Identifying RFID’s Biggest Threats

Longstanding principles regarding the design of RFID chips are currently under attack, and could undermine all of the hard work put into RFID standards to date, as well as the future rapid adoption of radio frequency identification. I’m talking about practices that defy the concept that the Unique Item

Identifier (UII) or Electronic Product Code (EPC) must be monomorphic—that is, having a single form or structural pattern—and be assigned by the tag's manufacturer or end user only as a birth record, then locked into tag memory location (Memory Bank 1; the UII memory bank), as specified by the EPC Gen 2 and ISO 18000-6C standards for passive ultrahigh-frequency (UHF) RFID tags.

If my warning sounds ominous, well… it just might be, since communication and misunderstanding are at the root of the problem. Let me build the case slowly, and solve the communication-of-terms issue first.

The Language of an RFID Reader

The interrogator of a passive tag sends out an RF signal in a specific pattern, as dictated by International Organization for Standardization (ISO) standards. This is similar to people speaking German or French or English. The reader basically says "hello" in a particular language, and the tag of the correct design (i.e., language) absorbs that RF signal and reflects back a signal encoded with its own ID serial number. For instance: "*Bonjour*" would be replied to with "*un, deux, trois, quatre*", or "*Guten Tag*" with "*eins, zwei, drei, vier*." (And, yes, a reader can be programmed to understand multiple types—in this example, languages—but I prefer to use a simple monotype for this example.)

Since the dawning of radio frequency identification—going back to World War II—this has basically been how it has worked: A reader sends out an RF signal, and the tag responds with its identification. When low-frequency (LF) tags emerged in the 1980s for animal tagging, among other uses, followed by high-frequency (HF) tags in the 1990s, they worked by the same principal. The chip had an ID number serially programmed into it by the chip manufacturer. This very important ID number had several features. First, it was serialized and unique to a particular chip (and hence, to the tag) and it was locked at the time of the chip's manufacture, thereby assuring authenticity. Today, the common term for this is a Tag Identifier (TID). As UHF RFID chips and tags emerged in the late 1990s, the TID was as common a feature as it had been for 100 percent of RFID since the Second World War. This notion of TID assigned by the chip manufacturer is an excellent example of a monomorphic unique identifier.

Now imagine you are in the Alps and you try the famous mountain echo. You call out "hello," and the mountain replies "hello …heellloo …heeellllloooo…." Now imagine the same experience if you shouted out "hello, ladies and gentlemen, my friends.…" In this case, the mountain would already echo "hello" before you finished your sentence, drowning out your message. This word image is intended to illustrate that in radio electronics, of which RFID is an example, short message units are a key feature to effectiveness. More modern examples are text messaging (SMS) on a cell phone, or conducting searches on the Web. In both cases, simple (shorter) is better.

Reading a Tag

Now let's imagine you begin a conversation. The first exchange is always "hello," followed by a decision (do I continue talking to this person, or do I move on?). In the world of RFID, after the initial "hello," the decision could be "thanks

and goodbye", or it could be "tell me more." For the past 25 years LF, HF and early UHF tags all worked exactly in this way. The reader would transit a signal that signified "hello" (a request that the tag transmit its TID), followed by "tell me more" (a request for additional information, programmed in a section outside the TID, often referred to as user memory, or just memory), and/or "thanks and goodbye." For example, ISO-18000-6b UHF RFID tags carried 2 kilobits bits of data capability, of which the TID accounted for less than 100 bits. Once the interrogator captured the TID and was locked into a conversation with a particular tag, it could then choose to read all or part of the remaining tag memory. LF, HF and UHF all worked this way until the dawn of the ISO 18000-6C or EPC Gen 2 standards.

