# RFID Systems: Applications

Applications using RFID technologies are expanding as industry, government and consumers increasingly understand how RFID works, and what it can do.

In this section we look at existing and future application areas. What they are, how they use RFID, and how they profit from it.

Future application areas will influence how the technology develops, and will also expose more challenges.

Readings for this section will be on line.

# Tag internal data organization

Tags are getting lower power, and more sophisticated. A typical modern tag architecture (EPC Gen2) with respect to data is shown below.

[See figure 8.29 in the text book.]

Most modern tags, including the ones we use in the lab, are similar.

# Expansion of applications

- We saw at the beginning of the course how RFID has been in society for a long time, especially for single bit applications.
- Modern RFID tags can do a lot more than reflect single bits.
- For example, the systems we have in the lab can do:

- Reader to Tag: 1.65 kbits/sec or 26.48 Kb/sec depending on mode
- Tag to Reader: 6.62 kbits/sec or 26.69 Kb/sec depending on mode
- 2048 bits of user read/write memory
- 64 bits of tag ID
- 24 bits of tag product code ID
- 16 bits of special data, such as application identifiers

- The standard used is ISO 15693. There is no limit on data size imposed by the standard. Only the tag imposes a practical limit.

# Applications in manufacturing

This is a short list of current application areas.
Think about and discuss some of these areas. Are they profitable?

Manufacturing and tracking:

- Knowing where components and sub-assemblies are located.
- Knowing who shipped the components, when and how.
- Knowing who the suppliers of the components are. Reliability of that supplier.
- Matching your rate of component intake with your product output. Inventory and distribution.
- Knowing where your products are, and if your customers have them.

Manufacturing and assembly:

- Using the right parts.
- Using genuine, authorized (not counterfeit) parts.

# Manufacturing

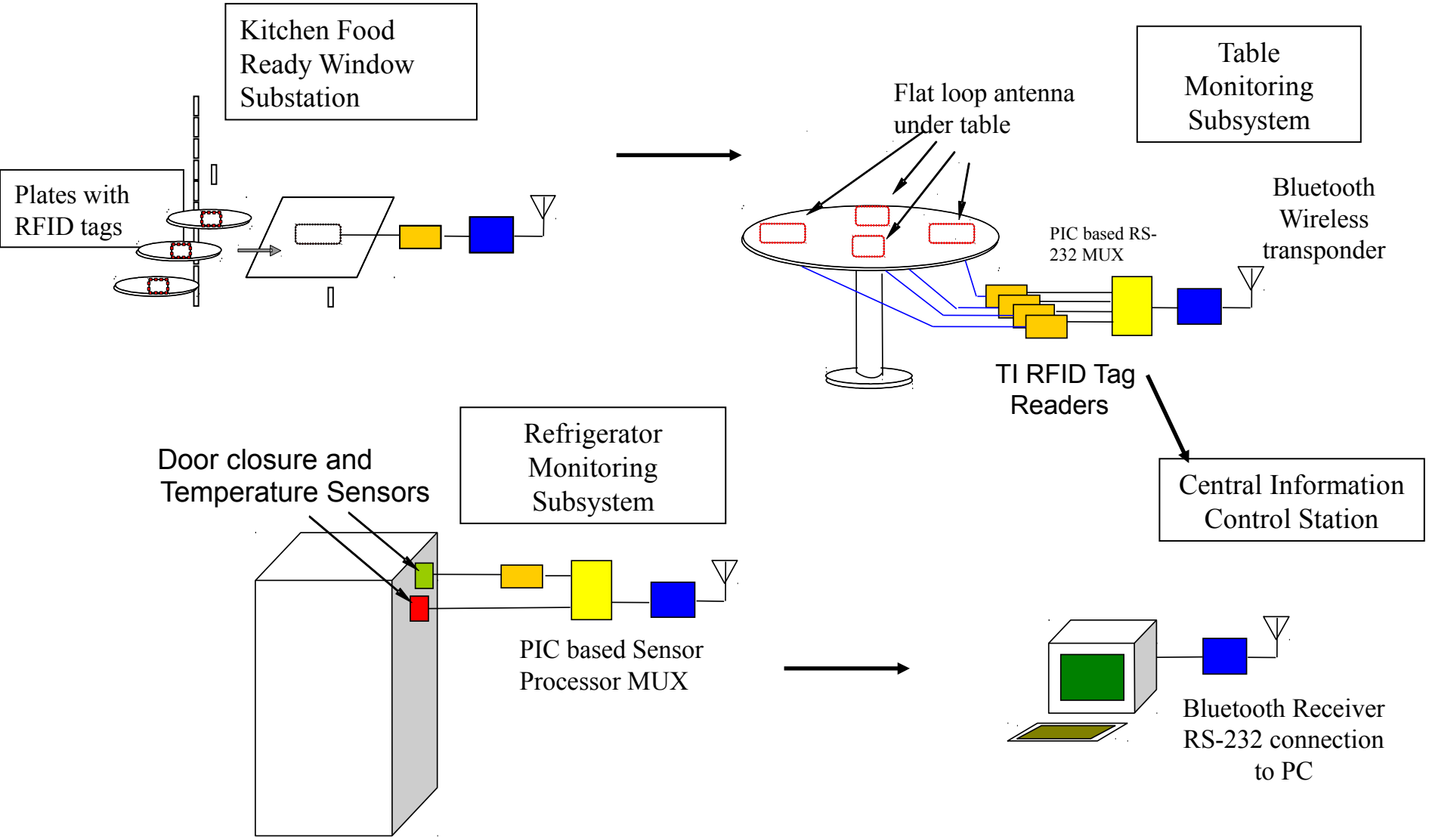
Manufacturing and assembly:

