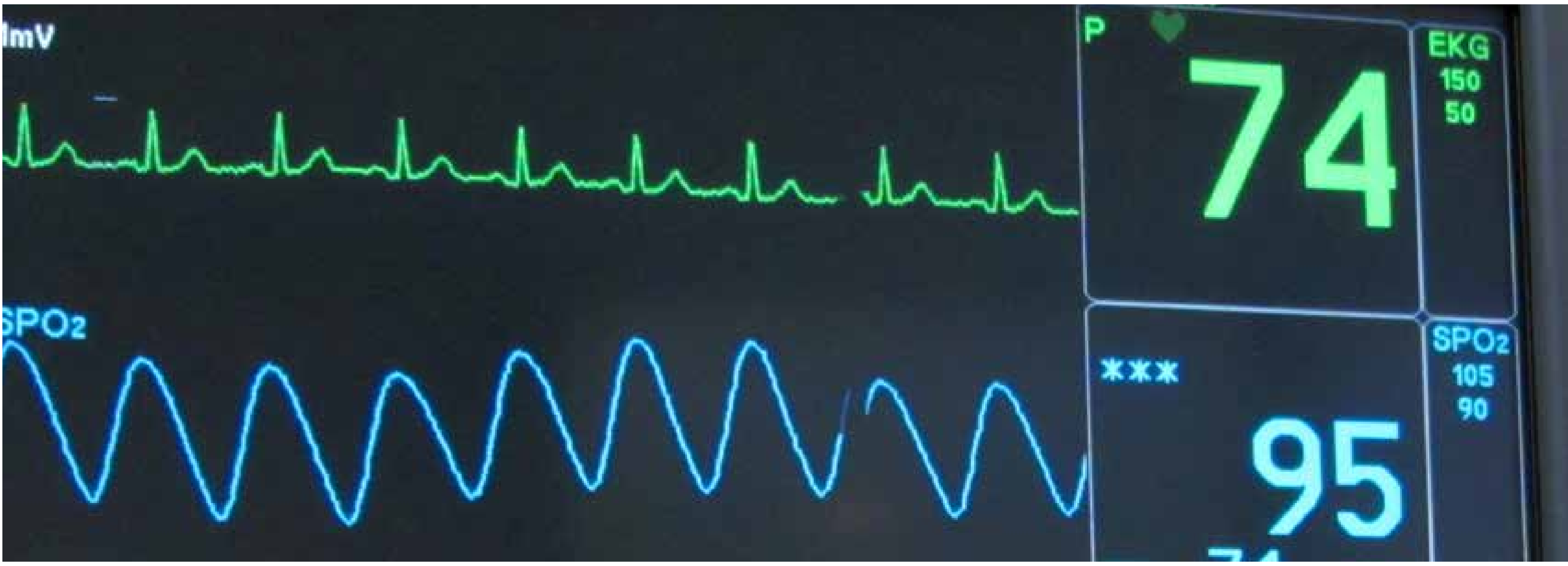
WIRELESS COEXISTANCE:

PAIRING WIRELESS MEDICAL DEVICES



Datakey®

The power of memory. Secured.

PRESENTED BY:

NEXUS
INDUSTRIAL MEMORY

EXPERTS IN RUGGED INDUSTRIAL MEMORY SOLUTIONS

Tel: +44 (0) 1794 301439
E-mail: info@nexusindustrialmemory.com
Web: nexusindustrialmemory.com

Datakey products are exclusively distributed by Nexus in Austria, Denmark, Finland, Germany, Ireland, Norway, Sweden, Switzerland and the UK.

From smart thermostats to Wi-Fi enabled dishwashers, smart, connected devices are all around us. These technologies present original equipment manufacturers (OEMs) with a variety of challenges which take on added significance when the wireless product is a medical device.

With the proliferation of wireless medical devices in-and-around medical facilities, it is critically important that wireless medical devices be able to coexist with each other and that the electromagnetic (EM) emissions from other devices not interfere with normal operation. If interference between their respective transmissions occurs, data transmitted by medical devices could be delayed or lost, potentially interfering with timely communications of critical patient information or device control commands.

This white paper gives an introduction to the topic of wireless coexistence of medical devices, including what the FDA has to say about it. It then takes an in-depth look on how to manage multiple instances of the same wireless medical device in the same proximity. Several options are discussed for linking or pairing of these wireless medical devices.