Prior to the creation of the EPC Gen 2 standard, and for almost 60 years thereafter, RFID began with "hello" in the form of an exchange between the reader and the chips' TID. British and American World War II-era warplanes had TIDs and were recognized by Allied forces. When your dog has an LF glass tag injected under the skin, the animal can then be identified by the tag's TID. When you use your smart-card HF passport, the initial read is between the interrogator and the TID. And when the Automotive Industry Action Group (AIAG) first demonstrated UHF applications (in its development of the B11 Item-Level RFID standard) at GM's plant in Detroit, the reader identified tires by interrogating the TID. In the case of the passport, the chip is encoded with additional information that may be interrogated, if required. In the case of the GM tire, the chip also contained additional information chip, but was accessed only after the TID was identified.

What Changed With Gen 2

Part of the genius of EPC Gen 2 is that, upon being initially interrogated by a reader, the tag transmits an Electronic

Product Code—a UII that identifies the product the tag to which it is attached—instead of transmitting a TID number assigned by the chip manufacturer (which just identified the tag). The "genius" is that it achieves two benefits over past designs: First, it assures that the initial read provides actual item identification, and second, it enables the UII to provide the key to a long list of business and consumer benefits, accessed via the Internet or some other network. The creation of EPC Gen 2 was the first time in RFID history that the TID was not read as the initial action between the reader and the chip. What's more, the first supply of Gen 2 chips did not even contain a TID. This has been corrected, and the standards now support that a unique serial number can be written—and locked—to the TID in Gen 2 chips, thereby providing assurance that the tag's data has not been duplicated into another tag (unique data = UII + TID).

The Problems With EPC Gen 2

There are now two major threats to EPC Gen 2's approach: The first is the use of proprietary item numbers instead of the numbering system specified by the EPC Gen 2 standard that enables the UII to serve as the birth record for both a tag and the item to which it is attached; the second involves violating the concept that the UII must be monomorphic.

The UII must be the birth record for the item to which the tag is being attached, and not an arbitrary number assigned after the item's manufacture. Within EPCglobal, the Gen 2 standards provide clear solutions when programming the UII memory bank (MB01). In simple terms, this memory bank is programmed with a code that first identifies the company making the item, then the item's product number and, finally, its unique serial number. When all three come together, a globally unique serialized item number—the EPC—is created. In the ideal scenario, this number could be rapidly searched for on the

Web, even during RFID scanning, in order to provide additional information regarding this particular item. Non-EPC applications are somewhat more flexible in how they can program data into MB01.
If Michelin were to program a tire's RFID tag, for instance, it would program MB01 (UII memory bank) with the company code, product code and serial number, then lock this information. If a customer wanted additional data, such as the Department of Transportation (DOT) code or other particular customer information, then Michelin would program that into the portion of memory known as user memory, or Memory Bank 11 (MB11). Michelin's unique number (UII or EPC) would be locked and never changed, regardless of what might happen to the tire in the course of its lifetime. Any additional data desired to be recorded would either be in a remote database (Web-based solution) or within the RFID tags MB11. During the life of this tire, the customer may wish to add information to the tag, such as mileage or a specific fleet number, which can all be placed into Memory Bank 11 (user memory).

The problem is that some businesses and customers have expressed a desire to place their private numbers into MB01 ((where such data is not, by intent, normally placed), and thereby be assured that their number is part of the information read first. On the surface, this could appear rational, or even reasonable; however, it basically violates any ability to assure interchangeability among users. The reason is that the EPC standard, for example, provides published company identifiers to which the EPC number can direct Web-based systems with full interchangeability. A world where companies can apply proprietary item numbers would destroy interchangeability. The principal of a monomorphic UII is well established for EPCglobal-based applications, but is less understood for non-EPC applications.

Even if a non-EPC application wishes to follow ISO procedures for programming a chip, it is imperative that simple

(monomorphic) UII procedures be employed, and that the UII be the birth record of the manufacturer, and not a customer number. Imagine, for instance, if Michelin were required to program every single tire with the customer ID numbers of every distributor, OEM and fleet to which it sells that type of tire, as opposed to 100 percent of the identical tires having clear birth UII numbers readily recognized as a specific Michelin tire. For more than 60 years in RFID, the birth UII (TID) has been the item's principal ID. Historically, it has been used for the chip, and now it has been extended for the item itself.