- Self documenting parts. Lots of links to product information.
- Assembling parts in the right order. If a critical part is missing, the line knows right away.
- Guaranteeing that all product pieces are in the box. The box can be closed and sealed, and you can still check.

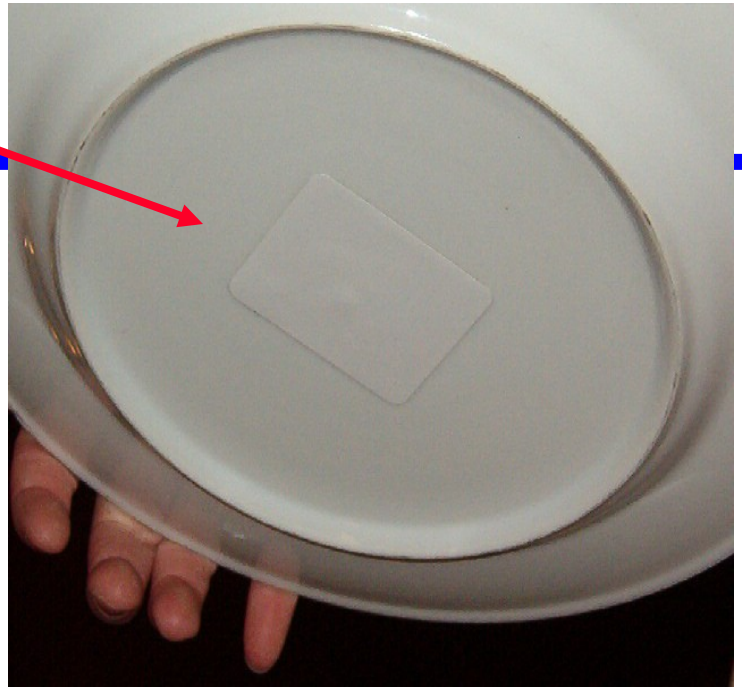
Manufacturing and lifetime history:

- Record all manufacturing details with the product, such as where it was manufactured, when, who's shift, what machines, etc
- Record all the components assembled into the product (can know if any parts have been replaced, and if so when).
- Who bought the product and when for warranty information.
- Reliability tracking of the entire product line.
- Defective product recall. Makes it easy to find defective units.

# This is a restaurant real-time logistics support system done by students at California State Poly Technical Institute (Cal Poly, San Luis Obispo).



# Antenna and tags. (They could go through the dishwasher.)



# Retail sales

This is a huge area. Wal-Mart, CVS and other stores have been drivers.

- Tracking and locating stock. “If you can’t find it, you can’t sell it.”
- Putting stock on the right shelves. The product distributors can now do it themselves.
- Helping customers find the right products.
- Helping customers find more information about a product, such as ingredients, expiration date, health risks or caloric content.
- Collecting data about how customers select products. Do they pick them up and examine them, or carry them around the store and put them back, or ?????
- Detecting potential theft.
- Payment
- Suggesting other products to go with the ones selected, for example clothing stores.
- (How many more can you think of? Probably hundreds.)

# Asset tracking

"Assets" can be just about anything that has value. That includes people.

- Portable equipment. "What was the last location of …."
- Heavy equipment. Cars, trucks, trains. It is possible to lose a train.
- Documents. This can track them, and also mark them as being authentic, original or copies and indicate if the are part of a set. Passports. Document management is a big business.
- Mail and packages.
- Airline baggage.
- People tracking. Prisoners, patients, children, resort guests, conference attendees, employees, university professors, …
- Animal tracking. Livestock, food supplies, pets.

