VIATOR® *Bluetooth*® Interface

Industrial Use Application Note

September 2008

AT1100000TAB

Introduction

The MACTek VIATOR® ***Bluetooth*** Interface is a wireless point-to-point HART® PC modem for temporary connections with HART field devices. This Application Note discusses some of the issues and concerns with using VIATOR ***Bluetooth*** Interface in industrial environments and covers topics such as RF range, interference, coexistence issues, security and HART compatibility.

VIATOR Bluetooth Radio Specification

Item	Specification
Bluetooth	Version 2.0 EDR, Class 1. Also works with ***Bluetooth*** 1.1, 1.2
RF Range	100 meters (open air)
Frequency	2402 – 2480 MHz
Modulation	FHSS/GFSK
Channel Intervals	1 MHz
RF Channels	79 Channels
RF Data Rate	721kbps – 2.0Mbps
RF Receive Sensitivity	-80dBm typical
RF Transmit Power	18dBm (63mW). ***Bluetooth*** Class 1
Antenna	Integrated Omni-Directional
Encryption Key Size	56-bit

Range

The MACTek VIATOR ***Bluetooth*** Interface is a ***Bluetooth*** Class 1 device and has a range of 100+ meters in an open air environment. Internal testing at MACTek has shown ranges exceeding 125 meters with reliable HART communication in an outdoor open air environment.

Radio range is highly dependent on the environment that the device is being used within. Typical industrial settings have large amounts of metal and obstacles that can greatly affect the range you can expect to get. A general rule of thumb for getting long range is to not have obstacles in the path between the PC (acting as the ***Bluetooth*** host) and the MACTek VIATOR ***Bluetooth*** Interface. If obstacles are in the path, the ***Bluetooth*** connection may still work but only at a shorter range.

Range is also highly reliant on the ***Bluetooth*** Adapter used on the PC. Many ***Bluetooth*** USB adapters and laptops with built-in ***Bluetooth*** are only rated for ***Bluetooth*** class 2, which has a range of only 10 meters. The MACTek VIATOR ***Bluetooth*** Interface will certainly work with these adapters, but the range will be limited to the 10 meters range of the adapter. To get the best possible range, be sure to use a ***Bluetooth*** Class 1 adapter on your PC.

Interference Susceptibility

One of the main concerns people have when using RF devices in an industrial setting is how susceptible the device is to interference from other devices. No RF device can guarantee 100% reliability, but ***Bluetooth*** uses several techniques that make it ideally suited for use in industrial environments that have a large amount of RF interference.

Bluetooth in inherently more robust than most other 2.4GHz protocols, including WiFi and Zigbee, since it is a Fast-Frequency Hopping Spread Spectrum (FHSS) system. FHSS systems were originally developed by the military since they are highly resistant to jamming and very difficult to intercept. Many other protocols are fixed-channel and are more sensitive to interference.

The FHSS mechanism that ***Bluetooth*** uses splits the 2.4GHz ISM band into 79 1MHz wide channels, and hops between them every 625us in a pseudo-random fashion. The RF energy Class 1 ***Bluetooth*** uses to transmit (+18dBm) is concentrated into this small narrowband 1 MHz channel, and the ***Bluetooth*** receiver tends to reject most RF energy outside of this small band. Therefore, to interfere with ***Bluetooth*** you have to have very high RF energy on a particular small frequency band at the right time.

Bluetooth also adds automatic error correction and packet retries at the very low level. At a higher level, the MACTek VIATOR ***Bluetooth*** Interface is built upon the RFCOMM / SPP ***Bluetooth*** profile, which adds things like high level protocol retries and timeouts. These profiles also guarantee that the data sent is received by the other end in order and not corrupted. The data rate of ***Bluetooth*** is several orders of magnitude higher than HART, which allows for numerous low level retries to get the data through if needed.

Coexistence

Another large concern in industrial settings is how well a particular RF device will coexist with other RF instruments in the environment. Some FHSS type systems (such as cordless phones) tend to cause interference with other RF devices since they have a high data rate and will indiscriminately hop onto an RF channel already in use. Early implementations of ***Bluetooth*** were also shown to cause interference when located very close to WiFi radios (less than 1 meter) and transmitting at a high data rate.