If the first issue is not resolved, it will reduce Gen 2 to nothing more than a generalized serial number of no recordable meaning, perhaps even less interchangeable than the TID designs of LF, HF and ISO 18000-6b UHF of the past.

However, the second threat, if not addressed, would push RFID functionality back beyond where it had been for the past 60 years, thus reducing it to an entirely proprietary, closed-loop, client-specific solution tool.

Violating the Concept That the UII Must Be Monomorphic

The second threat—violating the notion that the UII must be monomorphic—is just as insidious as the first. Together, they reduce EPC Gen 2 to a state worse than where the industry was prior to Gen 2.

The basic problem is that when the first EPC specifications were published, very little was said about programming user memory. Many early adopters of Gen 2 technology relied on solutions that did not require any user memory—partly because in the early days, no chip supplier sold tags that contained user memory on-board. Early suppliers of Gen 2 chips offered only 64 bits (later upped to 96 bits) for the UII/EPC Memory Bank (MB01), and nothing else for additional memory (User Memory—MB11).

Recently, chip suppliers have begun releasing chip products with small amounts of user memory (up to 512 bits). Some companies feel that adding incremental amounts of information to MB01 is the fastest way to access "what they want." The correct answer is to place the intended and accepted construction of UII/EPC into MB01, and *all* other information in MB11. If companies begin to place "user information" (data intended to be placed into MB11) in MB01, that would create a scenario similar to the "hello" and its echo, versus the longer conversation described earlier. Readers would begin to become confounded by the additional information required to simply say hello. And we aren't considering the effects real-world RF interference would play in the longer message lengths. RF interference has always been the bane of RFID—more so today with the proliferation of RF-based tools in the workplace and throughout the supply chain: When RF interference is present, the message may have to be sent more than once, and can take longer.

Again, history teaches us something about user memory. In the first releases for LF, HF and UHF tags, each had TID only, with no extra memory. Within two to four years, however, LF, HF and UHF tags each offered up to 2 kilobits of memory. Unfortunately, that message was lost in the evolution of Gen 2 technology. Chip suppliers needed to know how memory to offer. Since the retail sector represented more that 80 percent of early UHF RFID Gen 2 adoption, and retail had no user memory requirement at that time, chip suppliers lacked a clear mandate and began adding user memory to chips only incrementally. Retail is unlike the automotive or aerospace sectors, in which user memory has been historically employed and 2 kilobits has historical meaning. To no surprise, the 2-kilobit milestone is now upon us.

The fundamental problem lies in the intermediate-sized tags, where the tease is to just add some small extra piece of information into MB01 rather than to follow the standard and

historical practice and place 100 percent of user data (small or large) in the area reserved for user data—namely, MB11 (and never MB01).

Now imagine that interrogators would need to not only identify the UII, but also capture random additional information as well. This thinking is basically proprietary in nature, undermines universal exchange and reduces the Gen 2 standard to a convenient interface and protocol for proprietary exchanges.

What Needs to Be Done

With this in mind, we need to honor standards and the need to maintain monomorphic UIIs, and not try to deviate from them for shortsighted benefit. Doing so will be key to the near-term assurance of interchangeability and long-term access to the "Internet of things."

Patrick King is the current leader for global electronics strategies for Michelin and the tire maker's representative to EPCglobal. He is also a member of Global AIDC 100 and AIM Global's RFID Experts Group (REG), and a contributor to RFID for Dummies. *Dedicated to the improvement of sustainable mobility, Michelin designs, manufactures and sells tires for every type of vehicle, including airplanes, automobiles, bicycles, earthmovers, farm equipment, heavy-duty trucks, motorcycles and the space shuttle. Headquartered in Greenville, S.C., Michelin North America employs 22,600 and operates 19 major manufacturing plants in 17 locations.*

- CONTACT

FOLLOW US ON

- Follow
- Follow
- Follow
- Follow

ABOUTCAREERSAUTHORIZED SERVICE PROVIDERSYour Privacy ChoicesTERMS OF USEPRIVACY POLICY