AUTO-ID CENTER

Low cost RFID and the EPC

Sanjay Sarma,
Steve Weis,
Dan Engels

MIT

outline

- RFID and the Auto-ID Center
- Protocols
- Security issues

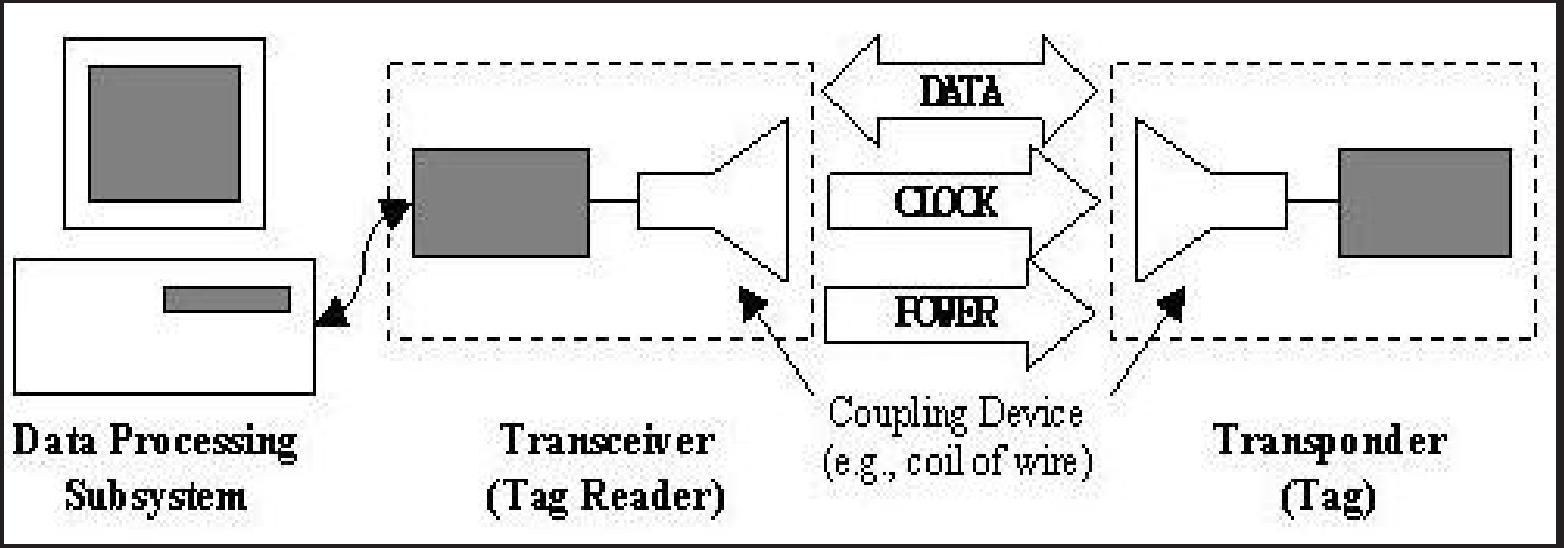
AUTO-ID CENTER

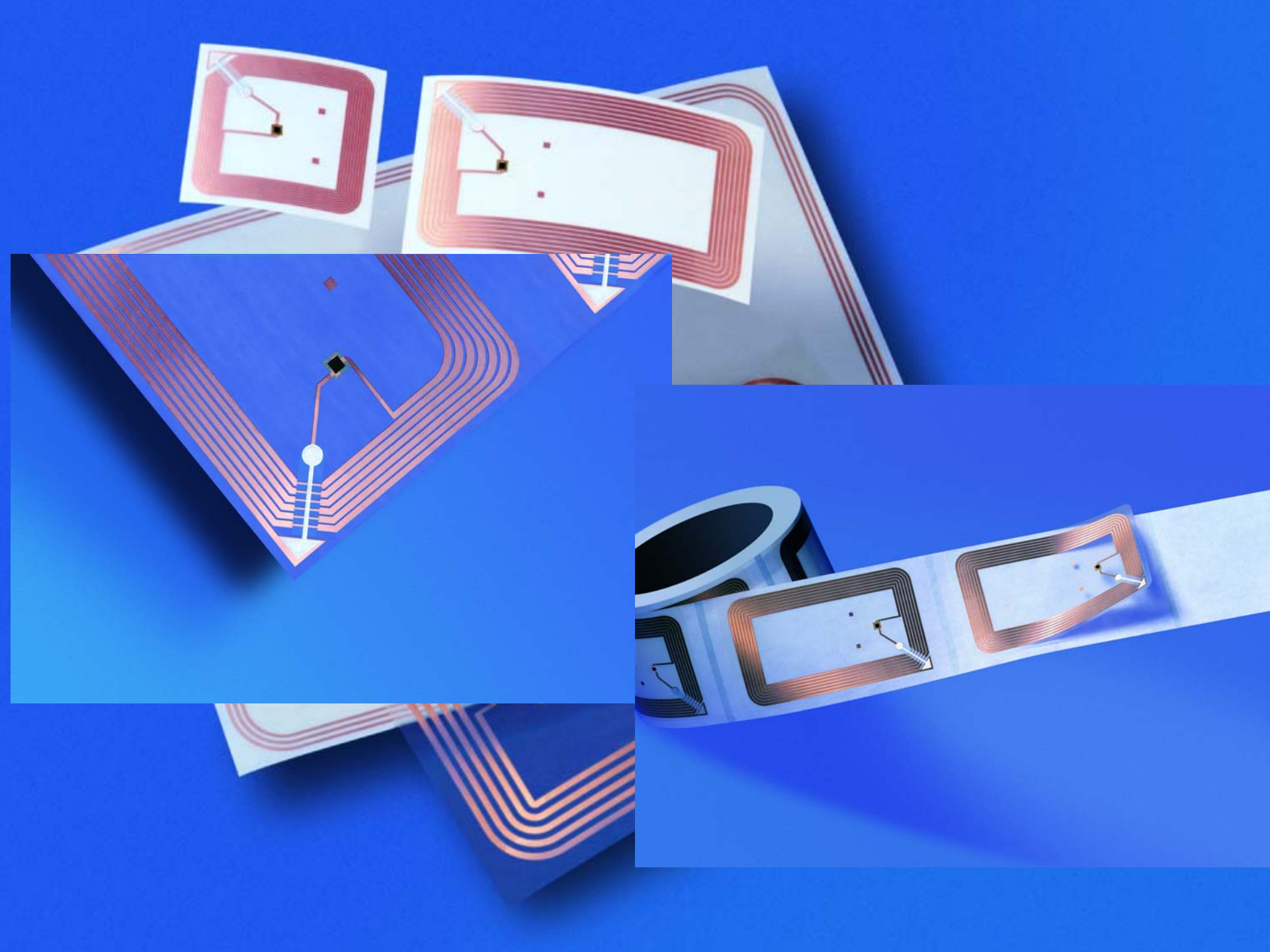
Part I Outline

- What and why of RFID
- The cost issue
- Manufacturing low-cost RFID
- Handling the data
- Current status

