Using RFID to detect UXO prior to repurposing land for civilian use

C. W. Axelrod
Delta Risk LLC, USA

Abstract

A major issue with repurposing heritage military sites is unexploded ordnance (UXO). The problem exists for firing ranges, minefields and bombed areas, especially when the land reverts to those who fired the projectiles, buried the landmines or dropped the bombs in the first place. UXO can lie buried almost indefinitely; ready to explode if struck accidentally, as when clearing the afflicted land for civilian or other military use.

One approach to detecting and identifying such buried UXO is to attach RFID (radio-frequency identification) tags to these objects in order to be able to locate them at some future date.

In addition to use for UXO applications, these same RFID tags can also serve to support the management of supply chains and reduce the number of lost, stolen or misplaced live ordnance, as well as duds. With RFID tags in place, individual items can be tracked and alerts issued if any go missing. Ideally, such controls would be applied throughout the manufacturing, distribution, storage and use cycle. When it comes to implementing supply-chain management for live ordnance, there are additional issues, such as interference by and to other wireless signals and accidental activation, to be addressed.

This section describes what needs to be done in advance to prepare for future cleanup efforts and suggests that a high return on investment should be achievable from implementing such RFID systems. We also examine the supply-chain management consequences of affixing RFID tags and using readers and tags in environments that may be inhospitable to wireless transmissions.

Keywords: unexploded ordnance (UXO), radio-frequency identification (RFID) tags, projectiles, landmines, bombs, clearing land, repurposing land, civilian use, supply-chain risk management (SCRM), radio-frequency (RF) interference.

WIT Transactions on The Built Environment, Vol 143, © 2014 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/DSHF140241

1 Introduction

Buried unexploded ordnance (UXO) represents a serious safety hazard for those in the vicinity and especially for those attempting to clear such land for civilian or other military use. The problem is huge, estimated as affecting some 3,000 sites in the United States alone, which account for tens of millions of acres, as described in Shubert [1]. This land may never again be suitable for repurposing for subsequent civilian and other military use and will have to be abandoned following its original military use. This will remain true for existing firing ranges and other sites where untagged projectiles, bombs and landmines may be buried, misplaced or improperly stored.

However, going forward, there are methods that can be implemented which will enable underground UXO to be located remotely and thereby reduce danger to searchers and others in the area. One such approach, namely, the use of RFID (radio-frequency identification) tags, not only serves to locate buried UXO from a safer distance, but has advantages for supply-chain management. Savings obtainable from the latter use may well exceed total costs.

While there are a number of technical issues that need to be addressed, as described in Shubert [2], research shows that such RFID tags will survive firing and can be used subsequently to find UXO at a depth of a meter or more.

2 RFID technology

2.1 What is RFID?

Simply put, RFID technology consists of readers used to scan objects to which RFID tags are attached and of software systems that support the technology, and collect, analyze and report the information obtained by the readers from the tags. As illustrated in Figure 1, RFID systems consist of tags (or transponders), readers, and enterprise subsystems. The interface between readers and tags is generally in the form of radio-frequency wireless transmission. Portable readers connect wirelessly to the enterprise subsystem, whereas fixed readers may connect by wire or wirelessly.

It should be noted that the acronym RFID is not used universally in the literature. For example, Klein [4] refers to electronic toll collector (ETC) tags as "transponders," not "RFID tags," whereas many RFID references, such as Karygiannis *et al.* [3], include ETC systems among examples of RFID implementations. Consequently, researchers might easily miss important references by only searching under the term "RFID tags" and not under "transponders" also.

