Data Integrity and Industrial Reliability via Wireless Mesh Networks

By Jeff Wilkinson, General Manager – Starrett Advanced Technology Division

Industrial environments demand rugged and reliable solutions regardless of the type of system to be deployed. Electronics as a group, are some of the most mechanically and performance fragile systems that live on the shop floor. Within the shop floor environment there are frequent examples of noise and interference sources that disturb or otherwise impair the reliable functioning of electronics.

While heavy steel packaging and seal rings keep harmful, volatile and corrosive liquids and particles out of sensitive electronics, they cannot protect the emissions of radio waves in wireless networks. More and more, wireless sensors and metrology instruments are being deployed in production areas. Wireless systems deliver their quality or production data to critical operations downstream and are crucial components of the modern production reality. With this said, wireless data transmission of data is critically needed and simultaneously vulnerable to shop induced interference.

Radio Frequency (RF) Waves

Radio frequency (RF) waves are the carrier for data in a wireless data acquisition system. These waves are simply energy propagated through free space. When free space is cluttered with other energy forms, intentional radio waves are compromised.

RF is highly susceptible to corruption and alteration via a variety of Electromagnetic Interference (EMI). EMI has been defined as the "degradation of the performance of a piece of equipment, transmission channel, or system caused by an electromagnetic disturbance." (ANSI C63.14, 1992) EMI can occur throughout the EM spectrum from 0 Hz to 20 GHz or higher frequencies.

However, EMI problems are most prevalent in the RF spectrum. Since in our application the RF carries the data, good RF handling must be dealt with to keep the data intact.

EMI types typical of (but not limited to) production shop environments:

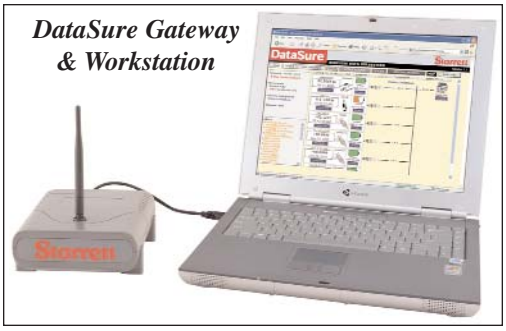
1) DC Fields: Quasi-AC fields and Magnetic: “plumes” or fields generated by rotating spindles, motor armature coils, de-magnetizers, magnetized steel beams in commercial buildings etc.

2) AC Fields and RF: generated by AC motors, induction hardeners, unshielded electronic devices, cell phones, microwave ovens, and walkie-talkies.

3) Transient Electromagnetic Fields: produced by the switching of inductive loads such as circuit breakers or motors. Lightning will also cause this type of disturbance. A transient signal in a cable can produce a radiated emission with spectral (frequency) content. Radiation from transient sources is rarely found to have significant energy at frequencies exceeding 500 MHz however.

Manage Performance Relative to Interference

In the presence of these EMI components, RF based systems must manage their performance relative to interference if they are to be useful. There is no such thing as a 100% noise immune radio system. So with that truth, systems designers must develop robust wireless data collection networks and sensors to be less susceptible to the presence of EMI.



There are many techniques that designers can use to offset the impact of noise in a wireless network. The scope of this paper is to discuss the mesh network as a primary means of making robust and reliable wireless networks.

Mesh Network Topology

A mesh network is a topology that has some distinctive features. First it has a single and central “gateway” function where all system wide commands and network management can occur. Data from the network also

returns here. Secondly, the sensor/measurement endpoint radios can be active components of the network. Thirdly, numerous routers or repeaters are present and can be added to enable multiple paths for OTA (Over the Air) transmissions.

The mesh is inherently robust to interference by its system configuration. An example of this can be explained by looking at what happens to the OTA flight of the RF. Figure 1a shows the endpoint radio acquires data from it's measurement tool or sensor, and transmits it to the gateway, a plume of EMI from an induction hardener cancels the RF in the immediate vicinity.

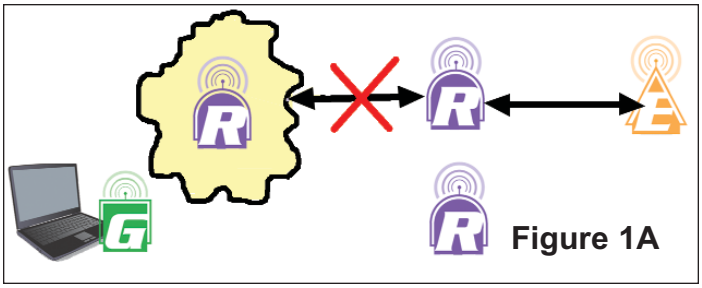


Figure 1A

Adjacent to the first router, other routers (Figure 1b) have also received the data transmission. Once the blocked router has found no data was received, it cannot pass along any data to the gateway. Simultaneously, the other routers get data poassed to them and attempt to send ahead to the gateway.

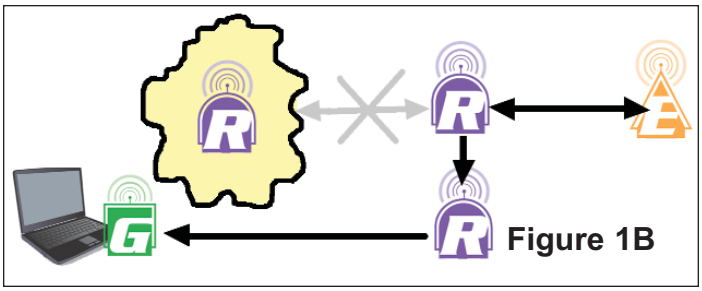


Figure 1B

A Series of Router Hops

The data may make a series of router hops until it reaches the gateway. While this is happening, other copies of the data are en-route to the gateway. When the gateway sees an exact copy of already received data, the gateway discards the additional copies. Endpoint radios on the network have a unique “address” which allows only the intended data to reach the gateway without duplication.

