Health Insurance Portability and Accountability Act of 1996) outlines a certifiable system test and a checklist that a system must meet to be HIPAA compliant. A compliant HIPAA solution is comprised of a full set of systems, organizational units, and processes that must work together to provide the right level of security and operations.

The relevant section of the HHS CFR is Title 45, Part 164, Subpart C. This section, titled “Security Standards for the Protection of Electronic Protected Health Information”, describes the three safeguards of a technical solution: Administration, Physical and Technical. As stated in Subpart C, a primary goal of a ‘system’ is to “ensure the confidentiality, integrity, and availability of all electronic protected health

information the entity creates, receives, maintains or transmits…" and "protect against anticipated threats or hazards to the security or integrity of such information". By adhering to the design principles in use today, and the security protocols and concepts outlined in this document, a system can be considered compliant with Subpart C and thereby a HIPAA compliant solution offering for the various systems in place.

Common standards that are not well known, but have major implications within the design of a facility are:

- UL 1069 (Standard for Hospital Signaling and Nurse Call Equipment)
- NFPA 99 (National Fire Protection Standard for Health Care Facilities)
- NFPA 70E (Standard for Electrical Safety in the Workplace & National Electric Code)

The UL 1069 standard has direct impact on the Nurse Call System (NCS) which must provide audible and visual notification between a patient and hospital nursing and critical staff. It is for this reason, as we show in this document, that NCS platforms require their own dedicated cabling infrastructure and equipment to support them. The NFPA standards play a vital role in designing the remote powering solutions that is used within the Optical LAN designs to ensure maximum backup power is available to the ONTs in the necessary spaces.

Design Methodologies for Passive Optical LAN in Critical Infrastructure & Care Facilities

It is suggested that any parties involved in the overall system design of a facility closely examine each system, and determine if a disparate network infrastructure and switching architecture is required. Table #1 outlines the rudimentary methodology which determines what infrastructure type and level of security should be present during any pre-design requirements phase.

Network/Service Description	Dedicated Network Infrastructure Required?	Converged Network Capable
Facility Staff VoIP Platform		X
Facility Data Network (non-guest/patient)		X
Facility BMS & Automation Systems		X
Facility Security, Badging & Surveillance		X
Life Safety Fire Alarm and Elevator Systems	X	
DAS (Cellular) & LMR (1st Responder) Systems		X
Digital Signage		X
Audio/Visual Systems		X
Real Time Location Systems (RTLS)		X
Patient Monitoring & Telemetry		X
PACS Imaging		X
Radiology & MRI		X
Tele-medicine		X
Patient Entertainment & Education		X
Nurse Call Network	X	
Patient & Guest Wi-Fi Access		X
PCI Compliant Point of Sale		X

Table #1: Common system convergence example

When taking these systems into account, and understanding that a facility may contain additional clinical, governmental (CDC), or specialized networks, it often becomes clear that the stakeholders of the final product have the ability to shrink what has commonly been five to fifteen different network switching solutions into two to three. Operationally the benefits include a reduction in cable plant and pathways as well as IDF/TR spaces; reduction in dedicated cooling systems and power systems; and a consolidation of IT staff required to manage each of the networks. This last functional benefit is often one of the most challenging to overcome based on the political landscape in place during the design phase and a perceived threats to job security. By pooling resources from various IT functions, network design, management, and security functions can be increased due to the broader knowledge of technologies, protocols and administration from each team or services that is consolidated.

There will commonly be networks which require their own dedicate infrastructure, pathways, and switching technologies. As show in Table #1, both the life-safety systems and nurse call networks are *usually* required to be on their own infrastructure and switches. In the case of the fire alarm communicator, elevator phone, and communications systems, the regional or national Authority Having Jurisdiction (AHJ) will determine if the analog or IP services used may run over the converged network. While it may be feasible to place these over a redundant and backed up Optical LAN solution, it is recommended that these services be fed with copper based and dedicated feeds to eliminate inspection and approval issues which could arise during final verification by the AHJ.

The same holds true for NCS platforms as defined under the UL 1069 standard requirement. Due to the nature of these systems, they require a dedicated network. By running a separate fiber strand for the Nurse Call ONTs from the zoned architecture, and providing the necessary backup ONT power and head-end OLT, a facility may also utilize the Optical LAN to support the nurse call network without requiring expensive switching systems and increasing the floor space of an IDF/TR.

