CloseTalk CONFERENCE SYSTEM™

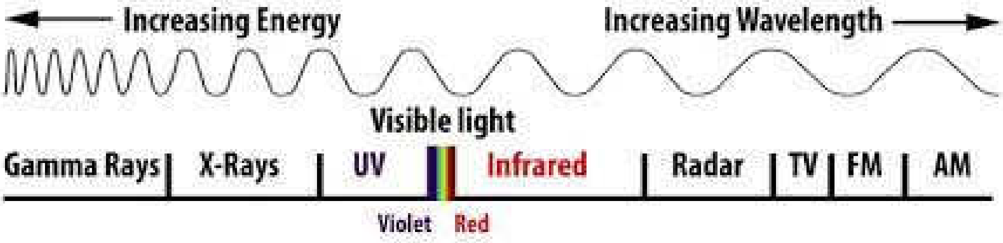
Why infrared is the safe and best choice

Date: 2014-02-17
Version: 1.04

Introduction

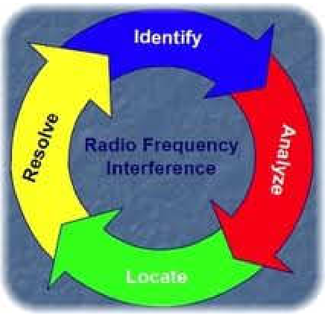
This document will discuss why infrared is the only safe wireless technology available today and why it is as safe as wired systems when used correctly. Using wireless and specifically infrared is also very convenient as this document will show.

Radio vs. light



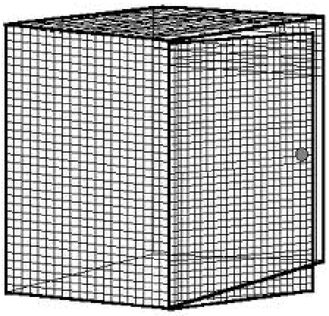
Radio and light are both parts of the same electro-magnetic spectrum but have quite different behaviour. The difference is a fairly complicated science and beyond the scope of this document, for this discussion there will only be an establishment of rules and effects concerning wireless transmission.

Radio

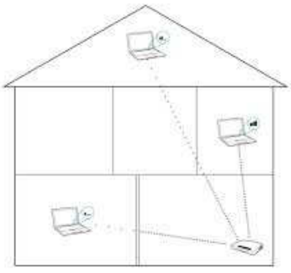


Designing a radio transmitter device is complicated and heavily regulated by national and international laws for very good reasons. The radio spectrum is limited and is shared by many different technologies and a poorly designed radio device can cause havoc with local or global radio operations. Even with correctly designed radio devices there is usually a lot of work to make them work together as the illustration to the right shows.

Controlling where and how far a radio signal travels only has one 100%-safe solution, a Faraday's Cage.



A Faraday's Cage is a "box" with electrically conductive walls that effectively shields the room from both outgoing *and* incoming radio signals. This is very convenient but also *very* cumbersome to construct. It requires a great deal of design consideration, calculations and special material which really only makes it a realistic alternative for highly special applications such as test houses and ultra-secure environments required by the military. Ultimately the room usually becomes a very dull "bunker" with no windows.



All this is naturally apparent for radio-based communication system manufacturers. To not have to require building a "bunker" and to maintain security they transmit freely and then include "encryption" of the signals, usually by using the available and ready encryption technology supplied with the electronic components they use in their design. Since the public radio spectrum is heavily regulated and inventing a proprietary radio communication technology is extremely expensive, radio-based conference system manufacturers choose market-ready technologies and components for their products and the cheapest and really the only feasible technology today is "Wi-Fi". Wi-Fi is the world-standard technology for wireless LAN, or popularly "internet" and is really intended to be used for that, the internet. As that, it is used by everyone and everything today, businesses, governments, private persons, shops, airports, smart phones, tablets, laptops,... the list is endless.

