A basic system has a Star topology where Wireless Sensor Transceivers are two-way communicating with a network controller – the Control Panel, either directly or through wireless range extenders. In a standalone system configuration the Control Panel is typically connected to a commercial SCADA system or a standard industrial controller (PLC), utilizing the industry standard MODBUS protocol (MODBUS RTU or MODBUS TCP/IP). All basic installation, maintenance and monitoring functions are performed by or via the Control Panel using simple and friendly to use user interface. The Wireless Sensor Transceiver family connects to a variety of industrial sensors, for the purpose of remote wireless monitoring and control. A robust and efficient wireless link is the basis to migrating from cabling to wireless data collection, or in some cases for starting to monitor data at points where it was not previously feasible. The Wireless Sensor Transceiver includes a superior performance two-way radio with an internal antenna, and is compact and unobtrusive. Designed for ultra-low power consumption, it combines long range and reliable communication with long battery life. Device registration, configuration, control and monitoring, are done remotely by the system so that field programming is not required. Upon activation, the transceiver begins to sample and transmit data, with the following options:

1. Readings transmitted at specified time intervals
2. Readings transmitted at scheduled times
3. Remote interrogation for on-demand reading of the sensor

Concerning compliance with 15.247(a)(1):

1. The system is a star-topology, time-synchronized network.
2. The network comprises one network coordinator (control panel) that generates free running system clock based on 32,768Hz crystal (i.e. clock tick equals ~30 microsecond).
3. The system clock is utilized with 32 bits counter. This means that the system clock rolls over every 1.5 days.
4. The local clock at every end-node (device) in the network is time-synchronized with the system clock to within +/- 2 ticks (i.e. +/-60 microsecond).
5. The timeline of the network is divided into time-slots. The duration of one time-slot is 15.6 millisecond. This means that there are 64 time-slots every second
6. At the beginning of every time-slot, every element of the network (i.e. network-coordinator and all end-nodes) calculates the proper frequency channel for that time-slot. This means that system switches frequency channel 64 times every second.
7. The bandwidth of a frequency channel (receiver bandwidth) is set to ~130KHz. The bandwidth is selected to be ~130KHz to accommodate ~100KHz signal bandwidth (50kbps, GFSK modulation and 25KHz deviation yields an effective bandwidth of ~100KHz and 20dB bandwidth of ~129KHz)

8. Every element in the network (network-coordinator and all end-nodes) calculates the proper frequency channel in the following way:
    8.1. The system clock is first AES-128 encrypted. Then the proper frequency channel is derived as a function of the encrypted system clock.
    8.2. Since the system clock rolls over every 1.5 days, the hopping sequence is 1.5 days long.
    8.3. Since the frequency channel number is a function of the encrypted system clock (and since the system clock changes constantly) the hopping sequence is both pseudo-random and evenly distributed (this is a fundamental concept in encryption theory, otherwise, the encryption would have been useless)

Concerning compliance with 15.247(g) and 15.247(h):

1. The system is a star-topology, time-synchronized, time-slotted network
2. The system comprises one network-coordinator (control panel) and multiple end-nodes (devices).
3. Each end-node has an attached sensor. The end-node wakes up periodically (typically every 10s seconds) and samples the sensor. After sampling the sensor, the end-node selects the next available time-slot and transmits a short burst (message) comprising the data sampled from the sensor (the message is less than one time-slot length, i.e. less than 15.6 milisecond length)
4. The short burst is sent at the proper frequency channel, the one associated with the time-slot in which the message is sent.
5. The system uses **50** frequency channels. The hopping sequence is 1.5 days long, and since it derived as a function of the **encrypted** system clock it is both **pseudo-random** and **evenly distributed**. Over time, both transmissions from a certain end-node and the overall transmissions from all end-nodes are both **pseudo-random** and **evenly distributed**.
6. No coordination of frequency hopping systems, in any manner, for the express purpose of avoiding the simultaneous occupancy of individual hopping frequencies by multiple transmitters is incorporate in the system.