Why UHF RFID Systems Won't Scale

Proposed ISO and EPC standards for UHF RFID systems don’t allow for many readers to operate simultaneously in one location, which will dramatically reduce the effectiveness of any large-scale implementation.

Everyone in the RFID industry and many potential end users are closely watching the development of standards for UHF RFID systems. It’s important for the industry to have standards, because standards make it possible for one company to read another’s tags, even if the two companies purchased their RFID hardware from different vendors. Standards proponents say this interoperability will enable widespread adoption of RFID technology to track goods in the supply chain with RFID tags.

Creating a global standard for the air interface protocol—the way tags and readers communicate—for UHF systems is a worthy goal. But before UHF systems can be widely adopted, something else is needed. Lots of RFID readers must be able to coexist in the same facility and same geographical area without interfering with one another. If standardized systems can’t be operated independently from each other within the same facility or geographic area, there’s little benefit to having a UHF standard.

The Problem

The main technical problem facing end-user companies is the possibility of large-scale reader interference that could render UHF RFID installations completely inoperable and severely limit the rollout of UHF RFID systems.

Up to now, installations of UHF RFID systems have been limited in scale. Most involve a small number of readers at the same site, which allows end users to use screens—metal shielding, for instance—to prevent readers from interfering with one another. Another option is to turn one reader on and simultaneously turn all others off, so the readers don’t interfere with each other. But if UHF RFID takes off, as many now envision, we could see hundreds of readers in one warehouse or manufacturing facility, and thousands of readers per square kilometer in an industrial area, which would make screening or timing readers either prohibitively expensive or impossible.

The problem is that readers transmit RF energy at very high power levels. The energy emitted by the reader decreases with distance; the rate of decrease is proportional to the inverse square of the distance. Passive UHF RFID tags (those with no batteries) reflect back a signal at very low power levels. A tag’s reflected signal decreases as the inverse fourth power of the distance between tag and reader. A reader can, therefore, effectively jam tag communications over a very long range relative to typical tag read ranges. In other words, a reader at one dock door could effectively prevent tags from communicating with a reader at a storage bay in a warehouse facility.

Possible Solutions

The problem has been recognized by some of the major players, notably by the Auto-ID Center, which developed the Electronic Product Code, and possible solutions have been proposed. One involves allocating small segments of the radio spectrum to readers in a given area; a reader in one dock door might operate at 916.4 MHz, while the reader in the next door operates at 917.8. This approach fails immediately in Europe,

because there is not enough bandwidth to allow partitioning. (In the United States, UHF tags can jump between frequencies from 902 MHz to 928 MHz, but in Europe proposed regulations would require readers to operate between 865.6 MHz and 867.6 MHz.) Even in the United States, this approach is unlikely to succeed, because a reader using one slice of the spectrum may have to be much further from another using the same slice than is practical in a warehouse or distribution center.

Having readers hop randomly between different frequencies in a particular portion of the UHF spectrum could alleviate the problem. But once again, this solution can't be used under European spectrum regulations. A standard that only works effectively in North America will defeat the primary purpose of defining a global standard.

A second possible solution is to synchronize all the readers in an installation and to assign them time slots in which to transmit. This is called time division multiplexing. While it's conceivable to synchronize readers in one installation, it's much more difficult to synchronize all the readers at different installations in one industrial area. The multiplexing can be done randomly, but in a large installation, the time slots would become very small, which would affect throughput at each reader station. In other words, if you have many readers in a location, each one can only be on for a short period to avoid interference, which means, for example, that conveyors would need to be slowed down to ensure all packages on them are read.

A third possibility is to separate the portion of the RF spectrum used by tags and readers as much as possible. Readers would send out energy at one frequency and tags would reflect back a signal at a different frequency. This would prevent the more powerful radio waves from the reader from overwhelming the waves reflected back by the tags. However, if this is not done in a mutually compatible and standardized manner, incompatible systems could still jam each other. Frequency hopping readers could, for instance, hop into the tag data spectrum band of another reader or system.

The answer to the problem may lie in differentiating between the two different types of communication between tags and readers. RFID systems typically have two modes of operation. With read-only tags, the systems use one-way communication—the tags send information to the reader. With read-write tags, the communication is two-way. The tags send data to the reader and the reader writes data to the tag. In most practical applications, the vast majority of reader-tag communications will be one way.

Even when tags are transmitting data to the reader (one-way communication), the reader is sending out information to the tag, asking specific tags to respond. This means readers are constantly emitting a lot of energy that could potentially cause interference. The best solution to the reader interference problem may be to have readers that do not transmit data at all during the tag identification cycle. Instead, the tags would randomly transmit their IDs.

The reader would still need to transmit energy to power up the tag, but this could be done in a very narrow band and could easily be filtered out. All readers can then operate at exactly the same frequency, reducing the spectrum requirements and making co-existence easy. In other words, instead of having thousands of readers in an area shouting at the tags to request information, they would simply use one frequency to power the tags and wait for a response in another frequency. Since the tags reflect low-levels of energy, there would be no interference problem.

The problem of reader interference would still arise where readers are used to write data to tags. But companies could do this in more isolated areas to prevent widespread interference with portal readers that are simply reading tag data. Moving to an isolated area shouldn't be a big problem, because the writing of data to tags will mostly happen during the initial registration process, when companies write EPCs and similar data to tags and then match the serial numbers to products in databases. These areas are typically situated away from dock doors and other reading areas. And the few readers needed to write data to EPC tags could be shielded to

prevent them from interfering with one another.

The latest proposal for a UHF EPC standard—the so-called Chicago Protocol—does call for a "dense reader mode," but this still requires time multiplexing in Europe, which has the limitations described above. Moreover, if restrictions are not placed on readers operating in normal mode—that is, those not in dense reader mode—then these readers will interfere with each other and with readers using the dense reader mode. EPC and ISO standards need to be amended to restrict readers from broadcasting data to tags in order to read them. Otherwise, large scale deployments will experience significant problems.

Hendrik van Eeden is the CTO of iPico Identification, a Pretoria, South Africa-based provider of RFID systems. To comment on this article, click on the link below.