



***Wi-Fi Devices
and the
Sensys™ Wireless Vehicle Detection System***

PERFORMANCE CHARACTERIZATION

Wi-Fi Devices and the Sensys™ Wireless Vehicle Detection System

The Sensys™ Wireless Vehicle Detection System relies upon radio links in the 2400 – 2483.5 MHz (2.4 GHz) unlicensed frequency band between its pavement-mounted sensors and a Sensys access point or repeater located on a nearby pole or other structure. Because this frequency band is unlicensed, it is possible that other devices operating in this band can potentially interfere with sensor-to-access point, sensor-to-repeater, or repeater-to-access point communications.

In particular, IEEE 802.11b and 802.11g (802.11b/g) Wi-Fi devices used for Wireless Local Area Network (WLAN) communications operate in the same 2.4 GHz band as the radios used by the Sensys Wireless Vehicle Detection System. As such devices have become more and more common in notebook PCs and other mobile devices and in homes, offices, and commercial establishments, they represent the most likely potential source of radio interference to deployments of the Sensys Wireless Vehicle Detection System.

Thanks to the fundamental design of the Sensys Wireless Vehicle Detection System, however, the possibility of interference with Wi-Fi devices can be easily avoided. And even if interference cannot be avoided, the impact on performance of the Sensys Wireless Vehicle Detection System is likely to be minimal because of mitigation techniques inherent in the way Sensys radio links are controlled and operated.

The 2.4 GHz Band

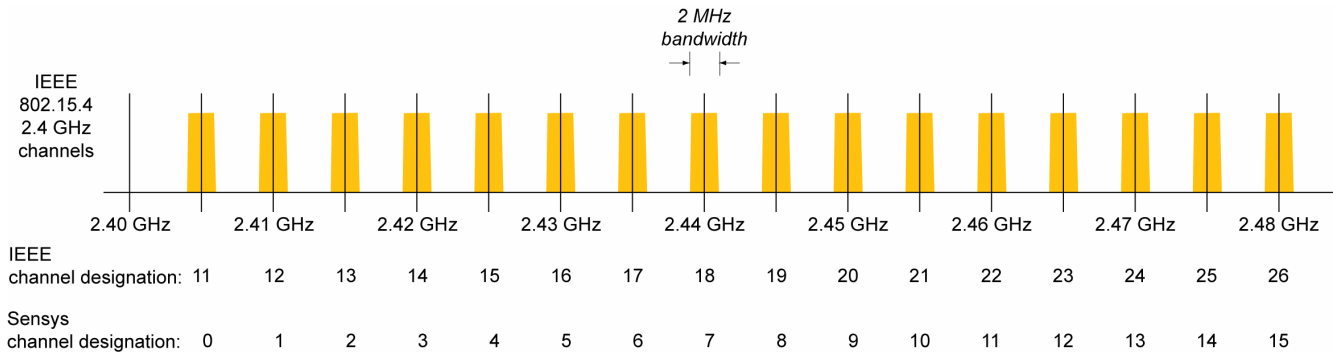
Although different jurisdictions may impose their own specific requirements governing transmit power levels and the process of type approval required to allow devices to be sold and operated, the 2.4 GHz band is the only worldwide spectrum allocation that is designated for unlicensed use without any limitations on the specific application or the transmit duty cycle. Its use of unlicensed spectrum in the 2.4 GHz band makes it possible to install a Sensys Wireless Vehicle Detection System at any location without requiring jurisdiction-by-jurisdiction regulatory approval or a site license to operate. Otherwise, access to licensed spectrum can require months, if not years, to obtain, and can be very costly in terms of legal fees and, in many jurisdictions, license fees that are escalated by competitive auctions. While use of the 2.4 GHz unlicensed band by Sensys components introduces the possibility of interference from other unlicensed devices, the advantages of license-exempt operation clearly outweigh any disadvantages.

Sensys Operation in the 2.4 GHz Band. The radios employed by Sensys wireless sensors, access points, and repeaters use commercial, off-the-shelf integrated circuits that implement the IEEE 802.15.4 PHY industry standard. This standard defines the modulation type, channel bandwidth, and other physical aspects of the radio channel to support a raw over-the-air data rate of 250 kbps in the 2.4 GHz band.

The Sensys Wireless Vehicle Detection System operates on 16 channels in the 2.4 GHz band as specified by the 802.15.4 PHY standard. Each channel is defined by its center frequency and its bandwidth, where most of the radio signal energy is present between frequencies above and below the center frequency spanning the bandwidth.