CREATING COEXISTANCE

Wireless coexistence is the ability of one wireless system to perform a task in a shared environment where other systems in that environment have an ability to perform their tasks and might or might not be using the same set of rules. A wireless medical device's performance can be limited by the amount of radio frequency (RF) spectrum available as multiple wireless devices compete for simultaneous access to the same spectrum. Coexistence testing is conducted to ensure the device isn't susceptible to EM fields being given off by other devices, like monitors, Wi-Fi signals, phones, or radio-frequency identification devices (RFID) in the area. To date, there is no set standard that addresses the risks associated with wireless coexistence for medical devices and systems. Also, most medical device manufacturers' test methods of evaluating wireless coexistence can vary greatly.

Coexistence among wireless medical devices is dependent on three main factors: frequency, space and time. The possibility of coexistence increases as the frequency separation of channels increases between wireless networks. The probability of coexistence also increases as the signal-to-interference-ratio (SIR) of the intended received signal increases. Finally, the likelihood of coexistence increases as the overall channel occupancy of the wireless channel decreases.

Although the U.S. Food & Drug Administration (FDA) does not have specific requirements for coexistence testing, the organization has issued guidance for medical device manufacturers to ensure the safety of devices they market titled, "Radio Frequency Wireless Technology in Medical Devices," issued Aug. 13, 2013.[1] Manufacturers should be prepared to test to IEC 60601-1-2 standards. When radios are incorporated into medical devices, coexistence and cyber security may need to be addressed, but specific guidance on how to perform the testing and specific test requirements is limited.

COEXISTENCE CONFLICT MANAGEMENT

To effectively manage conflicts among wireless signals and minimize disruptions in the shared wireless environment, it is important to take into account other wireless technologies and users that might be expected to be in the vicinity of the wireless medical device and test for coexistence. According to the FDA, the information addressing coexistence should include the following:

[1] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm

- A summary of the coexistence testing, set-up, findings and analysis.
- The wireless products (interferers) that were used in the coexistence testing, and their wireless RF frequencies, maximum output powers and separation distances from the device.
- The specific pass/fail criteria for this testing.
- How the device and wireless functions were monitored during the testing and determined to meet the pass/fail criteria.
- If it is reasonable to expect multiple units of the subject wireless medical device to be used in the same vicinity, the information should also address how the association and security between devices is established and maintained to prevent crosstalk among the devices.

When it will be common to have multiple instances of the same wireless devices operating in range of each other, one way to prevent crosstalk between these devices is by utilizing a linking or pairing procedure, whereby one transmitter (or transceiver) is linked or paired to one or more receivers (or transceivers).

LINKING WIRELESS DEVICES

Unlike a wired device, a wireless receiver has the potential to communicate with any like transmitter within range. With the possibility of multiple instances of both transmitters and receivers within range of each other, it is important to link each transmitter-receiver pair to ensure that the data being received is from the proper transmitter. Medical device designers have a variety of pairing methods to choose from, each having its own benefits and tradeoffs. Here are some of the possible pairing methods:

Over-the-Air Pairing

This method utilizes the same wireless communications channel to pair devices. Typically, the two devices are put into pairing mode and ID information is transferred/exchanged over the wireless channel. Because it would be possible for multiple units within communications range to be put into pairing mode at the same time, additional confirmation steps should be required to prevent an accidental pairing. This confirmation could vary in complexity depending on the types of operator inputs and display outputs available on the two devices. It could be as simple as a push button and LED to a more complex solution like entering a PIN code that was displayed on the other device. The more complex the operator interface, the more robust the pairing process can be.

Dedicated Wireless Pairing Channel

Whereas the previous method utilized the same wireless channel for pairing as the primary communications channel, an alternative would be to have a separate wireless channel that is solely dedicated to the pairing function. Some common examples would include Near Field Communications (NFC), infrared (IR) communications or RFID. With this method, once in pairing mode, the two devices to be paired must be brought together in close proximity. Once this communications channel has been established, ID information may be transferred/exchanged.

Having a dedicated pairing channel may be a preferred option for devices with no or limited operator interfaces. Because of the close proximity required during the pairing process, the chances of accidental pairings is greatly reduced. The drawback of this close proximity requirement is that it would not be ideal for large or fixed devices.

Pairing Cable

Using a pairing cable to physically connect the two devices to be paired eliminates the possibility of accidental pairing. Once the two devices to be paired are connected by the cable, ID information can then be transferred/exchanged. As was the case with a dedicated wireless channel like NFC or IR, using a pairing cable may not be ideal for large devices or those that have a fixed/permanent installation.