2.2 How does RFID technology work?

There are essentially two main types of RFID reader-tag technologies, as well as a couple of hybrid designs. In one, the RFID tag has no power source and is activated by energy from the reader/scanner; in the other, the tag contains a power source and emits signals without having to be powered from a scanner. Each of

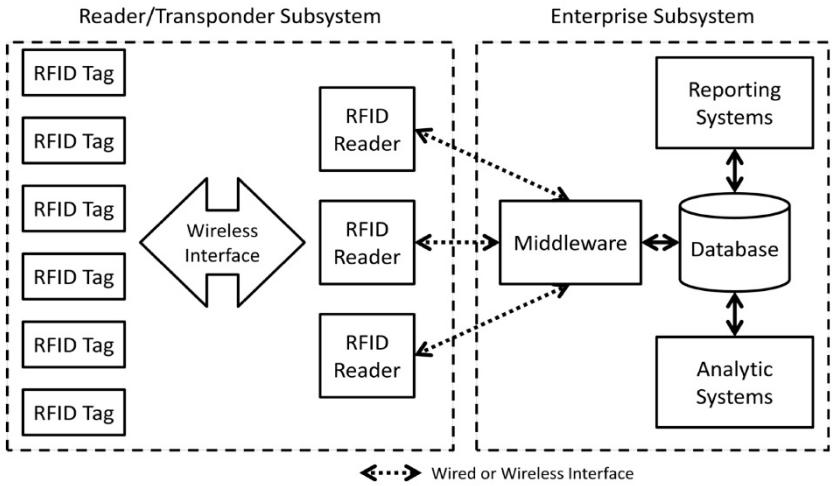

Figure 1: Typical RFID system architecture. (Adapted from Karygiannis *et al.* [3], pages 2–15.)

these technologies has a different range of suitable applications. For the purposes of this paper, we shall concentrate on the former technology in which there is not any power source in the RFID tag. Various tag categories are described in Table 1. Passive tags are most suited to the UXO applications discussed here.

RFID readers/scanners communicate wirelessly with the tags via specific protocols. The readers themselves may be fixed or portable depending on the particular application. For the UXO application, readers need to be moved across the terrain, whereas either portable or fixed scanners might be appropriate for various supply-chain phases, such as warehousing and distribution. Also, the enterprise subsystem may be built into a movable vehicle in support of scanners

Table 1: RFID tag categories.

Categories	Description
Passive	Tag obtains power from the reader, which transmits electromagnetic waves that induce current in tag's antenna. Tag modulates the reflected radio-frequency (RF) signal which is returned to reader.
Active	Tag has an internal battery that runs tag's circuitry and broadcasts a signal that is picked up by reader.
Semi-active	Tag remains dormant until it receives a "wake-up" signal from a reader, making for a longer battery life.
Semi-passive	Tag uses a battery to maintain memory or to power the modulating circuitry. Tag does not produce return signals.

Source: Karygiannis *et al.* [3].

Table 2: Selected device characteristics.

RFID Characteristics	Device	Description
Read-only memory	Tag	Programmed at factory; cannot be modified
Read-write memory	Tag	Alterable in use by writing to the memory
Induction	Comms*	Electromagnetic or inductive coupling
Propagation	Comms*	Propagating electromagnetic waves
Read technology	Reader	Can only read data from tags
Read-write	Reader	Can read data from tag and write data on tag
Stationary/fixed	Reader	Installed at fixed locations; read passing tags
Mobile	Reader	Can be moved to the locations of tags
Power source	Tag	Battery (active) or from reader (passive)
Power source	Reader	Portable (handheld) readers use batteries Fixed readers powered by batteries or electricity grid

*Communications between reader and tag.

affixed to the vehicle or installed in some central facility. Issues arise with respect to radio-frequency interference and transmission since the environments, which might include tanks, ships, airplanes, self-propelled artillery, and the like, are built with a variety of metals, often surrounding the RFID systems completely. Also, there are generally other communications activities, some very critical, taking place at the same time.

Table 2 shows the various characteristics of RFID readers and tags. For the UXO application, tags are read-only, portable and are powered by the scanners/readers.

Table 3 provides a comparison of features and capabilities of two categories of tags, namely, passive and active. Artillery projectiles preclude the use of active tags because their batteries would not be expected to survive firing of the ammunition. Landmine applications could theoretically use active tags except that the tags' useful lifetimes are too limited. This suggests that passive tags are needed even though the communications range between reader and passive tag is limited to one-to-two meters.