AUTO-ID CENTER

RFID System





AUTO-ID CENTER

outline

- What and why RFID
- The cost issue
- Manufacturing low-cost RFID
- Handling the data
- Current status

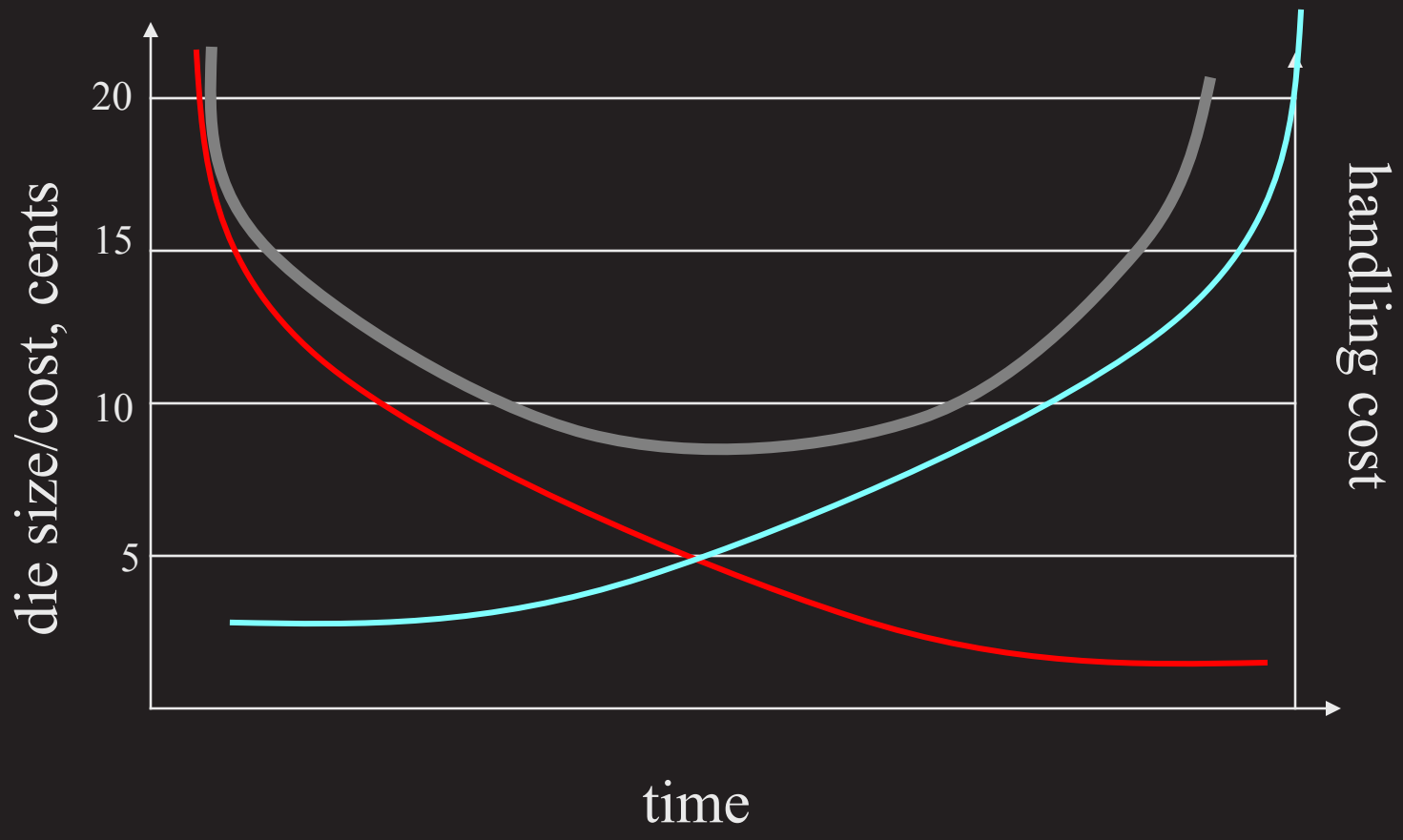
AUTO-ID CENTER

why low cost?

