LIFI NETWORKING IN THE CAMPUS ENVIRONMENT

Meeting the Future with Light Fidelity (LiFi)

In today's dynamic and mission-critical environments, Traditional LAN architectures often struggle to meet the evolving demands of modern warfare, leading to inefficiencies, vulnerabilities, and operational limitations. WiFi technologies present challenges in several field environments – Navy vessels, disaster areas, field operations and aircraft/aircraft hangars.

Challenges Facing the DoD

The DoD's reliance on legacy LAN infrastructures presents significant challenges in terms of agility, scalability, and security. Traditional LAN architectures are often static and inflexible, making it difficult to adapt to changing mission requirements or incorporate new technologies. Additionally, these legacy systems lack the advanced security features necessary to defend against modern cyber threats.

LiFi offers a transformative solution to address these challenges by providing flexibility, scalability, and enhanced security. This white paper explores some of the challenges facing the DoD and how Tyto Athene's' innovative solutions can effectively mitigate these challenges, ensuring mission success and operational superiority.

Challenge #1: Legacy Infrastructure Limitations

The DoD's reliance on legacy LAN infrastructures presents significant challenges in terms of agility, scalability, and security. Traditional LAN architectures are often static and inflexible, making it difficult to adapt to changing mission requirements or incorporate new technologies. Additionally, these legacy systems lack the advanced security features necessary to defend against modern cyber threats. WiFi, even the emerging 6GHz version, still presents challenges.

Challenge #2: Network Complexity and Management Overhead

The complexity of DoD networks, compounded by disparate technologies and decentralized management practices, hinders operational efficiency, and increases management overhead. Manual configuration and troubleshooting processes are time-consuming and error-prone, leading to delays in mission-critical operations and escalating support costs.

Challenge #3: Zero Trust Adoption at the Edge

The increasing reliance on mobile devices and remote connectivity introduces new challenges for securing DoD networks and data. Traditional LAN architectures struggle to accommodate the diverse range of devices and access methods utilized by DoD personnel, leading to vulnerabilities and compliance risks. Continuous monitoring of users and devices as they move about the network is increasingly difficult in legacy environments based on decades old Layer 2 VLAN topologies.

Understanding LiFi

LiFi is high-speed, wireless, bidirectional, and mobile communication technology using light rather than radio frequency. LiFi powers internet & local network connections, as well as device-to-device connections. It uses the entire unregulated light spectrum, both visible and invisible spectrum. LiFi is complimentary to Wi-Fi and other RF wireless technologies, such as 5G, LTE cellular, and the well-known Wi-Fi used for laptop and mobile device communications. The significant difference is how LiFi and Wi-Fi transmit data. Whereas Wi-Fi uses radio frequency to induce a voltage in an antenna to transmit data, LiFi uses the modulation of light intensity.