Implementation Guidelines for Healthcare Optical LAN Solutions

Taking into consideration the best practices, standards, and functional system requirements a common set of criteria can be formed that outline how a critical healthcare facility should be implemented. These can be broken into categories related to the passive layer-1 architecture, Tellabs Optical LAN component design and layout, network equipment security, backup and redundancy. This list below represents the minimal best practices Tellabs recommends for healthcare and critical networks. A redundant topology is shown in Figure #3 that provides sub-second optical failover of all services and meets the minimum Tellabs requirements for a critical care facility.

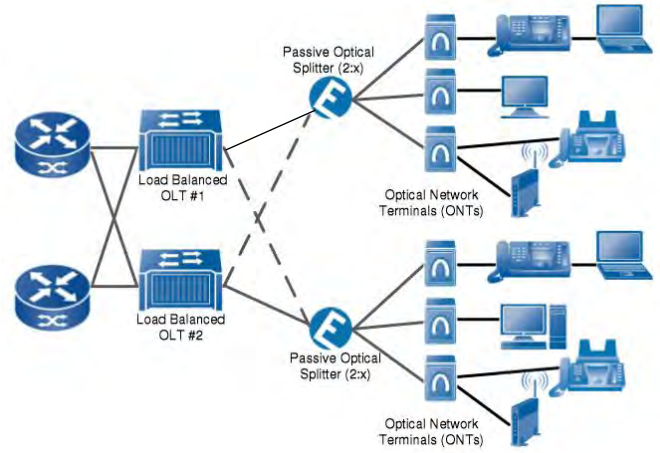

Figure #3: Required Tellabs Optical LAN Topology

Layer-1 Passive Implementation:

1. Redundant entrance facilities for incoming ISP or managed services in geographically diverse areas of the facility.
2. Redundant data center locations either on different floors and wings, or altogether

different buildings within a campus with dual fiber routes between buildings.

3. Tie single mode fiber cables between the data centers to support the redundant Optical LAN design and any other services; plus 50% spare capacity.
4. All data center tie fiber shall be fusion spliced, and terminated with SC-APC (Angled Physical Contact) connectors and bulkheads.
5. Riser fiber between the data centers and each IDF/TR space shall be sized to support the number of Optical LAN zones, additional fibers for Optical LAN redundancy, plus 100% growth capacity. For example, six (6) Optical LAN zones on a floor would require six (6) primary fibers, six (6) backup Optical LAN fibers, and twelve spare fibers yielding a 24-strand SMF fiber cable.
6. Zone boxes shall be fed with a 6-strand fiber to support a primary and backup Optical LAN feed, plus growth capacity for additional Optical LAN zones in the future or other services such as specialized equipment, A/V, or DAS. When possible, zone boxes shall be fed from two IDF/TR closets to provide greater facility protection.
7. Zone boxes should be designed with a 15% - 25% sparing capacity to allow future additions to the network.
8. Zone boxes shall be fed from the IDF/TR or Electrical closet with a 25.4-CM (1-INCH) EMT conduit to support ONT remote powering from a bulk, N+1 power source. All conduit shall be properly grounded at the closet space, and to the zone box to meet all NFPA and NEC standards. Every set of 8-ports of powering from a zone box shall be fed with a single copper pair to meet the amperage requirements of the combined ONT. This is commonly, based upon a 76M (250FT) distance from the power source, a #16/2 or #18/2. Proper power calculation assistance can be provided by Tellabs.
9. All splitters in a zone or closet based deployment shall utilize dual input (2:x) splitter to provide redundancy capabilities for locations and services which require redundancy. The secondary input to a splitter shall be attenuated by 5dB in the channel link when utilizing redundancy.
10. To maintain compliance with the TIA-1179 recommendations, a 2-strand SMF cable shall be utilized along with a 2-conductor copper pair to support ONT remote powering. A typical copper pair of #20/2 or #22/2 is sufficient for most installations less than 30M (100FT), however values shall be verified with Tellabs based on the ONT load requirements prior to installation. If remote ONT powering is not to be utilized as the distributed power circuits have UPS or generator feeds, a remote powering copper pair is not required.
11. Zone boxes shall contain NEC compliant, rate-limiting power distribution units (PDUs) for the ONTs that provide 100VA 46-56Vdc limiting circuitry. These PDUs may also provide compliant power for various DAS/LMR platforms as well. All power feeds shall be from an N+1 redundant AC-DC power source in the IDF/TR or electrical space that provides power to the ONTs at a minimum 54-56Vdc launch level. Ensure all N+1 AC-DC power sources utilize separate feeds from diverse breakers and panels for each of AC inputs to the units.
12. All fiber cables shall be tested for power loss from the data center, through the backbone and splitter, and to the ONT location prior to connecting ONTs. Additionally, all DC-power systems (if utilized) shall be tested for a minimum receive voltage of 46Vdc.
13. When utilizing Tellabs® 2-port in-wall (120W), a 10.16CM x 10.16CM (4-IN x 4IN), 8.9CM (3.5-IN)