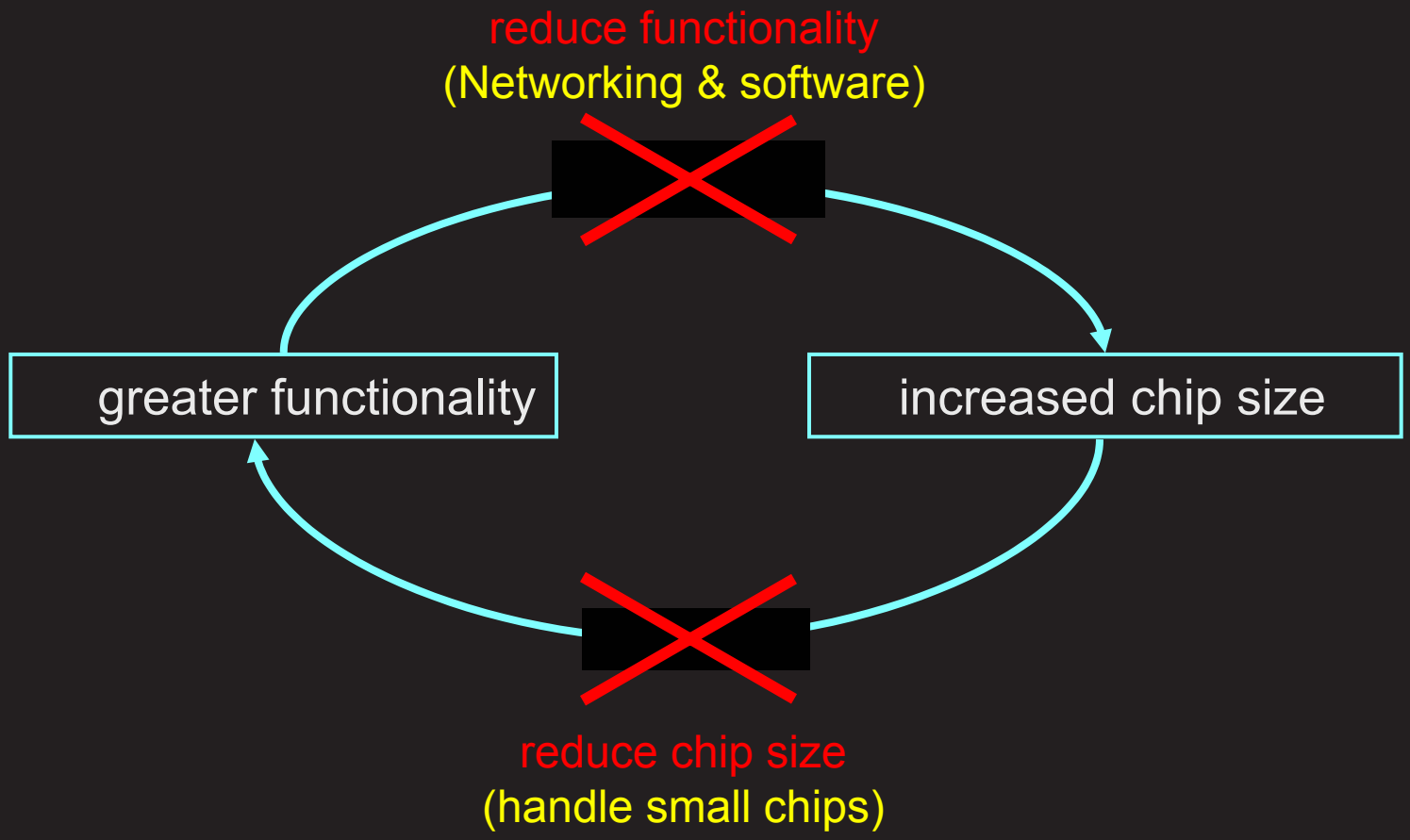
END USER	ESTIMATE NO. OF UNITS IN SUPPLY CHAIN (BILLIONS)
CHEP	0.2
JOHNSON & JOHNSON consumer goods division	3.0
KIMBERLY CLARK*	10.0
WESTVACO*	10.0
THE GILLETTE COMPANY	11.0
YFY*	15.0
TESCO	15.0
THE PROCTER & GAMBLE COMPANY	20.0
UNILEVER	20.0
PHILIP MORRIS GROUP*	25.0
WAL-MART*	30.0
INTERNATIONAL PAPER	53.0
COCA-COLA*	200.0
SUB-TOTAL	412.2
(Adjust for double counting @15%)	– 61.8
United States Postal Service	205.0
TOTAL INCLUDING USPS	555.4

low cost rfid

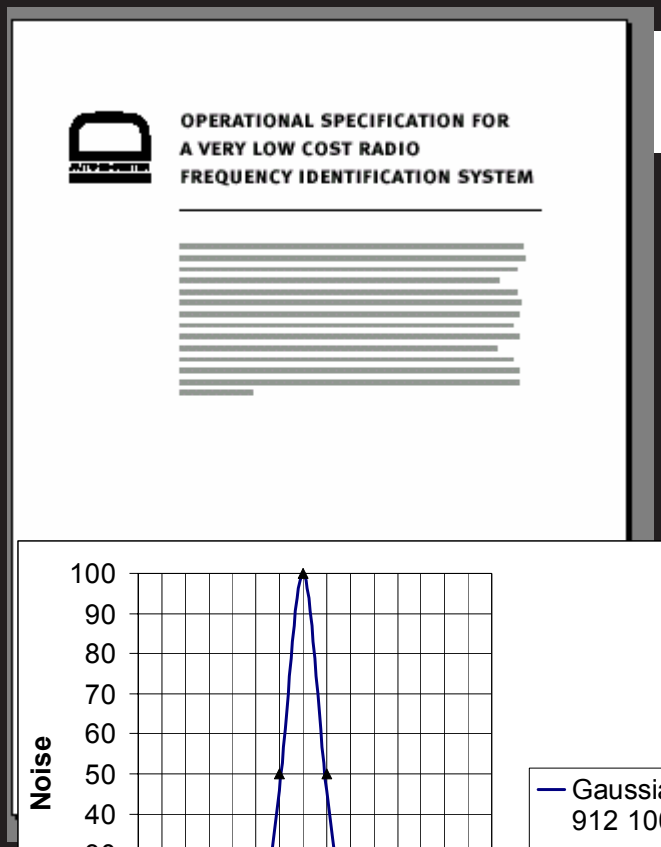
Silicon: 4c/mm^2

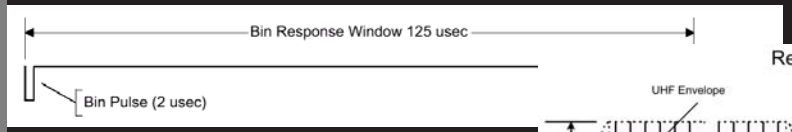


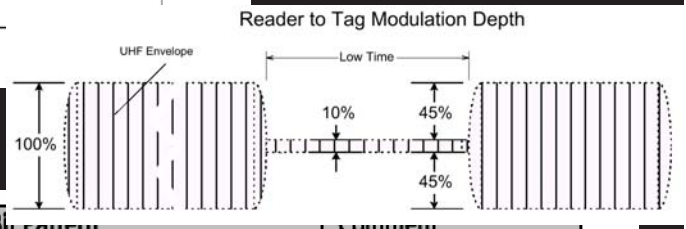
why is rfid expensive today?