The easy-access to this technology for all types of product manufacturers is also its problem: congestion. The first generation of Wi-Fi uses 2.4GHz radio frequencies and conference systems based on this technology are already today very difficult to use in larger populated areas. To handle the general 2.4GHz congestion problem a new frequency band at 5.6GHz has been established, again for Wi-Fi, where the congestion is far less, at least today. The 2.4GHz radio-based conference systems were introduced c:a 2003-2005 and already in 2007 reports of conference system instabilities were coming in. That is just 2-4 years stability for such an expensive product! The new 5.6GHz conference systems were introduced 2012-2013, how long will it be before they become unstable?

Shortcomings of radio-based audio technologies:

- Radio-based conference systems are based on Wi-Fi, an open technology use by everyone and everything. As such they cannot guarantee operation, today and much less so in 5-10 years
- Encryption is a powerful technology but also a false sense of security. National, international and industrial espionage organisations have access to huge resources, nothing guarantees information security today, much less tomorrow. If it can be encrypted it can be decrypted
- Wireless audio is very sensitive to short interruptions, Wi-Fi is primarily designed for data transmission where this is less important and as so the radio-based conference system manufacturers are relying and depending on having exclusive access to the Wi-Fi net. This is more or less impossible to have and to control outside a Faraday's Cage
- Conference systems are in effect local audio systems and as such they require very low latency or delay in the audio signal. Streaming both audio and video over Wi-Fi is today very common and effective but they rely on buffering to handle the instabilities in the Wi-Fi signals where the end signal can be delayed several seconds relative to the source signal. This buffering is of course not possible for a real-time conference audio system, again demonstrating the extreme sensitivity to the stability of technologies based on Wi-Fi

Light

Light can easily be controlled, where it originates from and where and how far it travels. Where the characteristics of radio requires a college degree in radio technology to fully understand and more importantly, to control, the basic behaviour of light in everyday use is quite instinctive and easy to understand.

Everyone has used a flashlight at some time and with that most of the basics of light can be experienced, experimented with and actually seen. Infrared has the same behaviour, the only difference is that humans cannot see it.

Light is also an electro-magnetic wave, just as radio waves, but at much higher frequencies. As an example, *Close Talk Conference System* uses infrared light at a wavelength of approximately 875nm (nano meter or billionth of a meter), this is equivalent to 342THz (terra hertz or 343000GHz). Compare this to the new Wi-Fi frequency of 5.6GHz, this is a difference of over 60000 times. Electromagnetic waves at these frequencies moves into a new realm of behaviour as both *wave* and *particle*. As all waves, light also *reflects*, *refracts* (bends) and *diffracts* (change of direction when passing an obstacle).

So what does this mean? Well, in the scope of infrared wireless communication it boils down to some very simple rules:

- ***Reflection***
  Light will *more or less* reflect within its range, more so if the reflecting surface is *reflective* for the light colour (white walls reflect visible light better than black walls) or less so if the surface is *absorbing* for the light colour (wavelength) used
- ***Absorption***
  The light that is not reflected off of a surface is *refracted* (bent) into the material. The light will then continue through the material until it exists into a new material *or* is fully *absorbed*. If the material exhibits low absorption of the light such as window glass it will travel through and then refract again as it exits out of the glass. If the material is *high absorption* such as wood, the light will release all its absorbed energy into the material and not exit out of it. This is why a black wall gets so warm from sunlight, most of the light energy is absorbed into the material

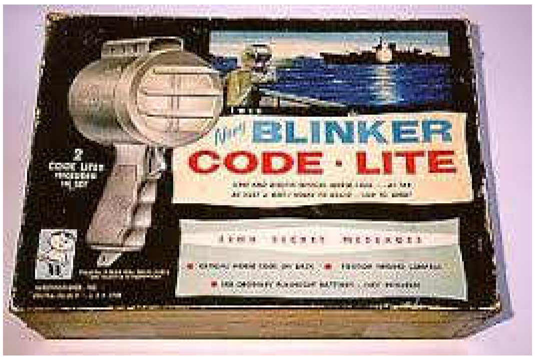
We have now reached a very important conclusion that is the key to why infrared is a superior wireless short-range technology:

- Where radio waves are *notoriously difficult* to absorb fully, i.e. control where and how far a wave travels, light is *very easy* to control. Radio waves are also subjected to absorption when it passes through a material but the much lower wavelengths causes much less absorption, that is why a radio signal can pass through a wall whereas light cannot

Now, compare a Faraday's Cage for a radio system with one for light. The one for light can be as simple as a cheap tent or more practically, a common office room. A cage for radio *must* be constructed solidly by steal or wire mesh and when you have blocked the radio signals from going out, all other signals are blocked from coming in, meaning that all other radio technologies such as mobile phones, local Wi-Fi data networks, are also disabled.