2.3 RFID applications

RFID technology is used in a variety of markets, including the following, as listed in Najjar [6]:

- **Supply-chain management**—warehousing, pallet/goods tracking, inventory tracking;
- **Work-in-process (WIP) manufacturing**—inventory tracking/management, product line efficiencies;
- **Asset management**—equipment tracking, fleet management, military and defence tracking;

Table 3: Comparison of tag characteristics and features.

Characteristics/features	Passive	Active
Power source	Electromagnetic waves from reader	On-board battery
Survive firing by artillery	Yes (specially-designed passive RFID tags)	No (battery likely not able to survive impact)
Reader-to-tag distance	About 1-2 meters	100 meters or more
Lifetime of tag	Very long	Limited by battery life, unless battery replaced
Relative size of tag	Small	Large
Relative data storage	Small (bytes)	Large (kilobytes)
Required signal strength	High (must power tag)	Low (information only)
Cost per tag (as of 2008)	Less than 50 cents	More than $7.00

Source: OECD [5], page 26.

- **Security and access control**—access control/tracking, automobile ignition, shoplifting prevention;
- **Consumer applications**—personal identification and authentication, maintaining shelf stock.

Here, the main focus is on asset management, although supply-chain management and security and access control are relevant to broader use of the RFID technology.

3 UXO security and other risks

Security issues will vary with the circumstances, particularly, the army in control of the land in question, the type of buried UXO, the need to protect against accidentally-triggered explosions, and the proposed civilian use of the affected land. First, we consider the safety and other risks related to using RFID and then list some specific software security lists.

3.1 Firing ranges and in the battlefield

Typically, when large-bore artillery is used for training on firing ranges or used in battle, one can expect that some projectiles may not explode on impact and might get lodged several feet below the surface. If the land used for firing ranges or battlefields has to be reused, for either civilian or military purposes, it will most likely be necessary to invoke the dangerous task of clearing the land. UXO represents a significant danger to those searching for such ordnance as well as to those who might later encounter UXO accidentally.

In the case of RFID use with ordnance, there are several risks related to security and safety, for example:

- An enemy might compromise the RFID tags or detection equipment so that UXO are not discovered, in which case, either (1) dangerous; ordnance is not recovered, or (2) it explodes without the advance notice that the RFID system would have provided;
- An enemy might compromise the RFID tags or detection equipment so that the system yields false positives about UXO existing where it does not, which could waste time and effort and distract operators;
- An enemy might acquire or hijack the RFID system for its own use and use it to detect and disarm UXO fired at enemy positions.

3.2 Minefields

In one sense, the reason for laying minefields is the opposite of that of removing UXO to make areas safe. Nevertheless, there is the issue of an army retaking land previously populated by the enemy, or the ending of a war, in which case civilians might, and do, get injured and killed many years after peace has been declared. In the case where one needs to remove mines that were previously laid or bombs that were dropped, which have RFID tags attached, the security issues related to firing ranges and battlefields also apply.

3.3 Supply-chain risk management

RFID systems can be used to control the movement of ordnance from manufacture through distribution and use. It can provide much needed information regarding the location of each projectile, bomb, or landmine. Specifically, RFID systems facilitate the control of duds and prevent stealing or misplacement of live ammunition. Such systems can also help reduce the manual effort involved in tracking and inventorying large amounts of ordnance.

4 RFID software and communications security

4.1 Cybersecurity threats, exploits, and vulnerabilities

There are quite a number of cybersecurity threats, exploits, and vulnerabilities that might affect RFID systems directly. Grimaila [7] lists the following RFID-related security concerns:

- **Sniffing attacks**— through the interception of wireless signals;
- **Spoofing attacks**—tags encoded by criminals so as to appear legitimate;
- **Replay attacks**—tags queried by attackers and data retransmitted;
- **Physical denial-of-service attacks**—tag removal, placing tagged items in foil-lined bags, swapping tags among items.

Rieback *et al.* [8] list the following RFID software characteristics that might facilitate exploitation by malware:

- **Large amounts of source code** in middleware systems, which might harbor many vulnerabilities;
- **Generic protocols and facilities** that may result in inherited security vulnerabilities;
- **Back-end databases** susceptible to security breaches;
- **High-value data**, such as classified information, which offer attractive targets for attackers;
- **False sense of security** from not expecting malware to exist in RFID off-line systems.