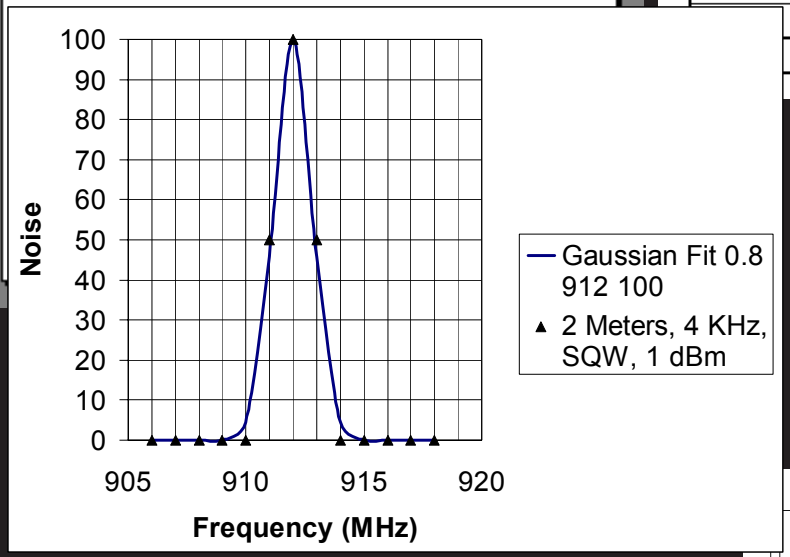
Cheap protocol

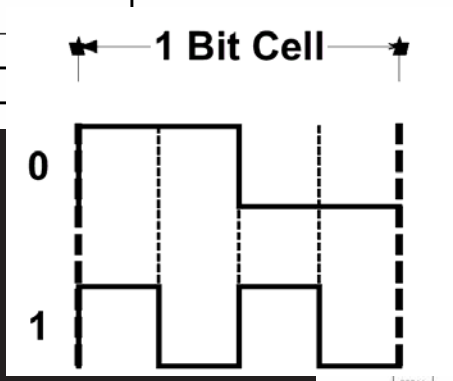


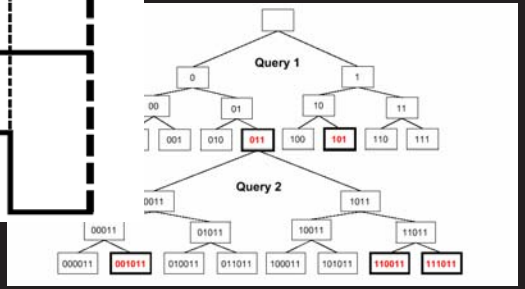


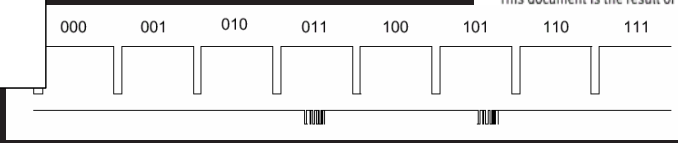


Programming Commands [CMD]	8-Bit Pattern MSB <- LSB	Comment
PROGRAM	0011 0001	
ERASE	0011 0010	After manufacture and Tag has been LOCKed, this bit pattern is used for the WAKE command.





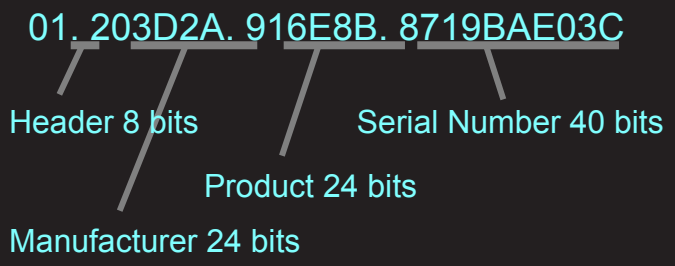




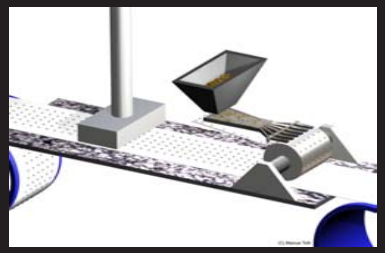
This document is the result of enormous and productive work by the Auto-ID Center's Cheap
esents considerable and ongoing collaboration between Auto-
Researchers at the Massachusetts Institute of Technology,
Technology, with assistance from Rafsec and Thing Magic, as
delaide. We acknowledge and recognize the generous
emarkable expertise of all concerned.

the hypothesis or bet

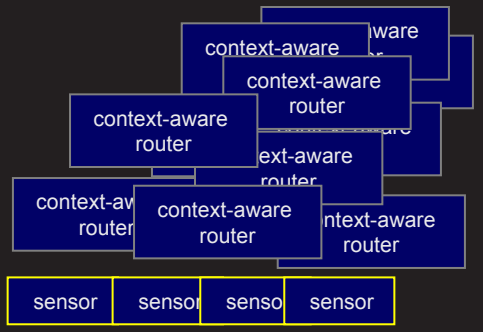
- Place unique number on tag
  - Electronic Product Code, EPC
  - 64 bit, 96 bit, and upwards



- Develop manufacturing technology for small chips and tags



- Move data on the network
  - Network service for resolving EPC
  - Network architecture for gathering and routing data