Pairing Using Portable Memory

Like the pairing cable eliminates the possibility of accidental pairings, using a portable memory device also does this, as the portable memory device is deliberately transferred from the receiver to the transmitter and back to the receiver (for example). The ID information for the devices is written to the non-volatile portable memory device and read by the device to be paired. This method has the benefit of eliminating accidental pairings, but can be used with large or fixed devices, as the small memory device is easy to walk across the room. One additional benefit of using portable memory is that it makes it easy to pair multiple devices. For example, it might be beneficial to be able to send data from a medical instrument to be displayed on multiple monitors for medical personnel to see.

Table 1, below, summarizes the capabilities of the various pairing methods:

	ADDITIONAL PAIRING CHANNEL NEEDED	OPERATOR INTERFACE NEEDED	IDEAL FOR LARGE/ FIXED DEVICES
“Over-the-Air” Pairing	NO	Complex	YES
Dedicated Wireless Pairing Channel	YES	Simple	NO
Pairing Cable	YES	Simple	NO
Pairing using Portable Memory	YES	Simple	YES

Table 1 – Pairing methods compared

A CLOSER LOOK AT PAIRING USING PORTABLE MEMORY

As discussed above, using portable memory to link wireless medical devices has certain advantages over the other pairing methods. Refer to the figures below to see how portable memory can be used to pair wireless medical devices.

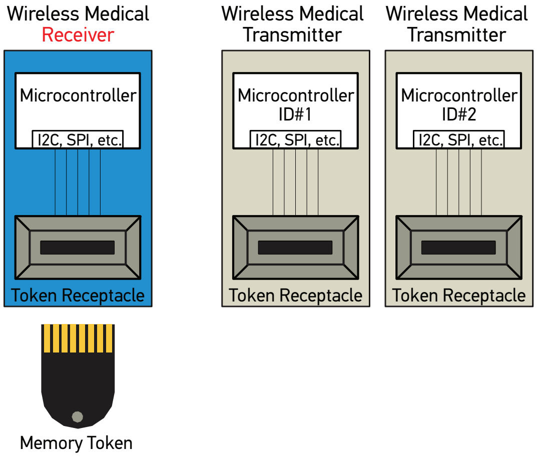


Figure A – Memory token is removed from its receptacle on the wireless receiver.

Figure A shows a wireless medical receiver with multiple wireless medical transmitters. All of the medical devices have receptacles that accept a portable memory token. The token normally resides in the receiver. When medical personnel wish to link a particular transmitter to the receiver, the memory token is removed from the receiver and inserted into the receptacle of the transmitter as shown in Figure B. The insertion of the token can be used to initiate pairing mode.

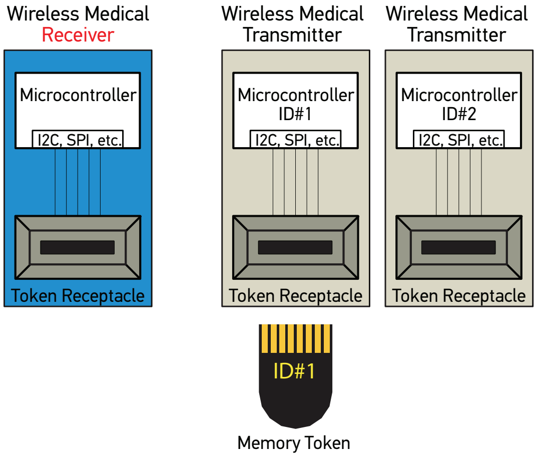


Figure B – Memory token is inserted into the target transmitter.

A memory token is inserted into the medical transmitter where its ID code is written to the memory token.

The ID code for that transmitter is written to the non-volatile memory inside the memory token. The memory token is then removed from the transmitter and inserted into the receiver as shown in Figure C.

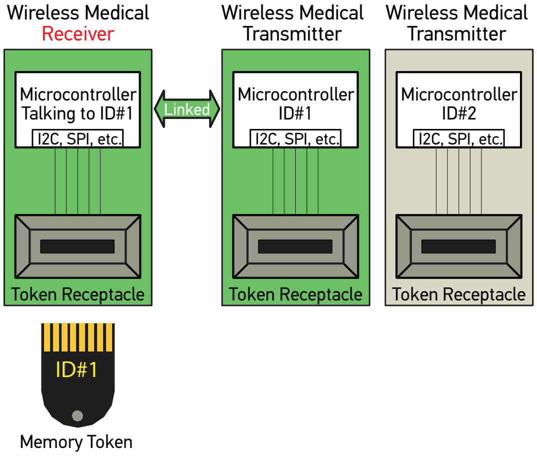


Figure C – With the ID of the transmitter known, the receiver is now properly linked.