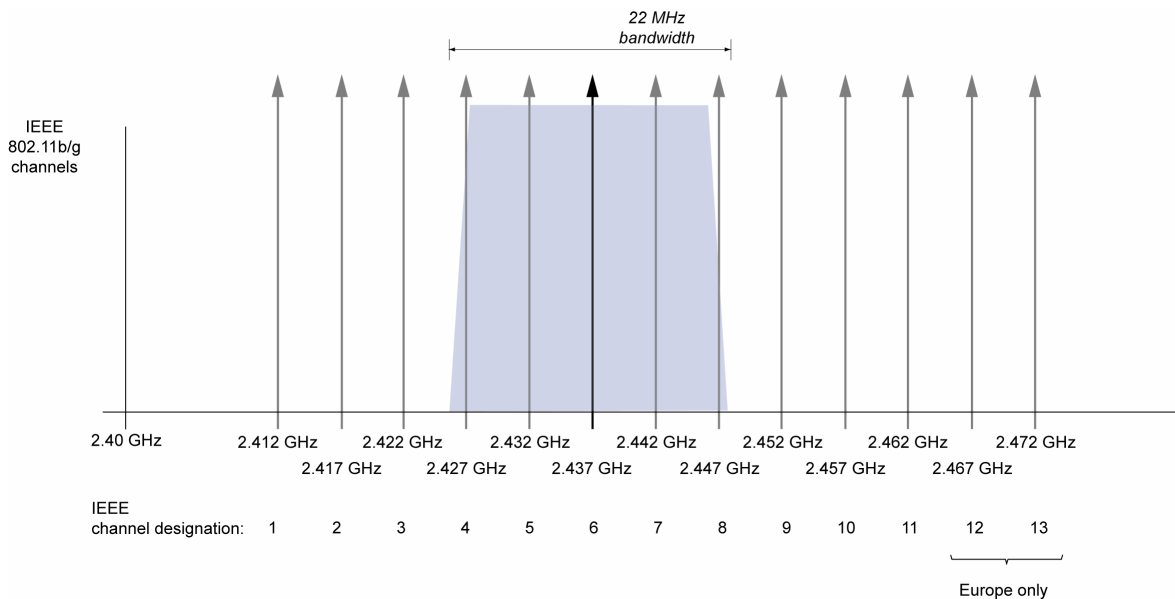
As shown in the figure below, each 802.15.4 channel occupies a nominal bandwidth of 2 MHz and is centered at 2.405, 2.410, 2.415, 2.420, 2.425, 2.430, 2.435, 2.440, 2.445, 2.450, 2.455, 2.460, 2.465, 2.470, 2.475, or 2.480 GHz. Because the 802.15.4 standard also defines frequency channels in the 900 MHz band, the 16 channels in

the 2.4 GHz band are designated by the standard as channels 11 through 26; in the Sensys Wireless Vehicle Detection System, these same channels are designated as channels 0 through 15.



16 frequency channels are available to each Sensys installation

Wi-Fi Operation in the 2.4 GHz Band. The IEEE 802.11b/g standards similarly define 14 channels in the 2.4 GHz band. Each channel is centered at 2.412, 2.417, 2.422, 2.427, 2.432, 2.437, 2.442, 2.447, 2.452, 2.457, 2.462, 2.467, 2.472, or 2.484 GHz. These channels are sequentially designated as channels 1-14, where the first 11 channels are authorized for use in North America, the first 13 are authorized for use in Europe, and the 14th channel is designated specially for operation in Japan. Each channel has a nominal bandwidth of 22 MHz, implying that, unlike the 802.15.4 channels, the 802.11b/g channels overlap each other.



802.11b/g frequency channels

The transmit power of an 802.11b/g device is typically fifty times greater than that of a Sensys radio. As a result, if an 802.11b/g device uses a frequency channel with center frequency close to the center frequency of a nearby Sensys device, then the Sensys communication link will suffer from the interference. Because of the relative bandwidths of the 802.11b/g and Sensys frequency channels, a fraction of an 802.11b/g signal's total spectral energy will interfere with each Sensys channel that it overlaps in frequency.