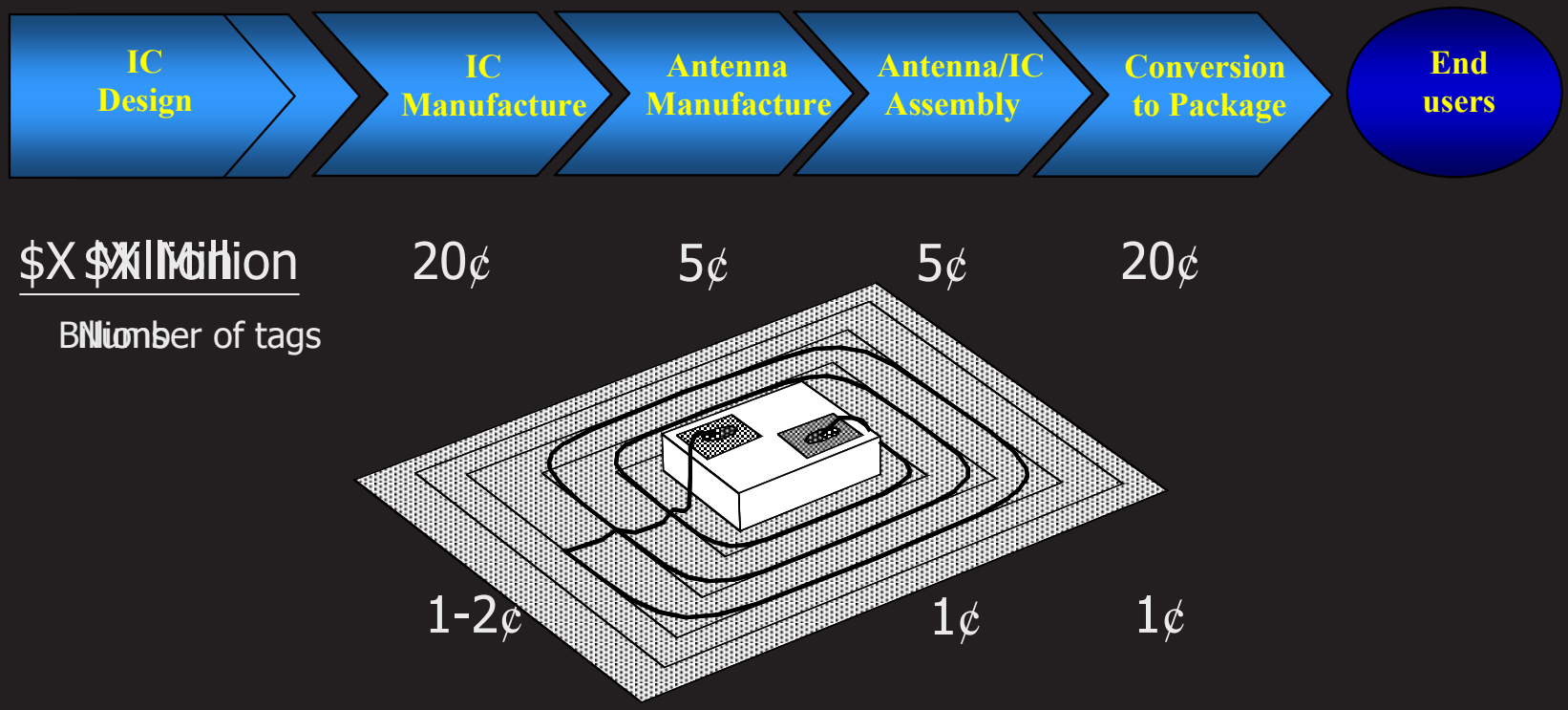


AUTO-ID CENTER

outline

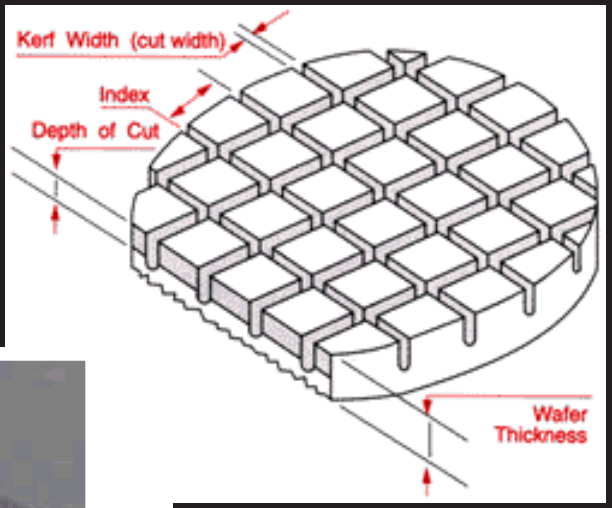
- What and why RFID
- The cost issue
- Manufacturing low-cost RFID
- Handling the data
- Current status

Low cost RFID



Slicing and Dicing

- Standard saw-dicing wasteful
- Instead, use separation by thinning



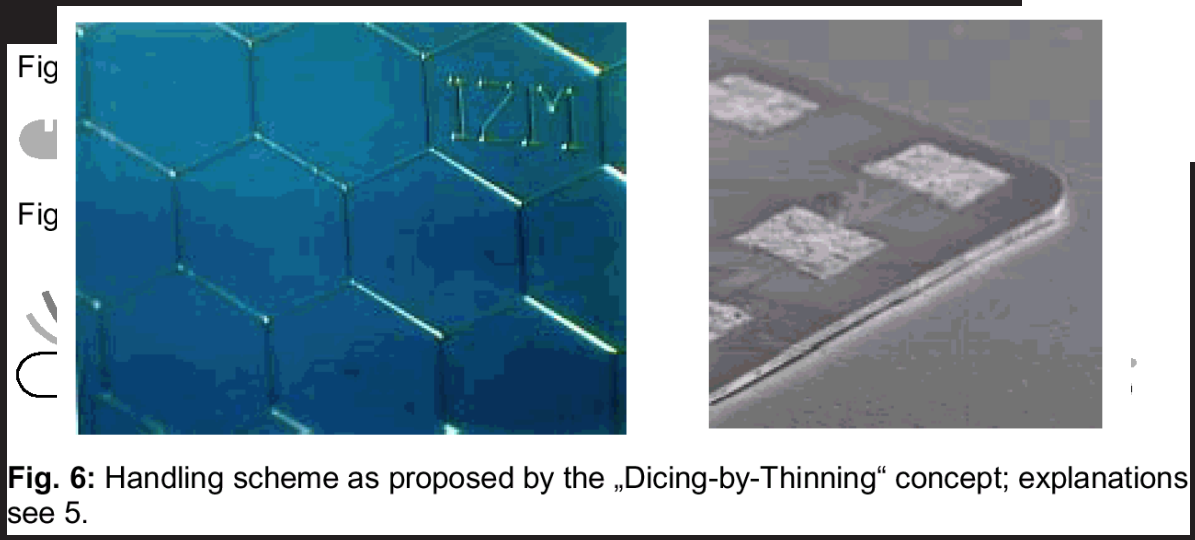
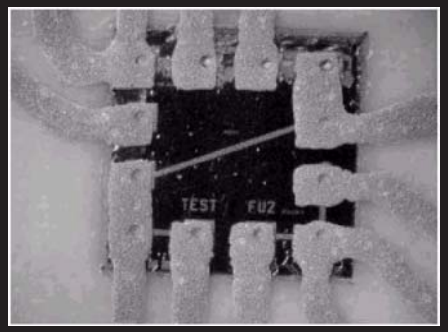


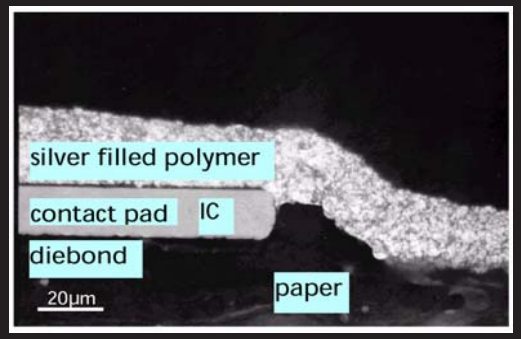
Fig. 6: Handling scheme as proposed by the „Dicing-by-Thinning“ concept; explanations see 5.

C. Landesberger, S. Scherbaum, G. Schwinn, H. Spöhrle: “New Process Scheme for Wafer Thinning and Stress-free Separation of Ultra Thin IC’s,” Proceedings of Microsystems Technologies 2001, Mesago, Stuttgart, pp. 431-436, 2001.