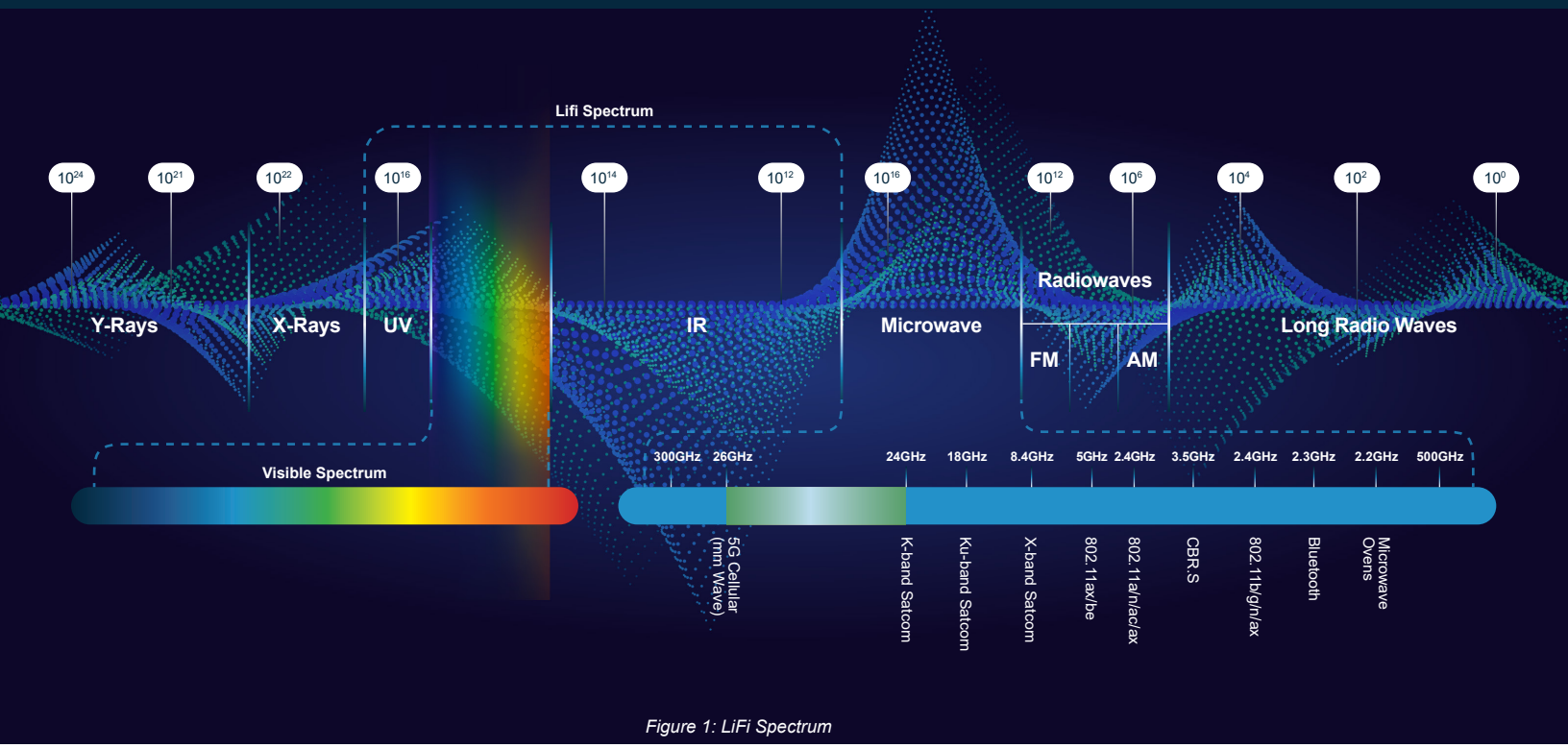

Figure 1: LiFi Spectrum

What is LiFi

- Provides high-speed, wireless, bidirectional, mobile communications using light
- Powers internet and local network connections, as well as device-to-device connections
- Uses the entire unregulated light spectrum - both visible and invisible
- Is complimentary to Wi-Fi and other RF wireless - uses radio frequency to include a voltage in an antenna to transmit data, LiFi uses modulation of light intensity to transmit data

This spectrum chart is not intended to be to scale, rather it shows a regionalized view of some of the various spectrum communications usages today.

Starting on the right are the long radio waves; these include the 300 to 3,000 hertz sound ranges that human ears can listen and imply meaning. There are several global communication systems in this range; extremely low and very low frequency waves can penetrate buildings, ground, and even water (so they can be used in submarines). For example, the US Navy operates an extremely low frequency system that operates at 76 hertz and Russia has one at 82 hertz. China and India are the other two countries that have these systems. These extremely low frequency systems can communicate globally however, the two US based stations located in Wisconsin and Michigan each have their own dedicated power plants to generate the massive power required to operate them. They call this range “long radio waves” as the sine wave generated by extremely low frequency systems is over 2,200 miles long which is more than a quarter of the earth’s diameter. The throughput of extremely low frequency systems is measured in 10’s of characters per minute; hardly broadband speeds however, if you need to communicate underground to a mine or an operational submarine it is the only game in town.

Moving to the left is the range for radio waves we typically think about, starting with the AM radio band. While AM radio could not deliver the greatest sound quality, it was better than nothing when working on a farm tractor. Next is the FM radio band where we finally got to hear real music. Unfortunately, the FM range is typically less than 75 miles. The important point being the higher the frequency, the shorter the distance the wave travels.

Next is the microwave range starting at 500 megahertz. Interesting to note, microwave ovens use 2.2 gigahertz to excite the electrons inside the oven which generates the heat needed to cook food. Older and high-powered ovens tend to be quite “noisy” and bleed over into a wider frequency range. The wider band causes some interference with Bluetooth devices at 2.3Ghz and with the 2.4 gigahertz Wi-Fi devices we use today for IT communications. Shown here, the 2.4 gigahertz Wi-Fi has several IEEE standards to increase effective bandwidth and throughput including 802.11B, “g”, and “n”. The Wi-Fi signal can penetrate most walls and floors to enable a Wi-Fi device to reach an access point several rooms away. The signal can’t travel more than a few hundred yards outdoors due to power restrictions which is why we don’t use Wi-Fi while traveling outdoors.