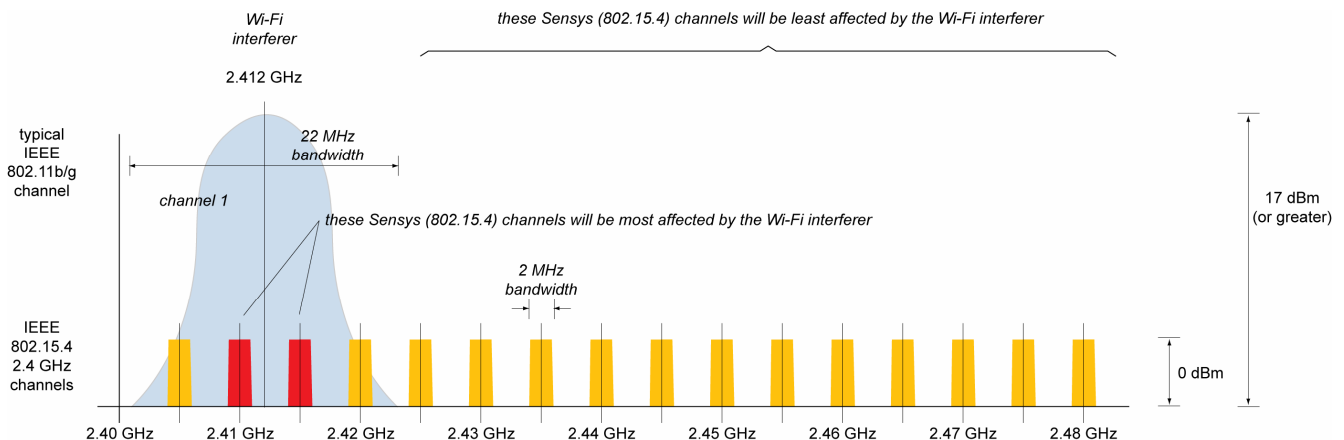
Interference Avoidance

Interference with the Sensys Wireless Vehicle Detection System can be avoided by properly selecting a Sensys installation's physical location and its operational frequency channels.

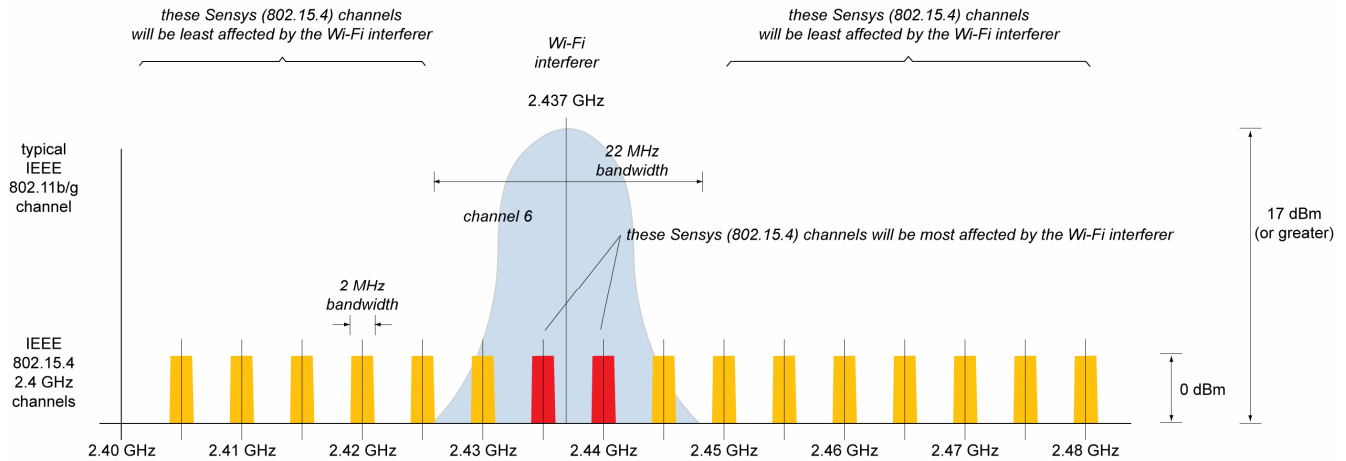
For each link between a Sensys wireless sensor or repeater and the Sensys access point, the software used in deploying a Sensys installation provides an RSSI (Receive Signal Strength Indicator) measurement of the received signal power and an LQI (Link Quality Index) figure of merit reflecting the quality of the link in a way that is analogous to its signal-to-noise ratio. At the time of installation, these values are inspected by field personnel to ensure that the selected radio channel is not subject to local interference and that no sensors are beyond the range of the access point or repeater. If interference from a Wi-Fi device is present, the RSSI and LQI values will be outside their recommended ranges. As appropriate, the access point or repeater can be moved to a different location or pointed more directly toward the sensors and/or mounted at a higher elevation; a different radio channel can be used; or, as necessary, a Sensys repeater can be employed to extend the range of the access point. Once operational, the RSSI and LQI levels of a Sensys installation can be continually monitored via the installation's system connectivity so that, if, for example, a Wi-Fi device comes close to the Sensys components, the Sensys frequency channels can be changed or other action can be taken.