Antenna

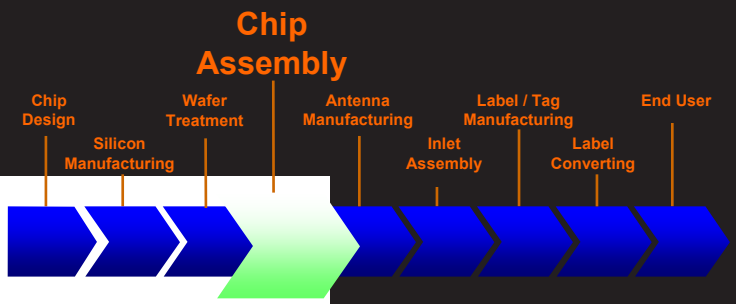
- Screen printing
- Etching
- Forming

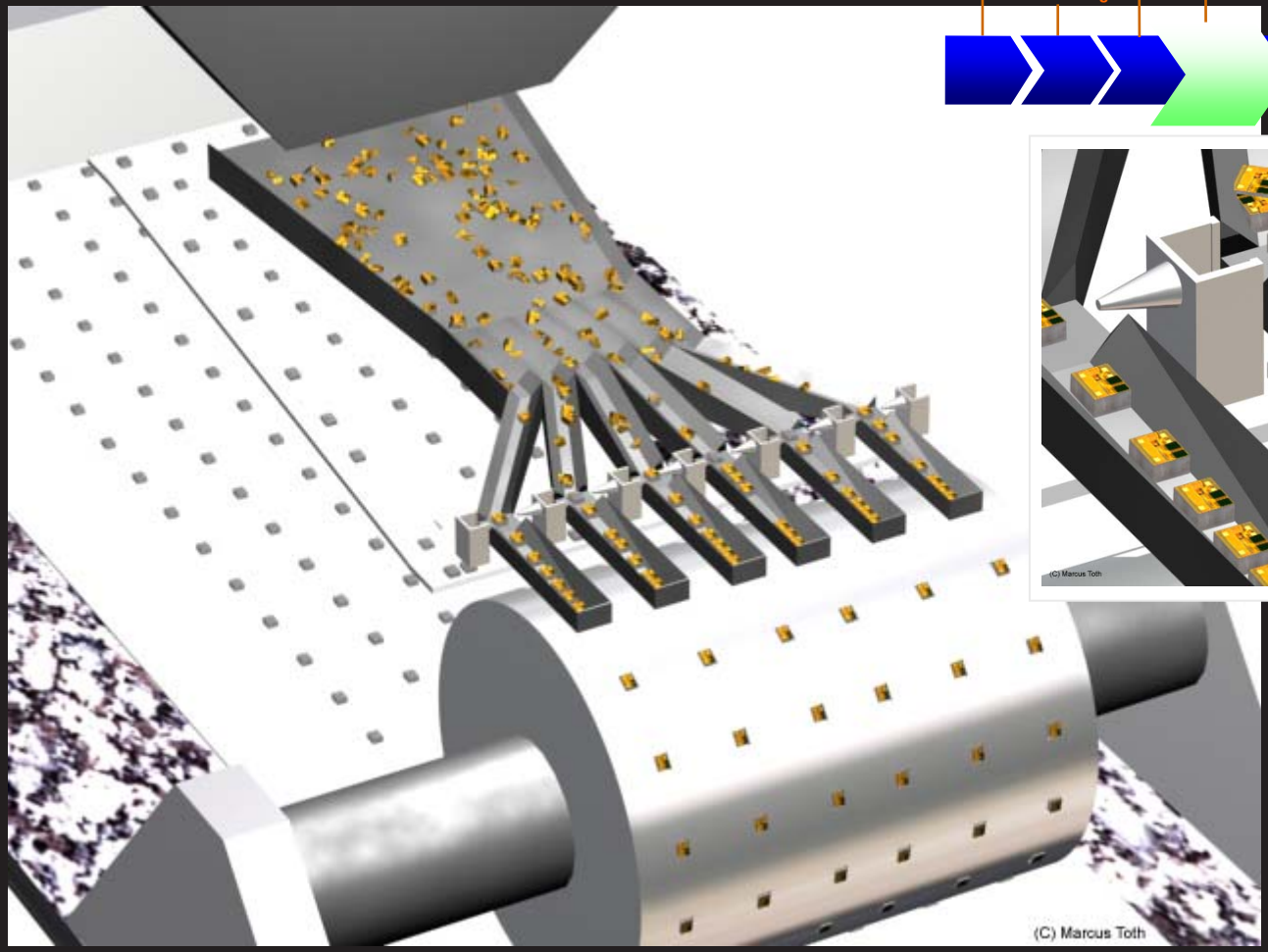


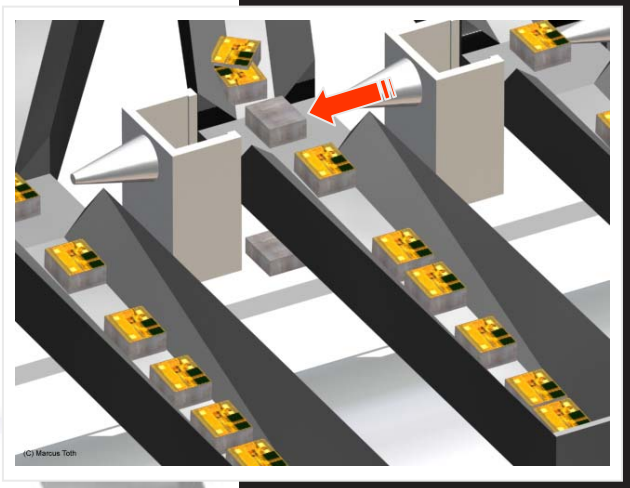


M. Feil, C. Adler, G. Klink & M. König: "Interconnection Techniques for Ultra Thin ICs and MEMS Elements", Proceedings of Microsystems Technologies 2001, Mesago, Stuttgart, pp. 437-442, 2001.