At 3.5 gigahertz is the citizen broadband radio service (CBRS) which is the reserved shared spectrum used for private 5G communications. CBRS is effective for tens of miles due to higher power levels. At 5Gigahertz is another Wi-Fi band which it less congested than the 2.4 gigahertz range, it’s increasingly saturated with Wi-Fi devices and it has similar coverage patterns as the 2.4 gigahertz spectrum.

At 6gigahertz is another slice of Wi-Fi service known as Wi-Fi 6 or “clean Wi-Fi”. The range has fewer competing devices at least for today, however it doesn’t propagate as far as the 5 gigahertz Wi-Fi. This means that the new Wi-Fi 6 devices are not exact replacements for the Wi-Fi 5 access points therefore upgrade projects require new site surveys to ensure user and device workspace coverage.

Continuing to the left are several satellite communications bands up to 26 gigahertz where the millimeter 5g bands begin. Remember, the higher the frequency, the shorter the distance a signal travels without significant power boosting. That means that commercial 5g in the higher millimeter ranges are more distance limited than the lower frequencies and are unable to penetrate building walls. Commercial 5g towers can help overcome the distance constraint by using higher power however, the mobile phone devices are unable to match the power output.

Starting at 300 gigahertz is the infrared range where the LiFi spectrum begins, and the effective range of today’s radio frequency systems ends. The scientists of the world are working on a 300 gigahertz radar system that may someday extend RF slightly into the infrared range slightly however, physics is a tricky thing when pushing the envelope of RF communications and their results reflect this reality.

LiFi continues through the visible spectrum and the ultra-violet ranges. This is the terahertz and petahertz frequency ranges. We’re getting into large numbers here, so we typically refer to these frequencies in the **frequency distance per second**, or more accurately, the **milli-** and **nano-** inch per second ranges. Recall the submarine communication system that has over 2,200 miles wavelength to keep things in perspective.

The x-ray and y-ray range correspond to the exahertz, zettahertz, and yottahertz frequencies that are not yet used for communications.

802.11 Standards				
Generation	IEEE Standards	Adopted	Maximum link rate (Mbit/s)	Radio Frequency (GHz)
Wi-Fi 7	802.11be	2025ish	1376 to 46120	2.4/5/6
Wi-Fi 6E	802.11ax	2020	574 to 9608	6
Wi-Fi 6	802.11ax	2019	574 to 9608	2.4/5
Wi-Fi 5	802.11ac	2014	433 to 6933	5
Wi-Fi 4	802.11n	2008	72 to 600	2.4/5
Wi-Fi 3	802.11g	2003	6 to 54	2.4
Wi-Fi 2	802.11a	1999	6 to 54	5
Wi-Fi 1	802.11b	1999	1 to 11	2.4
Wi-Fi 0	802.11	1997	1 to 2	2.4
Li-Fi 0	802.11bb	2023	1 to 9608	1000

Figure 2: IEEE Standards

The Institute of Electrical and Electronics Engineers (IEEE) is the standards body that regulates communications signaling standards through the consensus building and approval stages. The IEEE 802 Working Groups addresses standards for local area networks (LANs), personal area networks (PANs), and metropolitan area networks (MANs). Figure 2 lists several standards that are important to Wi-Fi and LiFi. Starting at the top is the emerging Wi-Fi 7 standard that is currently being discussed with an anticipated ratification date some time in 2025.

The Wi-Fi 6 standard from 2020 has a shared bandwidth of up to 9.6 gigabits between users in the same geographic location.

At the bottom is the LiFi standard 802.11bb, which emerged from the 802.11 standards group in March of 2023 and enables up to 9.6 gigabits of throughput starting at the 1 terahertz range.

As LiFi continues to evolve, we expect it to adopt FM-type communications by simultaneously modulating both the lights intensity and frequency to exponentially increase the available bandwidth for devices. From a device perspective, LiFi will seem to provide unlimited bandwidth. It's not unlimited as physics still rules, but the available bandwidth will exceed the mobile device throughput capabilities, battery life, and computing power for many years to come making is seem like unlimited to the user.

