

## A passing test:

There's more than one way to solve the challenge of RFID data integration

By John Burnell

### True or False:

1. When you're very thirsty, you should drink from a fire hose.  T  F
2. If you had a racecar, you wouldn't get stuck in traffic jams.  T  F
3. Standards mean everything works the same.  T  F
4. Read speed is the best measure of RFID system performance.  T  F

They're all false. Hopefully, the last two questions were as easy to answer as the first two, but for many RFID users the answers are not so clear. In fact, users find a lot about RFID unclear. That is why people tend to latch on to easy-to-understand concepts like reading speed and tag cost. However, how the enterprise will manage the vast amount of data that is produced will have much more impact on the value the RFID system provides. RFID systems that provide data management instead of just data collection pass the value test.

"If you are just reading the serial numbers from RFID tags on cases as they pass through a dock door, at typical read speeds you are generating about 3,000 bits of raw data a second," said Mike Fisher, Intermec senior business development manager for RFID. "If the reader can't sort multiple reads, you can potentially overwhelm your system."

This leads to a multiple choice question to consider: What is the best option for managing RFID data?

- A. Middleware
- B. Enterprise or application software
- C. RFID reader
- D. All of the above

Most people answer "A" and are planning their systems accordingly. Spending on RFID middleware will grow an average of 162 percent annually through 2007, according to a study

by Venture Development Corp. However, the correct answer is D. The complete RFID system must work together to create meaningful information from collected data. While software is the obvious mechanism for doing this, the role of the reader is often overlooked.

RFID is most often compared to bar code, but a comparison to wireless networking technology better illustrates the value of the systems approach and how the technology will evolve. Before the IEEE 802.11b standard was created, wireless LAN technology was marketed much the same way as today's RFID—vendors emphasized the superiority of their chosen frequencies, range, speed, radio modulation techniques and other technical characteristics that were difficult to understand and harder to verify. The 802.11b standard defined functional requirements, established reasonable performance expectations, and paved the way for interoperable products that lent themselves to apples-to-apples comparisons. Development of global standards is expected to do the same in the RFID world.

Once 802.11b was established, development shifted away from proprietary technology to standards-based systems with new features that provided meaningful and valuable differentiation. The resulting emphasis on improved security, network management, remote configuration and troubleshooting helped create the adoption boom that continues to this day. Wireless LAN users have learned that the value of their network isn't measured by the speed of the connection—ease of use, management requirements and the ability to integrate with the IT infrastructure all have more impact on performance and total cost of ownership.

"It's the same today for RFID. An intelligent RFID reader can be put out there and just work, and look like any other network device.



It doesn't need to require special management, configuration or handling," said Intermec Vice President Scott Medford. "Even if a company is doing 'slap-and-ship' and isn't doing more sophisticated applications, an intelligent reader will provide IT management benefits."

"For years, every early RFID adoption I ever saw had a server assigned to each reader. They kept all the data from getting to the enterprise system, but it wasn't a very efficient setup," added Fisher. "Most of the middleware has been developed because the majority of RFID readers don't do basic processing."

Using the reader, middleware or application software to filter RFID readings is not an either-or proposition. Hardware and software features can complement each other and network with other input devices and information systems to effectively divert the flood of RFID data.

### Start at the source

RFID readers are literally and figuratively best positioned to manage flow of RFID data. On one end they communicate directly with RFID tags; on the other, with enterprise systems. Intelligent data management at the reader level eases the burden on networks, middleware and application software.

NASA is filtering RFID data with readers to enable fast data transfer and processing so chemicals and hazardous materials can be reliably monitored and tracked. The ChemSecure pilot project in place at NASA's Dryden Flight Research Center in Edwards, Calif., uses networked, fixed-position and mobile RFID readers from Intermec to collect tag and sensor data, and to pass relevant information to its Hazardous Materials Management System (HMMS) database application. Oracle's Sensor-Based Services suite provides additional filtering and presents data to NASA Dryden's Oracle enterprise applications.