vibratory Assembly



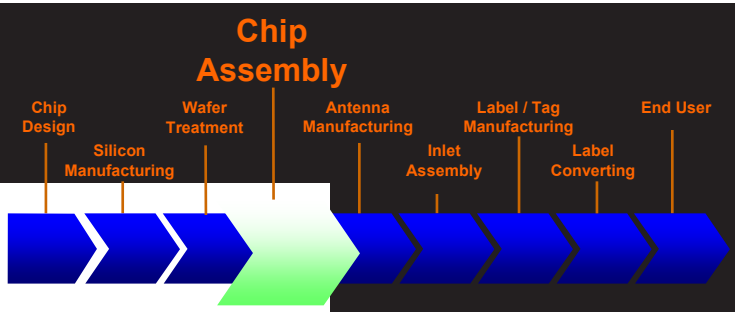


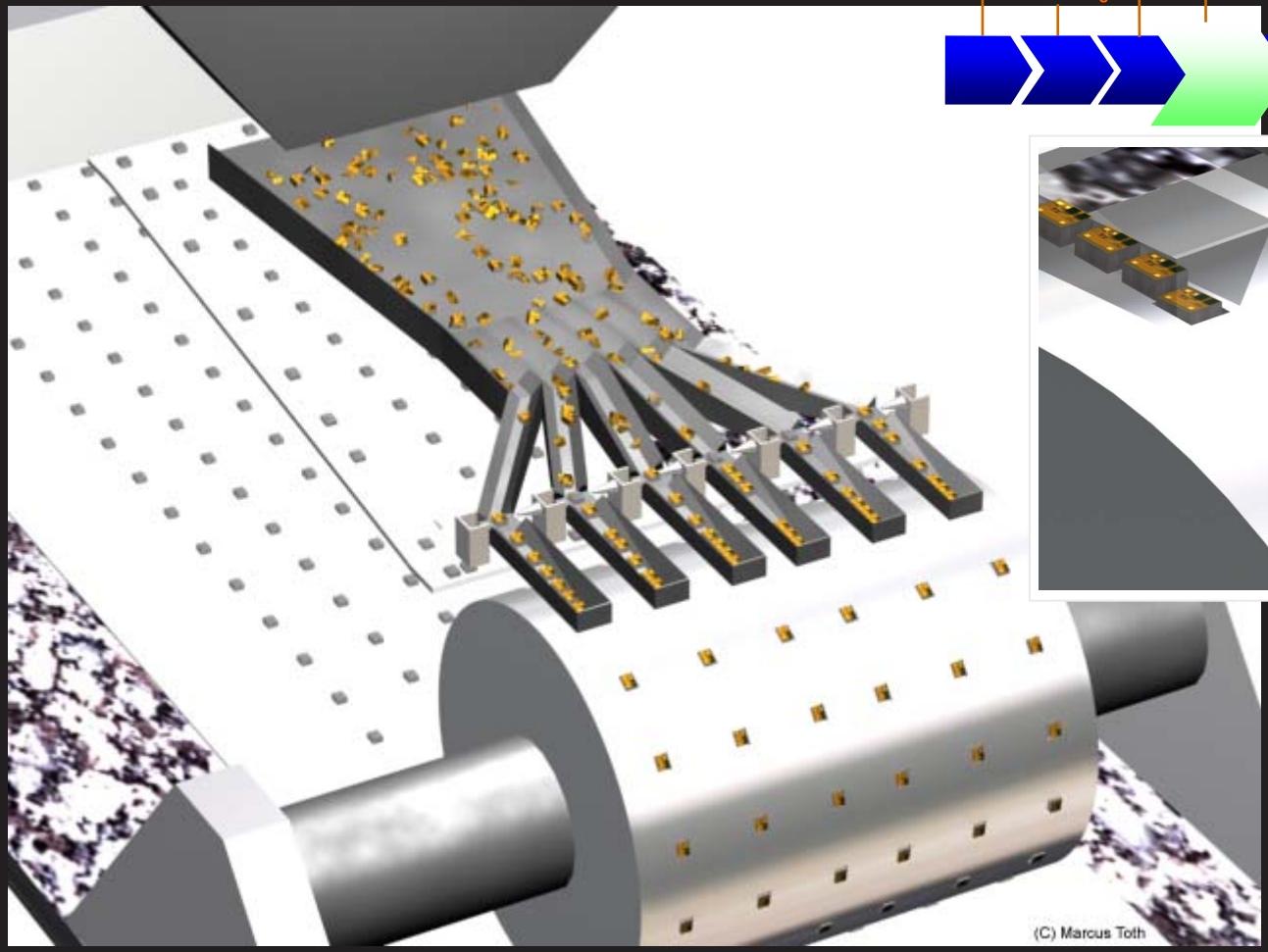


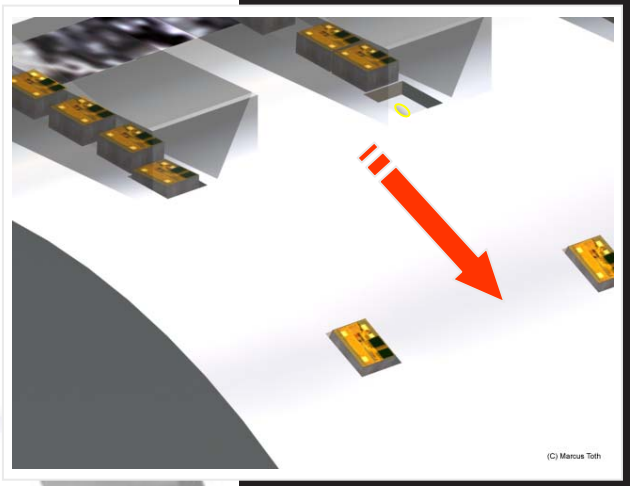
Orientation Check

Courtesy Philips

vibratory assembly





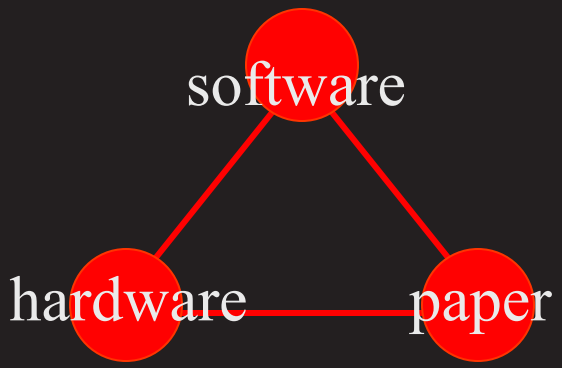


Vacuum cylinder

Courtesy Philips

conversion

- Paper/package/label industry expertise
- Scales well with mass production
- Capital equipment expenditure