The Solution: Why LiFi

LiFi has 2,6000 times the spectrum than all the RF communications combined. More spectrum means more bandwidth and more bandwidth means higher throughput.

LiFi uses the globally unregulated spectrum, meaning it uses a single chipset and the same software drivers anywhere in the world. This is a huge benefit for communications architects. For example, Tyto designs and deploys communications systems around the world and every country licenses the RF spectrum differently which means we can't always use a single technology and spectrum allocation for devices on both sides of international borders. Different wireless spectrum means incompatible communications, LiFi eliminates that constraint since it leverages the unregulated spectrum.

LiFi is inherently secure since light does not penetrate walls, floors, or even a single sheet of paper.

Because LiFi is point-to-point versus a RF broadcast technology, there is a near-zero chance of communications being intercepted. There are no detectable electromagnetic emissions outside of the access point, easing concerns around classified data and Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST).

The 802.11bb standard mandates standard encryption for all traffic, making is post quantum resistant and zero trust complaint out of the box. All the device capabilities that enterprise IT uses today to profile systems such as disk encryption, operating system patching, antivirus signature updates, etc. are all fully supported by LiFi without changes. LiFi Use Cases

LiFi Use Cases

Here are four general purpose uses cases for LiFi.

- It can be used for mobile and fixed networking – like on campuses and inside buildings.
- LiFi provides device to device communication like laptop to video conference connections or phone to TV or soundbar within a single room.
- It can be used to replace cables and connectors, like for desk area networking for keyboard, mouse, and docking station connections.
- The telecommunications industry is starting to use LiFi to extend 5G millimeter wave service inside buildings using signal bridging with LiFi through windows. This is important as the millimeter waves used by 5G service providers can't penetrate building enclosures.

Next, let's look at several practical use case applications for LiFi that will help bring the technology into focus across commercial and military settings.

There's a wide variety of commercial and industrial use cases for LiFi, including in medical and corporate facilities, emergency communications, and manufacturing. Many of these use cases overlap into government operations.

In medical facilities, Wi-Fi is typically congested RF space that suffers significant performance penalties due to the number of devices and the variable latency which can impact RF signals for human life sustaining equipment.

For many organizations, LiFi's secure communications is perfect for locations that require privacy, such as board rooms, proposal areas, and research facilities, virtually anywhere that Wi-Fi eavesdropping caries significant financial or regulatory compliance risk. In manufacturing, today's robotic process automation requires millisecond latency to control systems with pinpoint accuracy.

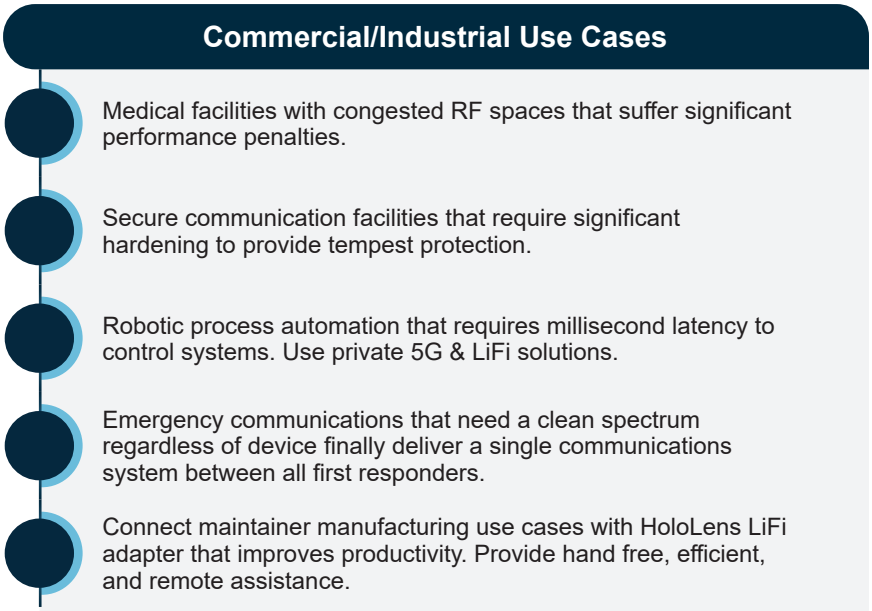

Figure 3: Commercial/Industrial Use Cases

LiFi enables rapid reconfiguring assembly areas that today are hardwired Ethernet connections needed to meet latency requirements. We all hear the constant 5G hype from providers about the high-speed and low latency on "the best network", whatever that means. What they fail to mention is the significant costs associated with building a 5G system both public and private versions. LiFi can be deployed at a fraction of the capital cost and no monthly usage costs.