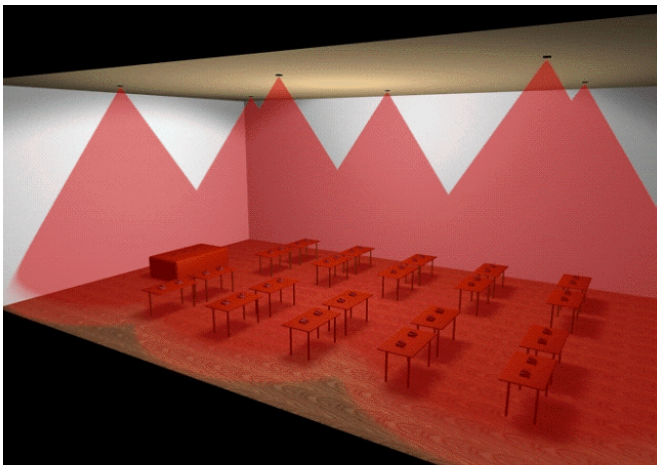
The infrared wireless technology

Sending information wirelessly over infrared can be compared to a signal lamp, the infrared emitters blink by turning on and off. The "blinking" is then received by the infrared receivers and decoded, analogous to Morse Code.



With the previous discussion in mind, it is now easy and instinctive to understand why infrared is so safe, if someone is blinking their flashlight in the office below you it is *impossible* to see or know about it, no matter how powerful eavesdropping equipment you have.

Even if the lamp used is very powerful, so powerful that the blinking can be seen indirectly by reflection through the windows it is very easy to remedy, just close the blinds, reduce the lamp power or direct it differently.



Close Talk Conference System uses a unit called a *Transceiver* to both emit and receive the light "blinking". The Transceiver is placed in the ceiling, face-down as the image to the right shows. The electric signals that powers and drives the transceiver is connected using double-shielded, industry standard CAT6 cables. The system is both CE and FCC certified. It has also been eavesdropping-verified by the head office security department from the world's largest electronics manufacturer *Samsung* using state of the art detector instruments.

This means that the only signals transmitted wirelessly in a *Close Talk Conference System* is the intended one: the infrared light.

Infrared interference

The first wireless infrared audio systems were introduced in the early 1980's. Unfortunately they quickly acquired a bad reputation due to their sensitivity to disturbance, usually by common fluorescent light. In the late 80's, early 90's, low energy lamps also became a problem.

Similar to radio, infrared transmission can also be divided into frequency bands. With light this is simply equal to how fast you "blink the lamp". The early infrared systems used very low frequencies, commonly between 30 and 100kHz which is also where the fluorescent lights emit noise. Modern infrared systems such as *Close Talk Conference System* uses much higher frequencies, between 1 and 10MHz where there are no disturbances from common appliances. Infrared remote controls, LCD, LED displays and video projectors are safe to use. Plasma displays should not be used with infrared wireless systems as they emit large amount of light noise but this is not much of a problem anymore as they are being faced out in favour of LED display technologies.

Infrared versus a cable system

Logically, an infrared conference system is the same as a cable system with the only difference being that the last 2 - 8 meters uses light instead of wire. It is also shown above that it is very easy to control light compared to radio. The conclusion is that an infrared wireless system is as safe as a wired system but adds a lot of convenience to the user such as:

- No cables on the desktop, setup the room and the delegate units freely; as desired
- Quick setup and take-down, usually no technician required
- Better reliability, cable systems connectors and cables wear out with frequent usage
- Excellent service life