deep electrical back box with a single gang reducer plate shall be specified to ensure proper mounting of the ONT. All boxes shall contain a 19-CM (.75-IN) conduit from the back box to the accessible ceiling space and ensure all conduits are properly terminated with bushings.

14. In utilizing Tellabs® 4-port in-wall (140W) ONTs, a standard back box of dimensions 10.16CM x 10.16CM (4-IN x 4IN) shall be used with a standard depth. A single gang reducer plate shall be specified to ensure the proper mounting of the 140W ONT and all boxes shall be fed from the accessible ceiling space with a minimum 19-CM (.75-IN) conduit that contains the proper bushings.
15. When providing network access within a patient room, it is recommended the ONTs either be in wall units (Tellabs 120W or Tellabs 140W) that can be mounted directly into mill-work or other finishes. Alternatively, ONTs may be placed outside of the space to minimize any IT requirements to enter the room and disrupt the patient or medical staff. If access to patient rooms is to be limited, ONTs shall be placed either in a wall enclosure or ceiling box outside of the door, and feed Category rated cables to the face-plates within the room.
16. ONTs placed directly in plenum spaces shall be utilized in conjunction with a plenum rated bracket.

Tellabs Optical LAN Equipment Deployment

1. The Tellabs® Optical Line Terminals (OLTs) shall be placed within a data center which meets the requirements of the facility. OLTs will be placed in diverse data center locations for maximum redundancy. When this is not possible either due to cost or facilities, the OLTs should be placed as far apart from each other as possible within a single facility.
2. All OLT components shall be connected to an A and B power source with each A and B feed being sourced to a unique power circuit fed from isolated panels and UPS/generator feeds. Each OLT shall be placed onto dedicated power systems such that a single overall panel failure cannot impact both OLTs. Given the nature of generator startup and transfer switches, all OLT and powering systems shall be connected to UPS systems.
3. All OLTs shall be placed in secured cabinets within the data centers to prevent unauthorized access and tampering. Ensure the cabinets are properly grounded, that the OLTs and AC-DC power sources are properly grounded to the rack, and that the cabinet design provides adequate airflow to the OLT.
4. Ensure that all cabinets, relay racks, power sources, and other Optical LAN components are properly grounded and bonded in all IDF and TRs. Zone boxes utilizing remote ONT power distribution units shall also be grounded to their respective IDF/TR. This becomes most critical in regions subject to heavy tropical or electrical storms and regular power outages.
5. Ensure that all OLTs are meshed to a redundant layer-3 core network utilizing a multi-chassis LAG to create a single core instance. All four 10G uplinks shall be fully meshed from each OLT supervisory card to both of the core nodes in the LAG. This will provide facility and card protection, and a 40Gbps aggregate connection from the OLT to the core network. When utilizing redundant OLT chassis, an 80Gbps load balanced link is provided.
6. At a minimum, all critical spaces shall be dual homed from the 2:x passive optical splitter to redundant OLT chassis. As spaces can rapidly change function, it is recommended that all spaces shall be setup for redundancy and at a minimum have a 2:x splitter and adequate zone

box to IDF/TR fiber to support a redundant link. Critical spaces shall be any that provide services for: patient monitoring, PACS, BMS, operating rooms, RTLS, medication fulfillment systems, NCS, bedside charting systems, and other systems impacting the ability to provide care to the patients.