Automated driving machines and human safety equipment all require exacting communications, for which Wi-Fi is rarely the right answer. LiFi can be deployed within a vehicle, aircraft or vessel for secure internal communications.

Emergency communications require clean spectrum regardless of device type and LiFi can finally provide a single communications system between all first responders anywhere in the world.

LiFi also allows integration with Hololens devices to enable ultra-low latency and very high-fidelity imagery for the metaverse, remote smart hands, and medical material review.

Military use cases include aircraft maintenance support, where during pre- and post-flight work, the military digital twin mandates the exchange of multi gigabytes of engine and airframe performance data, as well as mission information and maps for GPS systems. Wi-Fi begins to break down as the number of aircraft increases along with everyday device communications. LiFi enables each airframe to use a dedicated slice of the spectrum eliminating the shared bandwidth aspect of Wi-Fi communications.

Using LiFi to ensure classified communications with a SCIF are secure by design which significantly reduces the shielding and TEMPEST concerns. It also provides the ability to rapidly standup and tear down echelon mobile shelters for secure mobile communications.

Because light does not penetrate tent walls it is secure from eavesdropping a very important element in tactical spaces.

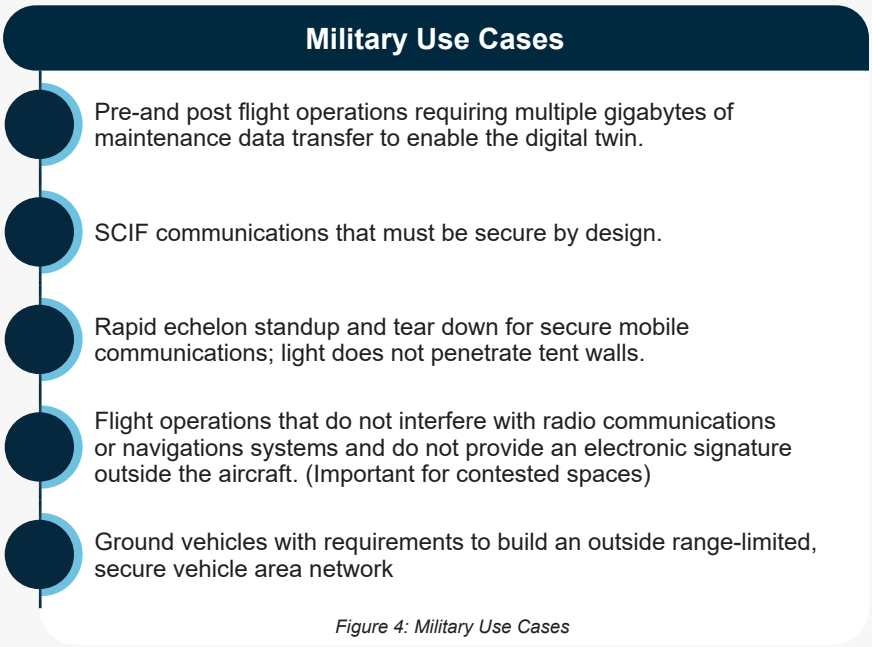

Figure 4: Military Use Cases

For flight operations, LiFi does not interfere with radio communications or navigation systems, and it provides no electronic signature outside the aircraft. All are important communication capabilities for contested spaces.

Finally, ground vehicles may need to build a secure, range-limited vehicle area network immediately outside the vehicle, or even have infrared filtering applied to glass to contain the LiFi signal inside a VIP vehicle.

Applications for the Department of Defense

Secure Communications	• **Enclosed Spaces:** Ideal for secure communication within buildings, vehicles, or aircraft where RF signals can be easily intercepted. Field operations withing tents can be secure environments. • **Temporary Installations:** Can be set up quickly for secure communication in temporary command posts or field hospitals.
Underwater Communication	• **Submarines and Drones:** Useful for communication with underwater drones or between submarines, as RF signals are not effective underwater.
Non-Interference Environments	• **Hospitals and Labs:** Can be used in medical facilities or labs where RF interference can disrupt sensitive equipment. • **Aviation:** In aircraft where RF emissions need to be minimized.
High-Density Environments	• **Operations Centers:** Suitable for use in operations centers where multiple communication channels are needed without causing interference.
Special Operations	• **Covert Communications:** Ideal for covert operations where radio silence must be maintained, as LiFi can provide secure, short-range communication.
Augmented Reality and Virtual Reality	• **Training Simulations:** Can be used in training simulations to provide high-speed data transfer for AR/VR systems, enhancing the realism and effectiveness of training exercises.