# Everyday home life

- Clothing management, such as washing, storing, locating and coordinating.
- Food management, such as storing food and coordinating menus. Is the milk not cold enough, or too old? (Could RFID tags be context aware?)
- Consumables management, such as paper products, cleaning supplies, computer supplies, medicines, etc.
- Yard and garden management. Do you really want to put that particular pesticide on your tomatoes?
- Trash management and recycling
- Doors and locks
- Bill paying and other transactions involving payment
- Universal password management for home PCs, set top boxes, and the endless number of free accounts like those on Google.

# Security

- Revocable identity management
- Accountability management.  Who used what and when.
- Security process verification.  Verifying that doors, rooms, other areas have been patrolled and verified OK.
- Access to assets like equipment, documents, rooms, computer files.
- Replacement for keys, even in cars.  Peugeot has a complete RFID ignition system for cars.  BMW combines keys with RFID.
- Replacement for passwords.  Can you build a RFID reader into a computer keyboard or mouse?

# Health care

Health care is also a huge area. Many, many RFID uses, and always more.

- Patent identity. Are you operating on the right patient?
- Access to patent medical records. Serious document control.
- Access to hazardous equipment like XRAY machines.
- Access to secure areas, like operating rooms.
- Finding vital equipment like EKG machines.
- Tracking items. You left *what* inside the patient? Did those items really go through the autoclave?
- Drug tracing. Are you giving the right medication to the right person?
- Drug interactions. Can the patent take all those drugs at once?
- Patent location, especially for older patients. Did they walk out of the medical center?
- Matching up mothers and children.
- Matching up the bills. Everything that is billable has to be accounted for because of insurance rules.

# Threats from RFID

- RFID systems pose threats to both users and organizations that use RIFD systems.

1. There are threats related to RFID being a radio technology that emits RF radiation.
2. There are threats related to the data tagging aspects of RFID.
3. There are threats related to security and RFID.

- We will look at each of these in turn to understand the nature and severity of the threat.

- Some of these perceived threats are controversial. Discussion is highly advised and encouraged.

# Threats related to RF energy radiation

There are two broad areas here:

1. Threats due to interference with other electronic devices.
2. Bio-hazard threat due to people being exposed to non-ionizing RF radiation.

- Problems due to interference with other electronic devices are clearly possible.
- Anything capable of capturing the energy from an RFID reader could in principle have its normal functions disrupted.
- Everyday examples are reflected in warnings about using radios on airplanes or in hospitals.

# RF as a bio-hazard

- The health damaging effects of *ionizing* radiation, for example radiation from radioactive sources, is relatively well understood.
- Health damaging effects of *non-ionizing* radiation, such as that from radio transmitters, are far less well understood.
- High level effects are not likely with RFID. (In effect, putting a high enough level of RF energy into a person will cook them.)
- Remember skin depth. Higher frequencies will have less skin depth, and the energy will be converted to heat.
- Low level bio-effects are very poorly understood.
- The fear is that as $\lambda$ approaches the size of cellular structures, then those cellular structures, or the electro-chemical environments that the structures are in, will change.
- If so, a wide variety of neurological, pathological or other disease conditions could exist.
- This is an active area of research.

# Threats related to RF energy radiation

- Currently the response for all these scenarios is that if it is perceived as life threatening, it is often completely banned.
- However, these bans are often a default response due to lack of data that allow the risks to be understood.
- Although testing RF effects on other equipment is relatively straight forward, this is especially hard to do in any bio-system.
- As such data emerges, and as the economic benefits of using RFID becomes apparent, rules that completely ban all use of RFID may be relaxed.

# Threats related to data tagging

This is possibly a larger threat area, as it is directly connected to privacy.

These issues come from:

- The data tagging nature of RFID. Objects are tagged.
- That the data can be read from a distance. In radiative RFID, that distance can be reasonably long.
- That RFID tags have no human interface on them. They can be read without the cooperation of a human.
- That RFID tags are getting cheaper and cheaper to make.
- The result of cheaper tags means that it will become economical to tag every item that is sold, or in other words we will see *item level tagging*.

- Note that this is compared with using RFID to tag entire shipping crates where only the crate or the truck is tagged.

# Databases and data tagging

Be sure to read *RFID: The Doomsday Scenario*

- The big problem here is not just that data can be read without the cooperation of a person, but that the data can be stored and mined.
- In many cases, the use of the stored data is constructive.
- In other cases, it is an invasion of someone's privacy.

Privacy as a definition:

1. Privacy of *self* as a fundamental human right, for example to be free from unreasonable search, seizure or intrusion.
2. Privacy of *personal information*, for example protection of personal information with respect to who owns it, sees it, uses it or alters it.

It is the 2nd definition that we are most concerned with in RFID.