Rieback *et al.* [8] list specific security exploits such as:

- **Buffer overflow**—inputting data strings longer than space allocated to overwrite data and thereby gain access to the system;
- **Code insertion**—injection of malicious code into an application via scripting languages;
- **SQL injection**—a type of code insertion that causes databases to run SQL code;
- **Worms**—self-propagating programs, not requiring user activation, which exploit security flaws;
- **Viruses**—self-sufficient malware that spreads via self-replication.

4.2 Mitigation of impact of malware

Rieback *et al.* [8] suggest a number of ways to mitigate the impact of RFID malware, such as:

- **Checking bounds**—ensuring that indices lie within the limits of arrays;
- **Sanitizing input**—only accepting data containing valid characters;
- **Disabling back-end scripting languages**—eliminating scripting support from HTTP clients;
- **Limiting database permissions**—using the most restrictive rights;
- **Segregating users**—disabling the execution of multiple SQL statements in a single query;
- **Parameter binding**—using stored procedures with parameter binding;
- **Isolating RFID middleware server**—using network configurations that limit access to other servers;
- **Performing code reviews**—scrutinizing source code frequently.

5 Improving cybersecurity and physical integrity

5.1 Cybersecurity

Appropriate cybersecurity-oriented measures should be introduced at each stage of the System (or Software) Development Lifecycle (SDLC). In particular, it is important to include specific security-related tasks and activities within each SDLC phase. Furthermore, security testing tools should be used to ensure that the design and coding of software systems meet acceptable security standards and that the systems are tested by individual component and for integrated systems as a whole. Integrated systems should include ancillary systems that interact in some way with the RFID system.

5.2 Physical integrity

There are several specific physical issues with respect to ordnance. Stimek [9] describes issues relating to projectiles and bombs with respect to the required ruggedness of tags needed to survive firing/dropping/placement and impact. The main issue with placement or handling ordnance is the possibility of triggering a premature impact explosion that could injure or kill personnel.

There is also a requirement for the RFID tags to survive the handling of the ordnance, to which they are attached, throughout the various stages of manufacture, storage and distribution, so as to potentially support supply-chain management applications.

6 Further research

Once a determination has been made to affix RFID tags to projectiles, bombs and landmines, then, as has been mentioned, the same tags may be usable throughout the supply-chain cycle to track the locations of such ordnance.

Several important points should be made here, however. One is that the initial travels of ordnance will usually be through regular manufacturing and warehousing facilities and distribution channels where there is a long history of using RFID systems to track inventory. However, assurance that the systems can in no way activate nearby explosives is needed and must be tested thoroughly under a full range of potential conditions. The U.S. Department of Defence has published a series of guidance reports addressing HERO (Hazards of Electromagnetic Radiation to Ordnance) which include *Interface Standard MIL-STD-464C* "Electromagnetic Environmental Effects – Requirements for Systems," December 2010, and *Handbook MIL-HDBK-240A* "Hazards of Electromagnetic Radiation to Ordnance Test Guide," March 2011.

Furthermore, ordnance will certainly travel through less hospitable environments such as tanks, artillery, ships and planes where various metal environments predominate and numerous types of wireless communications abound. One has to be concerned about whether the wireless transmissions to, from, and within the RFID systems will be diminished in their effectiveness by

other transmissions and by dynamic metal environments. Conversely, there is a need to ensure that the transmissions related to the RFID systems do not interfere with other highly-critical transmissions. Again, the danger of an RFID system accidentally triggering explosive devices must be tested for and eliminated to high levels of confidence. Defence departments generally have rigorous standards for such testing that must be followed to the letter.

7 Economics

Economic evaluations of RFID systems for use in detecting and removing UXO are subject to highly-variable results since they are largely based on avoiding loss of human lives, reducing the risk of maiming, and eliminating other physical and psychological consequences. Costs attributable to death and serious injury are largely intangible, even though estimates are regularly provided for insurance purposes. We must also consider the potential for injury or death of those doing the searches, versus not searching, with resulting unplanned explosions.