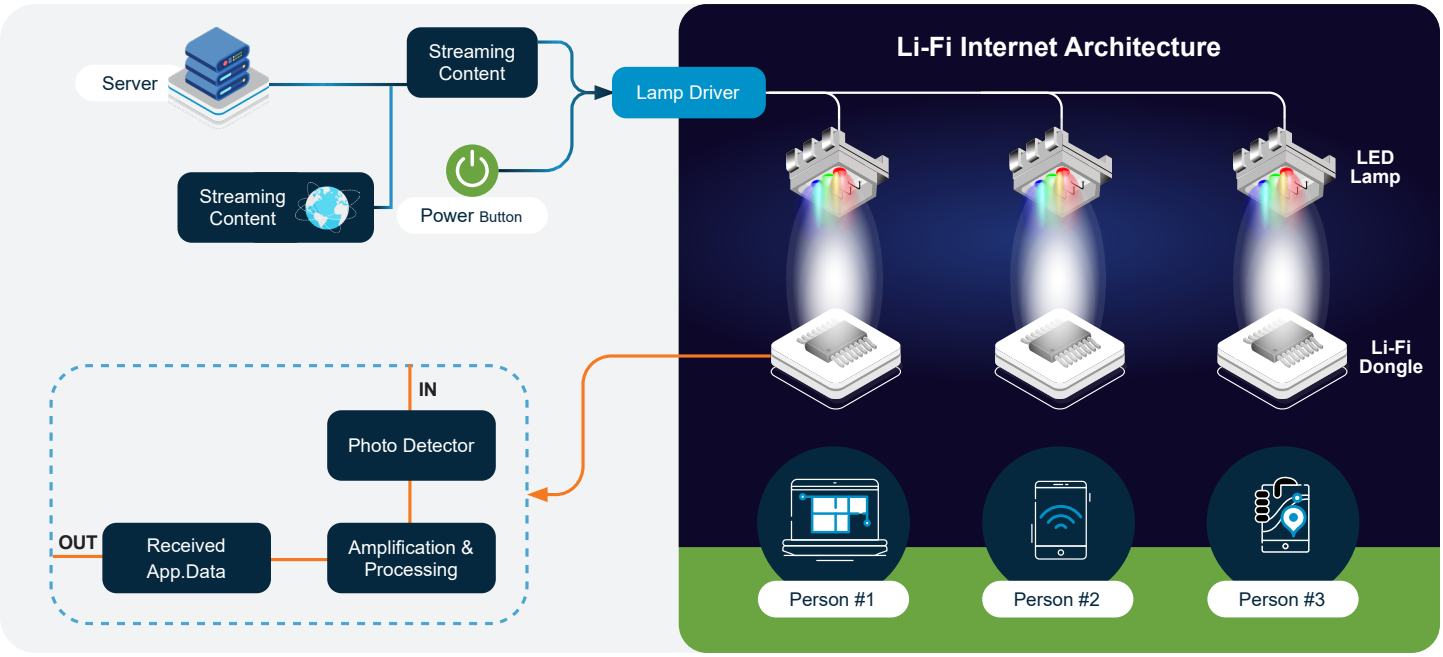

Figure 6: Baseline Reference Architecture

This is a simplistic reference architecture for a Wi-Fi deployment at a single location. Notice at the bottom, the Wi-Fi access points connect mobile devices to the wired Ethernet access switches. This in turn connect to the core building switches.

The Wi-Fi architecture needs an access point controller, DHCP services to assign IP address, DNS services for name resolution, 802.1x to drive device profiling, remediation and authorization, and finally the application servers.

The important point is that today we have a well-established IT infrastructure to support Wi-Fi communications along with staff and support policies to manage each component. In addition, most IT operations management systems have automated the provisioning of employee and guest connectivity over Wi-Fi which significantly reduces the burden of IT admins and improves the user experience.