Location Selection. By physically locating the Sensys wireless sensors, access points, and repeaters away from Wi-Fi devices, interference to the system can be avoided. In most cases, the presence of Wi-Fi devices will have little if any effect on Sensys wireless communications if they are at a distance of approximately 200 feet / 60 meters from each of the Sensys components. In most freeway applications of the Sensys Wireless Vehicle Detection System, the likelihood of there being a Wi-Fi device at this distance is relatively small. In some urban and suburban locations, however, it may not be possible to ensure this minimum distance between Wi-Fi devices and Sensys components. Even if 802.11b/g Wi-Fi devices are closer than recommended, interference can still be avoided by configuring the Sensys Wireless Vehicle Detection System to use frequency channels offset in frequency from the channel(s) used by the Wi-Fi devices.

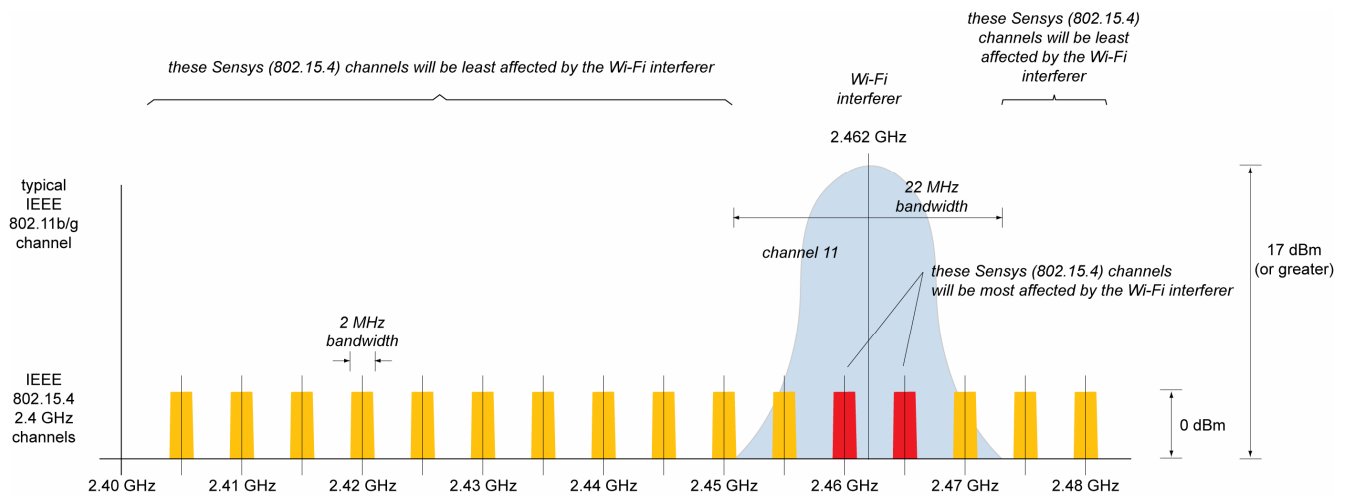
Frequency Channel Selection. With the Sensys Wireless Vehicle Detection System, one can select and configure different frequency channels for the links between the sensors and access point or repeater and between the access point and repeater. The following figures illustrate the range of Sensys frequency channel options that are available to avoid typical 802.11b/g Wi-Fi interferers.



Many Sensys frequency channels can be used to avoid a Wi-Fi interferer on channel 1....



Other Sensys frequency channels can be used to avoid a Wi-Fi interferer on a channel in the middle of the band....



Still other Sensys frequency channels can avoid a Wi-Fi interferer on channel 11, the highest frequency channel allowed in North America

As seen from the preceding figures, the Sensys Wireless Vehicle Detection System provides many frequency channels that can be used to avoid direct interference with an operational 802.11b/g channel. Even Sensys channels that are partially overlapped by an 802.11b/g channel may not suffer from interference effects – published research concerning the effects of 802.11b/g interference on 802.15.4 systems has shown that, because less radio energy is present at the edge of each 802.11b/g channel, the interference effects are minimized as long as there is a frequency offset of 7 MHz between the Sensys and 802.11b/g center frequencies. In the figures above, only the Sensys channels shown in red would be affected by the Wi-Fi interferer. For any single Wi-Fi channel actively in use, there are thus 14 Sensys channels that can be used without suffering from interference effects.