The receiver reads the transmitter's ID code off of the memory token and a positive communication link is established.

THE LINK TO COEXISTENCE

Wireless medical devices can eliminate wires in the operating room and can free patients from being tethered to monitoring equipment. As more and more wireless medical devices are implemented in hospitals, it is more important than ever to ensure that these wireless medical devices are able to coexist with each other. Designing and testing for wireless coexistence can prevent the likelihood of data transmitted from these devices from being lost or delayed. Designers can ensure coexistence between multiple instances of the same device by pairing transmitter and receiver.

WIRELESS COEXISTENCE CASE STUDY

Stryker Corporation is one of the world's leading medical technology companies. The company produced the first high-definition endoscopic digital camera and was also the first to market a wireless platform for transmitting high-definition video in the operating room. Its WiSe™ Wireless Platform includes HD cameras, wireless HDTV transmitters, wireless receivers and HDTV surgical displays. When designing the WiSe™ Wireless Platform, engineers at Stryker needed to ensure that the wireless devices would coexist with other WiSe™ systems located nearby.

Stryker's WiSe™ HDTV Transmitter and WiSe™ HDTV Surgical Display allow surgical video captured by HD camera systems, as well as video signals from other devices like surgical robots and radiology devices, to be transmitted wirelessly and displayed remotely in high definition. The wireless connection allows operating room personnel to position the remote monitors in their desired locations without having to account for lengthy video cables. The WiSe™ system even allows video from a single camera to be shown concurrently on multiple displays.

"With WiSe™ systems, it is important for us to ensure that a transmitter and display are linked intentionally," said John Shen, Senior R&D Manager for Stryker. "That is, we needed to make sure that a transmitter or display didn't accidentally link to a display or transmitter in a different operating room. With the wireless signals penetrating walls, ceilings and floors, it was important to ensure intentional linking, both for accuracy and for HIPAA compliance."

Portable Memory Establishes Link

To ensure that there is an intentional link between a WiSe™ HDTV Transmitter and a WiSe™ HDTV Surgical Display, Stryker chose to use a portable memory device to carry link information from the transmitter to the receiver (display). In selecting a portable memory solution, Stryker wanted a memory device with the following characteristics:

- Long-term Availability
- Proven Technology
- Proven Manufacturer
- Simplicity of Design
- High Reliability
- High Durability
- Security

Stryker reached out to ATEK Access Technologies and selected its Datakey extended SlimLine™ memory token. For the mating receptacle, Stryker selected the SR4210 panel-mount receptacle. Together, this system met all of the characteristics Stryker was looking for.

"We didn't want to use a consumer memory device, like an SD card or a USB flash drive, due to the possibility of loss/misuse, as well as the fact that it is difficult to support all of the variations of these devices," said Shen.

A Best-in-Class Solution

The memory token utilizes solid over-molded construction, so the memory IC is completely encased in a durable, custom composite material. This makes the memory token impervious to liquids and long lasting. The tokens can even be sterilized by an autoclave or via an EtO gas process, although not a design requirement for Stryker, as both the display and the transmitter are used outside the sterile zone.

In addition to the token, the receptacle is also very durable. Its contacts are rated for 50,000 insertion-and-removal cycles, which ensures that a receptacle should never wear out during the life of the transmitter/display. As a point of comparison, a typical USB receptacle is only rated for 1,500 cycles.

Since 2009, the WiSe™ Wireless Platform by Stryker has been allowing hospitals to confidently view live video from surgeries without the pitfalls of video wires. In 2013, Stryker launched SYNK®, its second generation wireless platform, which also uses Datakey SlimLine memory tokens.

"We had great luck with Datakey tokens in the WiSe Wireless Platform," said Jake Thiede, Product Manager for Stryker Endoscopy. "We've definitely prevailed as best-in-class in terms of wireless video systems in the OR with the WiSe platform."

WiSe is a trademark of Stryker Corporation. SYNK is a registered trademark of Stryker Corporation.

Datakey®

The power of memory. Secured.

Wireless Coexistence:
Pairing Wireless Medical Devices

WHITE PAPER