To add LiFi to the infrastructure, we only need to add the LiFi access point devices and a centralized controller, just like for Wi-Fi. The access point is connected to the same wired Ethernet access switches and leverage the same IT infrastructure elements, policy, and staff without change. User and device provisioning remains automated and performance monitoring is baked into the solution elements.

Adding LiFi to an existing building that has power over Ethernet capabilities does not require a forklift upgrade nor cumbersome staff training. For buildings without power over Ethernet low voltage capabilities we can use powerline technology to signal over existing branch electric circuits as a slightly higher cost point due to the integration of power and Ethernet technologies. As hard as it is to believe we have a better, faster, and more secure solution at comparable costs to Wi-Fi.

Figure 7

It is easy to facilitate multi-tenant deployments in a few different models, each working seamlessly for the user community. Users from multiple agencies share a single LiFi access point to gain access to the Internet for VPN or SASE secure connectivity in a hoteling scenario.

The client traffic is encrypted so east-west traffic between users is restricted to within the tenant agency based on zero trust policies. We can also deploy LiFi access points dedicated to a specific tenant and connect the backhaul circuit to the tenant enterprise. The LiFi access points use different portions of the light spectrum, so no congestion occurs from the user perspective.

The tenant traffic is still encrypted to ensure privacy and east-to-west traffic flows are restricted to with a tenant agency once again based on zero trust policies. Finally, a single access point can use different portions of the light spectrum and assign a VLAN to each tenant to maintain traffic separation. This scenario leverages 802.1x device and user authentication and zero trust policy enforcement to implement east to west traffic flow policy and depends heavily upon the maturity level of the tenant agency.

These scenarios are deployable in both carpeted office spaces as well as industrial and tactical deployments. Based on the pilot work with the US Army, LiFi infrastructure complies with DISA WLAN STIGs making secure deployment a reality today. DISA will be updating numerous STIGS and SRGs to bring them into compliance with changes from the fifth revision of the NIST SP 800-53.

Compatibility and Integration Challenges

While all challenges are readily overcome, there are several factors to consider when deploying LiFi.

Line of Sight: Requires a direct line of sight between the transmitter and receiver.

Range: Limited to the reach of the light source, typically a few meters.

Dependency on Lighting: Needs a light source to function, which may not always be practical.

Other factors include.

- **Training and Expertise:** Introducing Li-Fi requires personnel to be trained in the principles of visible light communication (VLC) technology, including understanding how light signals are modulated, transmitted, and received. This training is crucial for engineers, technicians, and IT staff who will be responsible for installing, maintaining, and troubleshooting Li-Fi systems.
- **Infrastructure Deployment:** Installing Li-Fi infrastructure involves positioning light sources (LED bulbs or panels) strategically for optimal coverage and signal quality. This requires coordination between electricians, network engineers, and construction teams to ensure proper integration with existing lighting systems and network infrastructure.
- **Integration with Existing Systems:** Integrating Li-Fi with existing wireless networks (Wi-Fi) and IT infrastructure poses challenges related to compatibility, interference management, and seamless connectivity. IT personnel must ensure that Li-Fi networks can coexist with other technologies without compromising performance or security.
- **Security Considerations:** Li-Fi networks may introduce new security challenges, such as eavesdropping on light signals or interception of data through windows or reflective surfaces. Personnel responsible for network security must implement robust encryption protocols and monitor for potential vulnerabilities unique to Li-Fi technology.
- **Maintenance and Support:** Like any new technology, Li-Fi systems will require regular maintenance, software updates, and technical support. Personnel must be trained to diagnose and resolve issues related to signal degradation, device compatibility, and environmental factors affecting light transmission.
- **Regulatory Compliance:** Deployment of Li-Fi may involve compliance with regulatory standards related to electromagnetic interference, light intensity safety limits, and data privacy laws. Personnel must stay informed about local regulations and ensure that Li-Fi installations meet all applicable requirements.
- **Cost Management:** Managing the costs associated with Li-Fi deployment, including equipment purchases, installation labor, training programs, and ongoing maintenance, requires careful planning and budget allocation. Personnel involved in project management and finance must work together to optimize spending and ensure cost-effective implementation.

Current Market Solutions

Devices that are available today based on standard 802.11bb include the Plug&Play LiFi Cube Gateway, which is a portable LiFi access point for a table, shelf, or any off-the-shelf camera or speaker type mount.