Passive RFID tags are applied to chemical containers and read at various strategic points within the facility. RFID readers automatically track containers in chemical lockers, while sensors monitor storage conditions. It isn't necessary for all location and sensor data to

### RFID SECURITY: IT'S A NETWORK THING

Because RFID tags can be read and written to remotely, the technology is sometimes perceived as being insecure. However, simply accessing a tag usually doesn't put information at risk. Tags are typically encoded with a serial number that guides a lookup in an enterprise database, where actual information is stored. In this way, RFID tags are like most bar codes. For example, UPC symbols do not encode the item's price or any descriptive information. RFID tags and UPC bar codes simply serve as pointers to database records where information is held. Without the database, the number is meaningless.

Encryption and authentication features supported in RFID products and standards specifications can make it difficult for unauthorized users to access tag data in the first place. For example, tags can be set so they communicate only with the device that programmed them. Security features can also be used to protect tags from being altered after they are programmed. Tag memory is divided into blocks, which can be protected with different levels of security. The tag's unique ID number is usually encoded when the tag is manufactured, and locked so it can never be altered. The portions of tag memory that are rewritable can be protected through authentication. Keep in mind that the limited range of passive RFID technology requires hackers to get physically close to tags. This is a major difference from wireless LANs, which can be accessed by hackers thousands of feet away outside the facility.

Since it is relatively easy to secure tags, RFID security efforts should focus on blocking access to information in databases and software applications. Fortunately, the many excellent methods available to protect networks and computer systems can be applied to protect access to RFID data, so it can be as secure, or insecure, as the rest of the IT system.

"There are a lot of misperceptions about RFID security," said Medford. "RFID security is a lot like wireless LAN security. Users typically don't activate the basic security features that are available to them. The question isn't 'How secure is RFID?'— it is 'How secure do you want it to be?'"





be passed to the HMMS in real time. If the container is moved, an alert is issued and the system responds with actions to verify the credentials of the person handling the container. Temperature changes or other variances in storage conditions are also reported in real time. In the event of an emergency, first responders would be given Intermec 750 handheld computers with IP3 mobile RFID readers to identify the contents of the chemical container. Then, important information from the Material Safety Data Sheet would be pushed to the handheld from the HMMS database over a wireless LAN. Because the Intermec readers in the storage locations and Oracle Sensor-Based Services work together to process nonessential data, the system can access and process the information it needs in real time and trigger the appropriate response.

“The ChemSecure pilot is a great example of how organizations can leverage connecting the physical world to the information world to improve operations, enhance business processes and reduce costs,” said Allyson Fryhoff, vice president of Oracle Sensor-Based Services. “RFID and other sensor-based technologies can present many new challenges regarding information management. It’s imperative that organizations have the appropriate information infrastructure in place to meet these demands.”

A strong infrastructure helps users take advantage of all the features and capabilities that RFID offers. “If you have read/write tags, and know how to take advantage of the features that are supported in ISO standards and EPC Generation 2 specs, you can filter your data

with the reader. When a pallet leaves the dock door, you can set the system to only look for and record the pallet ID, or to capture the information needed to create an ASN, and to ignore all the case and item tags that might be read,” said Fisher.

Eventually, capabilities like these will be built right into application and enterprise software. Some warehouse management systems (WMS) vendors are offering RFID support, as are leading enterprise software vendors including Oracle, SAP and Microsoft. Oracle’s RFID solution is preconfigured to integrate directly with Intermec’s family of RFID readers. SAP has released its Auto-ID Infrastructure, which allows data from RFID readers, sensors, bar code readers and wireless devices to be logically integrated into applications. Different customers have integrated Intermec RFID systems with their SAP applications using both the Auto-ID Infrastructure and third-party middleware.

It will take time for enterprise and application software to natively support RFID. Agreed-upon standards will help stimulate RFID software development; however, it will not lessen the need for data management. EPC standards, for example, define the RFID data content and how it can be collected—not how it is filtered and used in applications. Thus, investments in intelligent infrastructures will provide long-term benefits.

“An intelligent system can present only the information that application needs,” said Medford. “If the data is relevant, and the network is secure, what else do you need?” ■

*John Burnell can be reached at [john@burnell.com](mailto:john@burnell.com).*