# Databases and data tagging

- The fear with respect to privacy of personal information is due to the creation and combination of databases driven by RFID tagged data.
- The *Doomsday Scenario* describes 4 database types that RFID data can be used to create.

1. Data relating to where an item was made, how and from what.
2. Data describing what the item is.
3. Data stating who bought the item.
4. Data that describes where the item has been seen.

- We need to address all of these to understand both why such data is useful, and where the threats come from.

# Data relating to manufacturing logistics

This is Database #1: *Where did this come from*

Examples of where this is useful:

- Supply chain logistics
- Manufacturing logistics
- Product delivery logistics
- It helps to maintain quality control, and allow for a highly optimized product realization process.

Is there a threat to privacy?

- It is felt that there is no real threat to *personal* privacy because the product manufacturer will want to keep this data secret.
- It is secret because the manufacturer does not want to give out any valuable process information to competitors.
- Except for large complex items like cars, these RFID tags will in many cases be removed before the item is completed and offered for sale.

# Data describing what the item is

This is Database #2: *What is this*

Examples of where this is useful:

- It uniquely describes the item in a machine readable form
- From that, one can get other information such as usage, ingredients, manufacture date, lifetime, etc.
- It can be used to control quality, such as recalling it if a defect is found.
- Because the data is machine readable, it enables other useful devices, such as the washing machine example.
- It can be coded or signed in such a way to insure authenticity.
- It can be used to enable useful services, such as helping customers select correct items (ie the right ink cartridge) or enable automatic payment.
- Recall the previous slide about retail applications of RFID. They are all valuable in some way.

# Data describing what the item is

Threats to privacy:

- Without one's knowledge, possessions one has can be identified.
- Unidentified people can know what items you are carrying.
- If one is carrying items of high worth, it could identify that person as a potential crime target.
- Governments, employers or other people may decide that items you have are subversive, or against a standard of morality. For example, books on political subjects or other literature.
- Identifying health conditions by reading RFID information in prescription drug containers.
- Identifying clothing, or other personal items of dress. This is an example of violation of *self* with respect to privacy.
- Identifying business or social associations. For example by implying where the item was bought, or who might have given it to you.

# Identifying people

This is Database #3: *Who bought it*

Examples of where this is useful:

- A knowledge of who owns the device can allow personalization of the device, such as language options.
- Owners can be notified if the product is defective, or needs to be recalled.
- Owners can be offered services, suggestions, use advice or other value adds for the item they bought.
- High value “owners” can be identified and offered premium services, such as frequent flyers, people with high bank balances, or other special people.
- People with special needs can be accommodated, such as individuals with allergies, or handicaps.
- In some cases, it is required such as for ID management in a company.

# Identifying people

Threats to privacy:

- Even without a RFID ID tag, just know knowing what items you are carrying, you can be identified.
- Even if your name is not known, other things can be determined about you, such as age, gender, physical properties, health status, income level and interests.
- From this information, and by combining this with other data such as credit card information, a complete identity picture can be assembled.
- This can be used to violate your privacy in many ways by providing this information to people who are not entitled to it.
- Stores, marketers, employers, insurers, parents, government agencies ie law enforcement, your neighbors, your work colleagues, anyone else you can think of.
- You have no control over the picture that has been assembled. What if the system thinks the items carried by a person standing next to you belong to you? How can you correct it?

# Tracking

This is Database #4: *Where has it been seen*

Examples of where this is useful:

- It can help establish a use pattern for the items you have, allowing a manufacturer to make better products.
- It can help customer experience, for example allowing resort guests to find and use resources, or helping conference attendees locate sessions and exhibits.
- It can help services manage resources, for example by knowing where people are, transit or media services can increase capacity in such ‘hot spots’.
- It can enable emergency services. If a person is in trouble, they can be found. An example is the E112 cell phone service in Sweden.

# Tracking

Threats to privacy:

- A person can be tracked without their knowledge.
- Inference as to what and who a person is associating with could be made.
- From this, attempts to infer what the person was doing or other activities could be made.
- No way to know even if the data inferred is accurate, and no way to control it, correct it or know who sees it.

# RFID security

Another privacy concern is RFID security. Major issues here are:

- Anyone can buy a reader. They are cheap.
- Although nothing prevents RFID data from being encrypted, it is generally not specified in standards.
- Many tags are writable. Although some standards specify a password to be able to write information to a tag, it is not mandatory.
- Spurious or false data then can easily be written to a card. Cookies for RFID.
- RFID tags are simple. They have to be because there is no power budget for complex functions, and they need to be cheap.
- This simplicity means that they can be cloned.
- This means that your identity can be stolen easily, or you might be made to appear to be someone else.
- See the article *Hacking the Prox Card*.