The *LiFi@home* downlighter fits existing recessed lighting fixtures using power over Ethernet. Augmented reality headsets feature wireless connectivity with consistently high bandwidth, low latency, and low jitter. The mobile device client features chips for OEM integration which are working with Motorola devices with a sleeve.

PureLiFi can work with the GSA preferred smartphone device manufacturers to integrate the Light Antenna Module to rapidly scale mobile connectivity.

Next is the *LINXC* LiFi bridge for 5G & satellite communications to bring fixed wireless broadband through windows with LiFi to reach where mmWave & 5G can't.

Kitefin tactical access points are deployed today by the US Army. The same capability is packaged and offered to industry as shown.

Tyto Athene stands ready to support small scale pilots and proof of concepts demonstrations.

Devices Available Today

Plug & Play LiFi Cube Gateway
0% install, 100% performance. Portable LiFi access point for table, shelf or any off-the-shelf camera or speaker

LiFi@Home Downlighter Gateway
LiFi and lighting in a familiar form factor, with easy installation and networking

Augmented and Virtual Reality Headset
Wireless connectivity with consistent high bandwidth, low latency, and low jitter

Mobile Devices and Consumer Electronics
Straightforward to integrate with any 802.11 baseband for D2D, network access, high-bandwidth offload from Wi-Fi, wireless cable replacement, and more

LINXC LiFi Bridge for 5G and Satellite
Bring fixed wireless broadband through windows with LiFi to reach where mmWave and 5G cannot

pureLiFi Kitefin
System highly secure headquarters and field tactical networked LiFi in use by the US Army in world's largest ever real-world deployement of LiFi

Tyto Athene Approach to Subject Solution

Tyto continuously advances our technology and innovative approaches to deliver cutting-edge solutions that address the evolving needs of our customers. By embracing these new technologies and innovative strategies, we provide the Department with forward-thinking solutions that enhance their security posture and drive operational excellence.

Tyto has extensive experience in developing robust technology solutions that are accompanied by comprehensive systems documentation. Our processes include the creation of detailed administration manuals to ensure seamless deployment, maintenance, and scalability. Our team of skilled architects and engineers work collaboratively to produce clear and thorough documentation that covers installation procedures, configuration settings, operational guidelines, and troubleshooting steps. Our documentation is crafted to include detailed architecture diagrams, facilitating ease of understanding and future enhancements. This commitment to thorough documentation ensures that the Department has all the necessary resources to effectively manage and utilize the solution, ultimately driving greater efficiency and success in their operations.

Next Steps

The DoD can benefit greatly from the high-speed, secure, and interference-free communication that LiFi offers. As the technology matures, its applications could expand further into various strategic and operational areas, providing an edge in both communication and data security.

Product provider, OEMs, and service providers all have a part to play in evolution of LiFi solutions. Tyto Athene is an experienced system integrator who advocates for mission needs for integrability, interoperability, and future proofing over pushing a brand to mitigate business risk. Tyto Athene is ready to help with an in-depth current system evaluation to understand the specific needs and challenges your organization faces in adopting LiFi as a part of the technology stack. Engage with our networking and systems integration experts and select vendors specializing in LiFi solutions to guide the selection and implementation phases. By following a structured approach and with Tyto Athene's partnership, you can ensure a smooth transition and maintain the highest levels of data security.

About Tyto Athene

Tyto Athene, LLC, a large portfolio company of Arlington Capital Partners, was established as an IT services and solutions providers specializing in mission-focused digital transformation. Our goal is to enhance client experience and drive successful outcomes through innovative technology solutions.

As a full-service systems integrator, Tyto Athene empowers clients with the ability to make informed, timely decisions by providing secure and ubiquitous access to enterprise information across their operating environments. We leverage cutting-edge technologies, strategic innovation, and proven methodologies to deliver successful results for clients worldwide. With a full spectrum of industry-leading capabilities, substantial scale, and extensive resources, we are equipped to meet the increasingly complex demands U.S. government agencies. Supporting the rapidly evolving mission requirements of federal clients remains our top priority.

Our combination of experience and forward-thinking technology solutions gives Tyto Athene customers a distinct strategic advantage. Our primary objective is to deliver the best solutions and services available in the market to our trusted partners and clients. Tyto Athene remains committed to providing our high-quality products, superior service, and world-class technical support.

TYTO Athene

DATA TO DOMINANCE

/company/gotyto https://gotyto.com

For more information about our digital transformation services, please email bd@gotyto.com