7. All ONT should be remotely powered to provide centralized UPS protected backup power unless local power sources are properly backed up (e.g. UPS circuit from a generator). Given the potential for special changes, it is possible that an area serving non-critical services could become a functional space for patients and require power backup. Designing the solution day-1 to support any service and with ONT remote powering cabling will avoid future costly re-cabling or additions to the space.
8. When placing ONTs within any enclosure, the thermal output of the unit must be taken into account prior to installation. A lack of proper ventilation from a ceiling, wall or floor box housing ONTs will void the warranty of the units and can lead to system outages.
9. Rack mounted ONTs (Tellabs® 728GP and Tellabs 729GP) shall not be placed in active ceiling zone boxes due to the acoustical volume of the ONT fans and the requirement to run high voltage AC power to the zone boxes.

Network Equipment, Security and Protocols

1. All systems designed for a critical healthcare facility will be designed with fully redundant power supplies, fans, supervisor cards, and network connections. Each Tellabs 1150-series OLT shall be furnished with redundant fan trays (top and bottom). When stacking multiple OLTs in the same rack, a pair of fan trays may be utilized for two OLTs.
2. To maintain compliance with HIPAA guidelines, all ports on an Optical LAN (or any network) that have access to EPHI (electronic Personal Health Information) will be designed with 802.1x port authentication to provide authentication and auditing of the access devices.
3. Network Access Control (NAC) services shall be configured on all ports in conjunction with the 802.1x services to provide dynamic assignment and control of the devices connected within the hospital. It is recommended that machine certificates and login credentials be utilized to provide the dynamic assignment of services.
4. Devices that do not support 802.1x or NAC functions will be authenticated via MAC Authentication Bypass (MAB) to authenticate against the known MAC database of the system. Commonly mobile patient monitors, VoIP phones, printers, and other lower-end devices will fall into this category. MAB will permit for security to be maintained and data segmentation based on VLAN assignment of these devices. Additionally, unauthorized access can both be alarmed, ports deactivated, and notifications made to the appropriate resources of any violations.
5. PoE enabled ports shall be configured to utilize LLDP-MED for power negotiation and to allow for remote inventory of all devices.
6. To ensure proper system operations, all core switches, WAPs, and Optical LAN OLTs shall be configured for SNMP V2/3 monitoring of health and utilization as well as notification of alarms.
7. In accordance with the HHS CFR and to be HIPAA compliant in the overall system architecture, the Tellabs® Panorama PON element management system (EMS) will be properly ‘hardened’ to restrict unused TCP/UDP network ports, have mechanisms to control local and remote server access as well as contain auditing, logging and notification of both successful and unsuccessful login attempts, and be patched regularly with the

proper software releases. Tellabs Engineering and Technical Assistance Center (TAC) is able to provide details on the specific requirements for each application.

Conclusion

Again, critical care and mission critical operational facilities are among the most important spaces impacting the design, implementation and management of ICT related infrastructure and networking components. Maintaining the highest possible availability of network services is a required, non-negotiable design criterion for these critical environments. The potential risk associated with implementing a facility which does not meet the level high availability to support the needs of a functional hospital is extremely great.

Through our examination of multiple components of the environment, a baseline solution-set including the passive cabling infrastructure, the network equipment requirements, security, and auditing protocols have been clearly defined. Healthcare facilities need to keep pace with evolving LAN needs and the technologies that meet those critical needs, including employing fiber optic cabling and the Tellabs Passive Optical LAN solution.

References

United States Health and Human Services (HHS) Code of Federal Regulations (CFR): http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html

HHS CFR Title 45, Part 164, Subpart C: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/dates.pdf

Facility Guidelines Institute (FGI) Guidelines for Design and Construction of Health Care Facilities: http://www.fgiguidelines.org/

Building Industry Consulting Services International (BICSI): https://www.bicsi.org/

Telecommunications Industry Association (TIA): http://www.tiaonline.org/

ANSI/TIA-1179 Healthcare Infrastructure Standard: http://www.tianow.org/articles/a-new-standard-for-healthcare-facilities-infrastructure-cabling/742/

US Health Insurance Portability and Accountability Act of 1996 (HIPAA): http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf