Sure Cross® Wireless Security and Data Integrity

Overview

The three most critical concerns regarding wireless I/O systems are:

- Network Security
- Data Security
- Data Integrity and Control Reliability

The Banner Sure Cross wireless systems were designed with these issues at the forefront. The SureCross wireless I/O systems provide a level of security, data integrity, and reliability far exceeding most wireless systems on the market today.

This technical note describes the concepts of network isolation, binding, setting a default output state, frequency hopping, restricted access, generic data transfer without context, and link health monitoring. These concepts, built within a proprietary protocol, provide a high level of security and data reliability. The Sure Cross system is an ideal choice for secure data monitoring and reliable control.

Network Security

Network security is an important issue for most organizations. No system can allow a hacker access to the company's internal information network. The Banner Sure Cross wireless systems are designed to completely eliminate all Internet Protocol (IP) based security threats.

- Closed, proprietary network; physical access is required to join (binding) the network
- No login, no port to access, no method of access through the wireless network
- There is no operating system; the DXM runs embedded firmware that has no facilities to gain access to other connected devices

Open protocols such as Wi-Fi can, if not managed correctly, provide hackers unfettered access to your organization's most critical data. Malicious TCP/IP packets and programs can cause grave security breaches and could cause the loss or theft of critical information. This is because standards-based network components such as Wi-Fi access points have the potential to route any and all data packets, which is why these systems use encryption, passwords, firewalls, and antivirus software.

Banner's Sure Cross systems, however, do not pose a security threat to the network because the Sure Cross system cannot physically route malicious TCP/IP packets. The Sure Cross protocol only carries sensor data values. It is not possible to gain access to the organization's main network through the Sure Cross wireless system and it is not possible for the Sure Cross wireless system to receive a web page or executable file over the wireless communication layer. Only I/O data is transmitted in the wireless layer.

There is no way for a malicious executable file or virus to enter your Ethernet network through a Banner Sure Cross wireless system.

Data Security

Data security is defined as reliably protecting your Sure Cross network sensor data from interception by hackers. Banner achieves data security by using a proprietary protocol, pseudo-random frequency hopping, and generic data transfer.

- FHSS it is greatly resistant to any narrow band interference and narrow band jamming
- Devices operate as a time synchronous network, so spoofing is much more difficult
- Custom protocol with very small data packets limits the transmission time and minimizes the chance of corruption; packet transmissions do not include metadata (data context)

The proprietary protocol alone provides a high level of security. Data security is far more of a concern when using open protocols. With an open protocol and no security encryption, anyone using that protocol can intercept and monitor your data. Widely used open protocols such as Wi-Fi have serious security issues. Even a high degree of encryption may not protect your data. It is common for new encryption schemes to be hacked within months of implementation. Proprietary systems are less likely to be hacked than open standards.

The second level of data security protection is the pseudo-random frequency hopping table. Each time a message is sent a new frequency is chosen, which makes it almost impossible for any system listening at a given frequency to hear more than a few messages out of hundreds. In addition to providing data security, frequency hopping technology also provides noise immunity.

Finally, and most importantly, the Sure Cross wireless system uses a concept of generic data transfer without context. Even if a hacker managed to crack the data packet format, all they would see is a set of 16-bit numbers with no reference as to what the numbers meant. No information describing the network layout or what the sensors are monitoring is ever sent wirelessly. A hacker, if they managed to receive Banner's Wireless data, would only see the actual sensor data, not what the sensor was reading or what role the sensor played within the wireless I/O network.

The use of a proprietary protocol, pseudo-random frequency hopping, and generic data transfer without context provides a high level of data security.

Data Integrity and Control Reliability

In a control or monitoring application it is unacceptable to have data lost, corrupted, or changed in any way. To guarantee the highest possible levels of data integrity, the Sure Cross wireless system employs binding, cyclic redundancy check (CRC), link health monitoring, and a preset default output state.

- Each remote device is 'bound' to the Gateway, which fixes the remote device to that Gateway
- A remote device uses the binding address as a seed that defines the channel hop sequence and the timing offset so multiple networks can co-exist
- When multiple networks are deployed, each Gateway uses a unique binding code so that each network uses a unique hop sequence and unique timing requirement
- Signal propagation works against injecting bad data, without being close enough to overwhelm existing transmitting devices, true devices will win in sending data

Binding the radios to each other adds an additional layer of security to an already secure platform. Binding locks radios to a specific master radio by teaching the radios the master radio's access code. After devices are bound, the radios only accept data from that master radio and the master radio only accepts data from those specific radios bound to it.

When the data is transmitted, a CRC algorithm ensures that the data arrives intact. If the CRC algorithm fails, the corrupt data packet is discarded and the data is automatically re-transmitted using a new frequency during the next communication cycle.

The Sure Cross wireless system continuously monitors the health of all wireless links in the system. A "link" is defined as the real-time connection between two radios. If any link is lost, the inputs and outputs associated with the radio are set to a predefined value. When a radio drops out of the network, from a lightning strike for example, the master radio detects the link has been lost and reports the loss to the control or monitoring application. At the same time, the master radio sets the inputs and outputs of the radio to predefined data values, resulting in predictable network behavior during a communications error.

To guarantee the highest possible levels of data integrity the Sure Cross wireless system employs binding, CRC checks, link health monitoring, and a preset default output state.

DXM Security

Most security questions customer IT departments may have can be alleviated by noting that the Banner DXM Controller does not run on a Windows- or Linux-based operating system. The DXM Controller runs an embedded RTOS control loop with no remote login capability. It has a limited ability to communicate with host systems by design.

The DXM is configured by an XML file created from the DXM Configuration Software and can be sent to the controller using authentication to update the DXM Controller functions.

The DXM Controller was designed to consolidate sensor data into register values and present that data to host machines using a push method to a server or using industrial protocols (Modbus RTU, Modbus/TCP, or EtherNet/IP). The communication methods are selected within the XML configuration file.

DXM Controller connection methods include the following:

- **USB**—Configuration port and console output. The configuration software uses custom API commands for sending configuration data. Data transactions can be controlled by authentication.
- **Ethernet - Industrial protocols**—The DXM Controller is a slave to the masters of the network. Ethernet protocols include Modbus/TCP, EtherNet/IP.
- **Ethernet - HTTP push to server**—DXM Controller creates push packets that can be encrypted using HTTPS. Acknowledgement messages from push packets offer limited control are also encrypted.
- **Ethernet - Configuration port and console output**—Configuration changes are made using the software, with the authentication controlled.
- **RS485 Modbus RTU master port**—Controlled by the DXM for accessing remote Modbus devices. The DXM is the Modbus master and is only programmed to use the Modbus RTU protocol. The configuration of this port is controlled by the configuration software, which can be username/password protected.
- **RS485 Modbus RTU slave port**—Read/write access to register data
- **RS232 port**—Some models support a RS-232 port that is completely controlled using ScriptBasic. Access with this port is limited to what the user programs.
- **CAN / J1939**—Some models support a CAN/J1939 port that is configured to read/write data based on the user configuration settings. Configuration is controlled using username/password authentication with the configuration software.
- **SDI-12**—Some models support SDI-12 connections for remote sensors. The DXM manages the SDI-12 bus and the SDI-12 bus is protected using username/password authentication with the configuration software.
- **Cellular LTE / GSM**—Allows for HTTP push packets to webserver and texting capabilities with appropriate configuration and firewall configuration.