But what frequency channels should be configured for the Sensys Wireless Vehicle Detection System without prior knowledge of the frequency channels that the Wi-Fi devices will be using? The answer reflects how

frequency channels have been defined for the 802.11b/g standards. Because the 802.11b/g frequency channels overlap, Wi-Fi devices can interfere with each other if they are not configured to use channels as widely separated as possible. Given the 802.11b/g channel definitions, there are only three channels in the band that do not overlap, and these channels are the ones that are typically configured for use by Wi-Fi devices. The non-overlapping Wi-Fi channels are different in North America and Europe, however, because most of Europe allows an additional 2 channels beyond those permitted in North America.

The table below lists the four Sensys channels that are least likely to be affected by nearby operation of an 802.11b/g device in each region:

least affected channels (North America)	least affected channels (Europe)
Sensys channel 4 (center frequency @ 2.425 GHz)	Sensys channel 4 (center frequency @ 2.425 GHz)
Sensys channel 9 (center frequency @ 2.450 GHz)	Sensys channel 5 (center frequency @ 2.430 GHz)
Sensys channel 14 (center frequency @ 2.475 GHz)	Sensys channel 10 (center frequency @ 2.455 GHz)
Sensys channel 15 (center frequency @ 2.480 GHz)	Sensys channel 11 (center frequency @ 2.460 GHz)

Without knowing which specific frequency channels are actually in use by nearby 802.11b/g devices, the Sensys channels in the above table are the best choices to use for the system's wireless links.

Interference Mitigation

In the very worst case, however, it is still possible that a Sensys Wireless Vehicle Detection System installation will experience interference from nearby Wi-Fi devices. If a Sensys device is located close to a Wi-Fi device and their center frequencies almost coincide, then the radio link to the Sensys device will suffer a higher rate of data loss than normal. Even in such cases, however, normal operation of the Sensys radios can help ensure that the data is ultimately received.

In the Sensys Wireless Vehicle Detection System, the protocol that governs how data in the transmissions are formatted, sequenced, and re-transmitted in the event of error is not the 802.15.4 MAC (Media Access Control) protocol but is instead the *Sensys NanoPower (SNP)* protocol. The SNP protocol has been developed by Sensys Networks with the explicit purpose of supporting reliable data communications between Sensys wireless devices with very low latency and extremely low power consumption.

To ensure communications reliability, the SNP protocol implements an ARQ (Automatic Repeat-reQuest) protocol: after a sensor transmits data, it waits for an acknowledgement from the repeater; if an acknowledgement is not received before a timeout period elapses, the sensor assumes the transmission has failed and re-sends the data in the next time slot. Retransmissions will continue for as many as 20 times, with each Sensys wireless sensor buffering up to 16 detection events while waiting for successful transmission.

As a consequence, if nearby Wi-Fi devices have interfered with Sensys communications and have caused data to be lost, the SNP protocol can often still ultimately deliver the data without errors through retransmission. In terms of system performance, the cost of this retransmission is in terms of increased latency and increased sensor power consumption. Typically, this performance degradation will be temporary until the mobile Wi-Fi

device leaves the vicinity of the Sensys installation; if the degradation continues, the Sensys installation can be re-configured to use different frequency channels to avoid the interference.

Conclusion

Like any radio system, the Sensys Wireless Vehicle Detection System can potentially be affected by radio frequency interference. Because it operates in the unlicensed 2.4 GHz band, the most likely interferers are 802.11b and 802.11g Wi-Fi devices operating nearby. The system's design and flexibility, however, allow radio interference to be avoided and mitigate the impacts of any radio interference that may be present.

The Sensys Wireless Vehicle Detection System can operate on any of 16 different user-selectable frequency channels. Four of these channels do not overlap with the frequency channels used by Wi-Fi devices and will thus not suffer any interference effects whatsoever. If other Sensys frequency channels are used and a Wi-Fi device operating on an overlapping frequency channel is brought within range after a system has been installed, the Sensys frequency channels can be easily re-configured using the system's software, either on-site or remotely. Regardless, even if Wi-Fi interference is present, operation of the Sensys Nanopower Protocol employs retransmission to recover data that may have been lost because of radio interference, allowing the Sensys Wireless Vehicle Detection System to continue operating normally.

For more information about advanced Sensys technology from Sensys Networks, please visit www.SensysNetworks.com or contact info@SensysNetworks.com

Sensys and the Sensys Networks logo are trademarks of Sensys Networks, Inc.
All other trademarks are the property of their respective owners.

Information contained in this document is believed to be reliable, but Sensys makes no warranties as to its accuracy or completeness. Sensys reserves the right to change product specifications without prior notice.