Another aspect is the loss in value of land made unusable due to the risk of death or injury. The potential benefits of land reuse have to be compared to the costs of developing, implementing and operating such RFID systems.

If the use of RFID technology can be extended to supply-chain management, then the costs of implementing such a system must be compared to the benefits of greater efficiency (that is, faster movement of items through the system), fewer lost or misplaced items, and reduction in the risk of running out of ammunition at a critical time. The latter suggests factoring in the risk to those firing the projectiles running out of ordnance and coming under attack.

In Shubert [1] it is argued that the benefits of RFID technology, versus other means of detecting UXO, are the high rates of detection and the lower false alarm rates. In addition, one has to consider the personnel time for monitoring and reporting ordnance locations manually, versus using automated RFID-based tracking systems, comparative error rates, and the like. Accuracy of tracking systems will have a major impact on risks of losing ordnance and, especially, unexpectedly running out of ordnance in the battlefield.

It is likely that both the improved ability to clear land of UXO and more efficient and effective supply-chain management will lead to substantial net benefits for the implementation of RFID technology. Consequently, RFID applications will probably be cost-effective for finding and removing UXO alone, as well as for their additional use for supply-chain management purposes. Therefore, once the technical feasibility has been fully demonstrated, it should be fairly straightforward to get approval for either separate or combined systems, subject to budgetary constraints.

8 Recommendations and conclusions

There are strong arguments for implementing RFID systems for ordinance both with respect to discovering UXO and improving supply-chain management. A critical part of the technology relating to the survival of RFID tags attached to

projectiles that have been fired, but did not explode, has already been validated. There is still much work to be done with respect to examining the impact of radio-frequency transmissions and enclosed metal environments on the operation of RFID systems as well as whether the RFID systems themselves affect wireless and physical environments.

However, despite the cost and effort for developing, testing and implementing such RFID systems, they can be cost-effective for both detecting UXO and for reducing supply-chain management risk and increasing efficiency. Consequently, it is strongly recommended that the military seriously considers using such technologies as a means of saving lives, reducing costs, and making land, which otherwise would have to be cordoned off and protected indefinitely, available for civilian and other military use.

References

[1] Shubert, K., *Enhanced Electromagnetic Tagging for Embedded Tracking of Munitions and Ordnance During Future Remediation Efforts, MR-1272*, Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP), 2007. http://www.serdp-estcp.org/Program-Areas/Munitions-Response/Land/MR-1272/MR-1272/(language)/eng-US

[2] Shubert, K. & Davis, R., RFID Tags to Aid Detection of Buried Unexploded Ordnance (Chapter 12). *Advanced Radio Frequency Identification and Applications*, edited by Stevan Preradovic, Intech, March 2011, http://cdn.intechopen.com/pdfs-wm/14428.pdf

[3] Karygiannis, T. *et al*., *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, NIST (National Institute of Standards) Special Publication 800-98, April 2007.

[4] Klein, L.A., *Sensor Technologies and Data Requirements for ITS*, Artech House, 2001.

[5] OECD (Organisation for Economic Co-operation and Development), *RFID Radio Frequency Identification: OECD Policy Guidance—A Focus on Information Security and Privacy—Applications, Impacts and Country Initiatives, OECD Ministerial Meeting on the Future of the Internet Economy*, Seoul, Korea, 17-19 June 2008.

[6] Najjar, N., RFID current applications and potential economic benefits. *OECD ICCP Foresight Forum on RFID Applications and Public Policy Considerations*, Paris, October 2005.

[7] Grimaila, M., Security Concerns for RFID Technology. *ISSA Journal*, pp. 18–23, September 2006.

[8] M. R. Rieback, M.R., Crispo, B. & Tanenbaum, A.S.,Is Your Cat Infected with a Computer Virus? *Proc. of the 4th Annual IEEE Int. Conf. on Pervasive Computing and Communications PERCOM '06,* Washington, DC, IEEE Computer Society, pp. 169-179, 2006.

[9] Stimek, C.M. & Paulsel, R.Q., *U.S. Patent No. US 8444059 B1: System and method of tagging an ordnance*, May 21, 2013.