Factory Automation Wireless Networks Cheat Sheet

by [deleted] via cheatography.com/2754/cs/11851/

Introduction

Credit: http://www.electronicdesign.com/industrial/factory-automation-banks-wireless-and-ai-technology-succeed

IEEE 802.15.4

IEEE 802.15.4 is designed to support peer-to-peer links as well as wireless sensor networks. The standard defines the basic physical layer (PHY), including frequency range, modulation, data rates, and frame format, and the media-access-control (MAC) layer. Separate protocol stacks are then designed to use the basic PHY and MAC. Several wireless standards use the 802.15.4 standard as the PHY/MAC base, including ISA100a, Wireless HART, ZigBee, and 6LoWPAN.

The standard defines three basic frequency ranges. The most widely used is the worldwide 2.4-GHz ISM band (16 channels), which has a basic data rate is 250 kb/s. Another range is the 902- to 928-MHz ISM band in the U.S. (10 channels). The data rate is 40 or 250 kb/s. Then there's the European 868-MHz band (one channel) with a data rate of 20 kb/s.

All three ranges use direct sequence spread spectrum (DSSS) with either binary phase-shift-keying (BPSK) or offset quadrature phase--shift-keying (QPSK) modulation. The multiple-access mode is carrier sense multiple access with collision avoidance (CSMA-CA). The minimum defined power levels are –3 dBm (0.5 mW). The most common power level is 0 dBm, while a 20-dBm level is defined for longer-range applications. Typical range is less than 10 meters.

6LoWPAN

Developed by the Internet Engineering Task Force (ITEF), 6LoWPAN provides a way to transmit IPv6 and IPv4 Internet Protocols over low-power wireless point-to-point (P2P) links and mesh networks. The 6LoWPAN standard (RFC4944), which is short for IPv6 protocol over low-power wireless PANs, also permits the implementation of the Internet of Things on even the smallest and remote devices.

The protocol provides encapsulation and header compression routines for use with 802.15.4 radios.

If your wireless device must have an internet connection, this is your technology of choice.

Cellular

With services from most network carriers, cellular radio provides data-transmission capability for machine-to-machine (M2M) applications. M2M is used for remote monitoring and control. Cellular radio modules are widely available to build into other equipment. Older 2G and 3G modules are now being replaced by 4G LTE modules such as NB-IoT. The working range is from 1 to 10 km, which is the range of most cell sites today.

Dust Networks

Dust Networks was acquired by Linear Technology, which in turn was acquired by Analog Devices. Its SmartMesh technology is based on the 802.15.4 and 6LoWPAN standards. The prime benefit of this technology is its ability to form ad hoc, self-repairing mesh sensor networks that increase range and reliability. Other key features are its 10,000-hour battery-lifetime modules and NIST-grade AES-128 security.

SmartMesh networks communicate using a time-synchronized channel-hopping (TSCH) link layer, a technique whereby all nodes are synchronized to within a few microseconds. Network communication is organized into TDM time slots that permit channel hopping and full path diversity. They also offer a version of a HART wired network called WirelessHART (see below).

ISA100a

Developed by the International Society of Automation, ISA100a is designed for industrial process control and factory automation. It uses the 802.15.4 PHY and MAC, but adds special features for security, reliability, feedback control, and other industrial requirements.

ISM Band

Most of these standards use the unlicensed ISM bands set aside by the Federal Communications Commission (FCC) in Part 15 of the Code of Federal Regulations (CFR) 47. The most widely used ISM band is the 2.4- to 2.483-GHz band, which is used by Wi-Fi, Bluetooth, 802.15.4 radios, and many other devices. The second most widely used band is the 902- to 928-MHz band, with 915 MHz being a sweet spot. Modulation is typically ASK/OOK or FSK. Other popular ISM frequencies are 315 MHz for garage-door openers and remote-keyless-entry (RKE) applications, and 433 MHz for remote temperature monitoring..

RFID

Radio-frequency identification (RFID) is used primarily for identification, location, tracking, and inventory. A nearby reader unit transmits a high-power RF signal to power passive (unpowered) tags and then read the data stored in their memory.
RFID tags are small, flat, and cheap, and can be attached to anything that must be tracked or identified. They have replaced bar codes in some applications. RFID uses the 13.56-MHz ISM frequency, but other frequencies are also used, including 125 kHz, 134.5 kHz, and frequencies in the 902- to 928-MHz range. Multiple ISO/IEC standards exist.

Wi-Fi

Wi-Fi is the commercial name of the wireless technology defined by the IEEE 802.11 standards. Next to Bluetooth, Wi-Fi is by far the most widespread wireless technology. It's in smartphones, laptops, tablets, and ultrabooks, as well as TV sets, video accessories, and home wireless routers. On top of that, it's deployed in many industrial applications. Wi-Fi is now showing up in cellular networks, where carriers are using it to offload some data traffic like video that clogs the network.
The initial version, called 802.11b, was popular because it offered up to 11-Mb/s data rates in the 2.4-GHz ISM band. Since then, new standards have been developed including 802.11a (5-GHz band), 802.11g, and 802.11n using OFDM to get speeds up to 54 and 300 Mb/s under the most favorable conditions.
More recent standards include 802.11ac, which uses multiple input, multiple output (MIMO) to deliver up to 3 Gb/s in the 5-GHz ISM band. Wi-Fi is readily available in chip form or as complete drop-in modules. The range is up to 100 meters under the best line-of-sight conditions. This is a great option, where longer range and high speeds are needed for the application.

Wireless HART

HART is the Highway Addressable Remote Transducer protocol, a wired networking technology widely used in industry for sensor and actuator monitoring and control. Wireless HART is the wireless version of this standard. The base of it is the 802.15.4 standard in the 2.4-GHz band. The HART protocol is a software application on wireless transceivers.

ZigBee

Emanating from the ZigBee Alliance, this software protocol and technology uses the 802.15.4 transceiver as a base. It provides a complete protocol stack designed to implement multiple types of radio networks that include point-to-point, tree, star, and point-to--multipoint. Its main feature is the ability to build large mesh networks for sensor monitoring. And, it can handle up to 65,000 nodes.
ZigBee also provides profiles or software routines that implement specific applications for consumer home automation, building automation, and industrial control. Examples include building automation for lighting and HVAC control, as well as smart meters that implement home-area-network connections in automated electric meters. ZigBee is widely used in factory automation and can be used in other M2M and Internet of Things applications as well.