In addition, when EMI is not present and optimal operating conditions exist, the mesh network speeds OTA transmission by constructing a routing table in each network element. The router table creates a predetermined path for data, which allows the other routers in the network to be either idle or available for other endpoints to be received.

This example shows that multiple paths in a mesh network provide alternative paths for data thus spatially and temporally avoiding corruption from EMI. There are other techniques a wireless system can employ that insure robust data, but that subject will be reserved for another application note.

Daisy Chain or Point-to-Point Network Failure

Unlike mesh networks, daisy chain or point-to-point networks suffer from “single points of failure”. See Figure 2. If one link in the chain is corrupted via EMI, then OTA transmission will stop at that break in the “chain”.

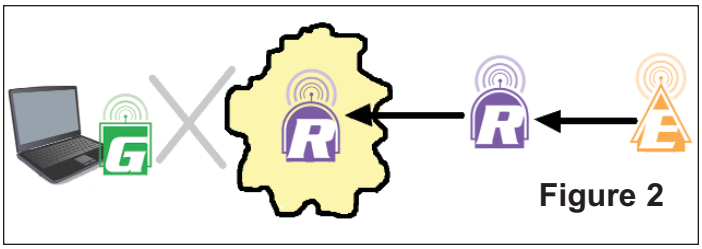


Figure 2

Suffice it to say, if the wireless network is capable of supporting a mesh configuration, then simply adding routers to the system will make the system more robust.

Other Causes of Data Integrity Problems

In addition to EMI, there are other environmental and user related issues that cause data errors. The well informed system installer and network administrator will be able to choose the right system and remedy for certain kinds of data integrity problems.

In paper and pen data recording, it is immediately apparent that data has been recorded. By looking at the paper, you can easily see what was recorded. Wired systems for data collection are typically connected to a local device that displays the most recent reading. Some installations of data collection have PC's at each work cell or bench showing the data and trend lines for the measurements in progress.

One of the key advantages of wireless data collection is freedom from the bench; host PC's, wires and the limitations of bringing a part for inspection to the tool.

Therefore, with wireless systems, data being recorded may not be immediately or readily visible. Consider a shop floor operator with a wireless tool. When data is recorded by pressing a button

on the tool or data cable, the data shows up at the gateway/PC screen. If the PC is not located in the immediate vicinity of where the data is taken, the operator is unsure data has been received. Some wireless data systems have no capability to alert the operator of the tool, that data actually made it to the intended destination – in this example, the PC/gateway.

Feedback Systems Ensure Successful Transmission

Advanced systems for wireless data collection have indicators/enunciators on the data transmission device itself, to show the operator the status of the system and the successful transmission of data. In many systems, the end node is "unaware" that the network or host PC loses power, and therefore, data will not be recorded. However, if the endpoint has the ability to show the user that data transmission has failed, a few good things can result. The operator can immediately see that there is a problem with the network and correct it. Conversely, without any system status indication, the operator can unknowingly corrupt his own data collection.

The operator can also continue pressing the data send button, which will send many duplicates of the data. Unfortunately, repeated pressing of a button is a typical or perhaps a natural response when an electronic device does not work as expected. By repeatedly pressing the data send button to "remedy" the problem, the data set will be corrupted and therefore corrupting the data sets' statistical significance. Additionally, without system feedback, the operator may continue to think everything is ok for sending data, then continues the data collection process but loses an entire shift worth of data collection. This is an undesirable situation indeed.

With a feedback method of system status oriented to the user, data can have more integrity. However, when the user ignores or misses the feedback, data can still be corrupted. As an additional safeguard to lost data, the endpoint radio can incorporate a means to store data recorded when the main systems is down. Often operators will take measurements quickly, yet accurately in a production environment. After taking e.g. 15 successive measurements with rapid button pushes, and the system crashes on the 10th measurement, then the remaining 5 measurements would be lost.

Modern wireless data collection system designs incorporate a storage feature that collects any data taken at the endpoint and holds it until the system becomes available again. All the while data is being stored on the endpoint, the endpoint radio alerts the user with the feedback system described above and waits for the system to come back online. Once the system is back on line, the endpoint will dump its data to the gateway/PC host system. No data is lost, even though the main system has failed.

During the OTA (over the air) transmission of data, a wide variety of interference can occur and modern systems have mechanisms to identify corrupted data and mark the data as such. By using CRC (cyclic redundancy check(ing)) and parity error detection methods, modern systems can tag or discard the corrupted data. Unfortunately, most systems today don't even do that. Without error detection and correction, there is no chance of recovering the intended measurement.

DataSure Ensures that Uncorrupted Data Arrives at the Gateway

With Starrett's DataSure, there is a system feature that communicates between endpoint and gateway and seeks to ensure that uncorrupted data arrives at the gateway. If the system tags the data sent with a CRC or parity error, the gateway informs the endpoint to resend the data again from the endpoints temporary memory. Data is then sent again, insuring good data ultimately gets to the data set. If data is received as good, then the gateway informs the endpoint to discard its temporary memory of that data, so that it won't get sent again. The temporary memory is only held until the gateway validates successful receipt of the data.

These methods are just some of the ways that DataSure ensures very high data integrity. Data collected in the field show remarkable performance figures. In one test, successful transmissions with zero failures in 3.5 million measurements have been recorded.