In ***Bluetooth*** version 1.2, Adaptive Frequency Hopping (AFH) was incorporated to help to reduce interference caused to other RF devices. Adapter Frequency Hopping detects which channels have RF energy on them and will avoid hopping through them. So in the case of a WiFi network being in the same airspace, the ***Bluetooth*** network will detect this and choose not to use these channels. The MACTek VIATOR ***Bluetooth*** Interface is compliant with version 2.0 of the ***Bluetooth*** specification and includes support for Adaptive Frequency Hopping

Note: In order to use Adaptive Frequency Hopping, the ***Bluetooth*** adapter on the host PC must be ***Bluetooth*** version 1.2 or higher.

The HART data rate is very low (1200 bps) and HART packets tend to be fairly short (10 – 30 bytes). This is several orders of magnitude lower than the ***Bluetooth*** transmission rate (721 kbps – 2.0Mbps). To send and receive HART data using the MACTek VIATOR ***Bluetooth*** Interface the ***Bluetooth*** radio is typically used less than 2% of the time.

The possibility of interference to other RF devices caused by the MACTek VIATOR ***Bluetooth*** Interface is extremely low, due to the use of ***Bluetooth*** Adaptive Frequency Hopping and the very low data rate of the HART messages being sent over the air.

Security

Bluetooth is a very secure protocol and includes several features that make it very difficult to intercept. The MACTek VIATOR ***Bluetooth*** Interface has to be authenticated with a PIN code

that the user enters when connecting to it and all data sent over the connection is encrypted with a unique key formed during the connection process.

The FHSS mechanism used by ***Bluetooth*** is also very useful for security purpose since the hopping pattern is known only to the transmitter and the receiver and only synchronized receivers are able to receive all the data. The FHSS technique used in ***Bluetooth*** hops over up to 79 channels 1600 times per second, making it nearly impossible to intercept all the packets without being synchronized.

Note: HART data transmitted on the 4-20mA current loop in not encrypted, nor is it encrypted on the PC host system that it is being used on. The security mechanism described is only used by the ***Bluetooth*** RF connection.

HART Compatibility

The MACTek VIATOR ***Bluetooth*** Interface builds upon the industry leading VIATOR family of HART Interface products and is fully compliant with the HART physical layer requirements.

The HART data-link layer protocol is very timing specific and was originally designed to be used with RS-232 type serial interfaces where timing could be well controlled. One of the major requirements of the HART protocol is that there cannot be gaps between bytes that exceed 9.2 milliseconds. Because of other possible connected ***Bluetooth*** devices and RF retries, the gaps between packets on a ***Bluetooth*** connection can easily exceed this number.

The MACTek VIATOR ***Bluetooth*** Interfaces uses several techniques to guarantee HART data-link layer compliance even with very large delays caused by the ***Bluetooth*** connection. This keeps a reliable HART connection even near the maximum RF range or in the presence of a large amount of RF interference. These techniques also ensure that the HART data on the 4-20 mA loop complies with the HART protocol timing and is exactly what is sent from your HART application.

References

Andersson, M., “Using ***Bluetooth*** in an Industrial Environment,” Reliability and Robustness, ConnectBlue AB, Sweden, Dec 2000

Koumpis, K., Hanna, L,. Andersson, M., Johansson, M., “Wireless Industrial Control and Monitoring beyond Cable Replacement,” PROFIBUS International Conference, June 2005

Kjesbu, S., Endresen, J., “***Bluetooth*** in Industry”, ABB Corporate Research AS, May 2000

Lucan, V., “***Bluetooth*** with Industrial Computers,” Tampere University of Technology Thesis, Dec 2004

Andersson, M., “Industrial Use of ***Bluetooth***,” ConnectBlue AB, Sweden, educational web page, May 2001.
http://www.connectblue.com/fileadmin/Connectblue/Web2006/Documents/White_papers/Industrial_Bluetooth.pdf

HP. Wi-Fi and ***Bluetooth*** – Inteference Issues, education web page, Jan 2002
http://www.hp.com/rnd/library/pdf/WiFi_Bluetooth_coexistance.pdf