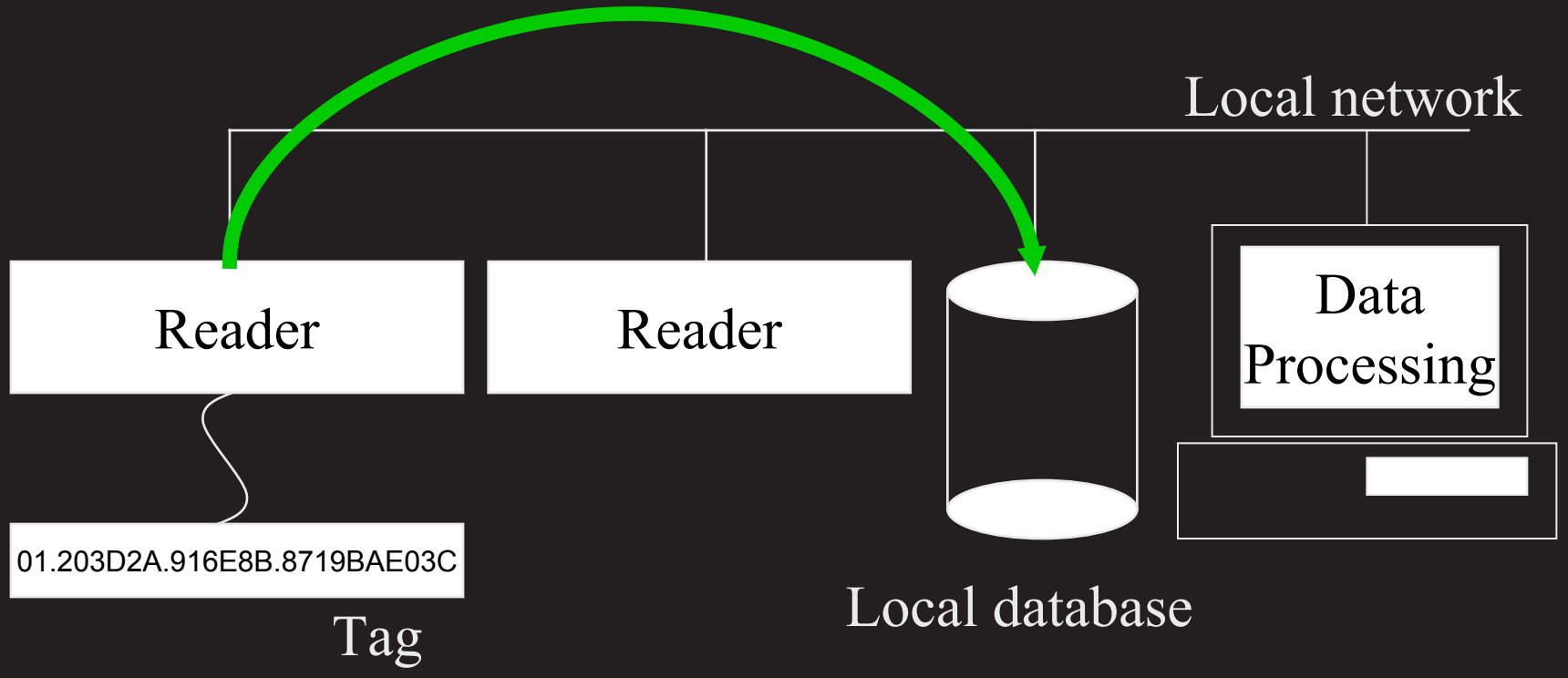


AUTO-ID CENTER

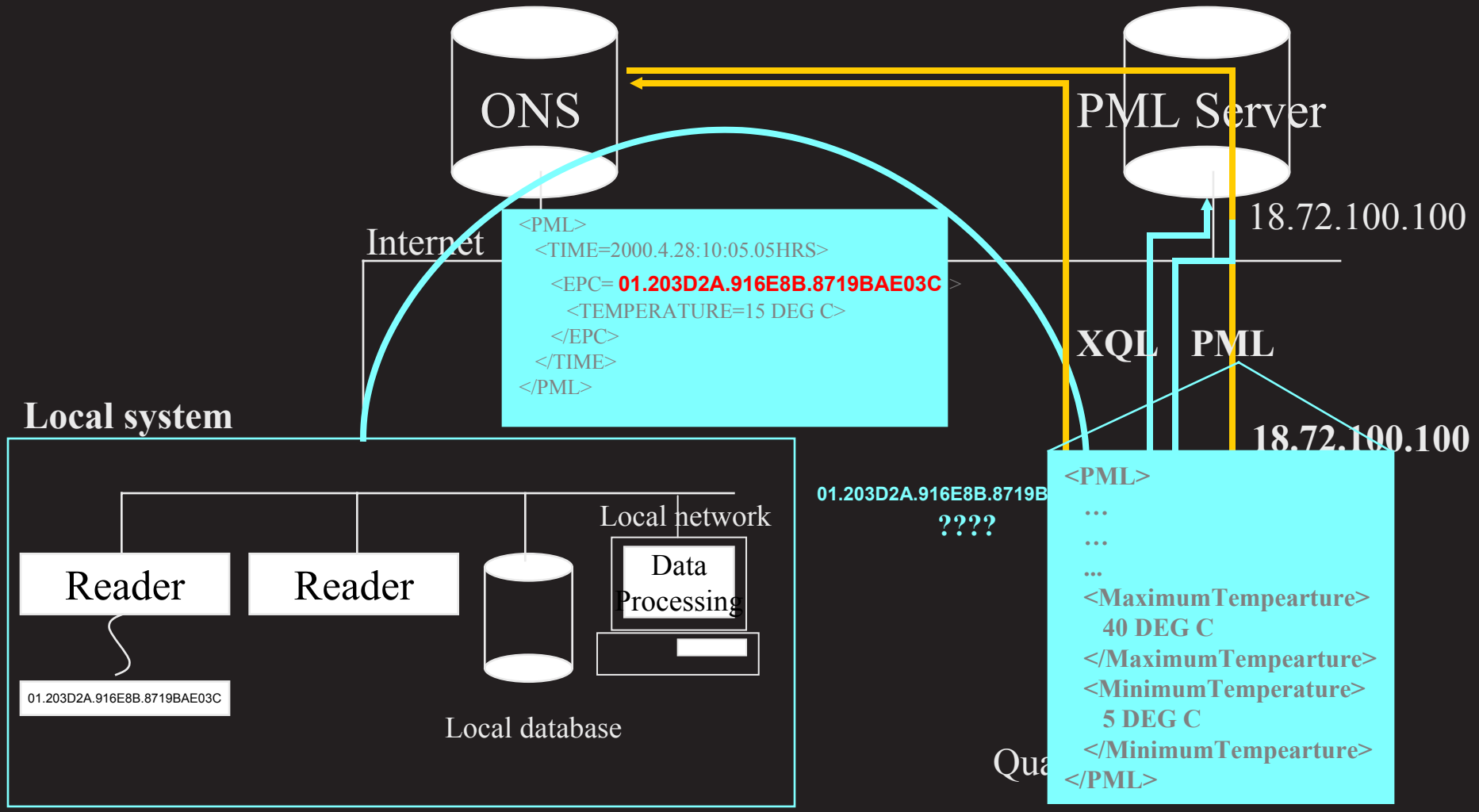
outline

- What and why RFID
- The cost issue
- Manufacturing low-cost RFID
- Handling the data
- Current status

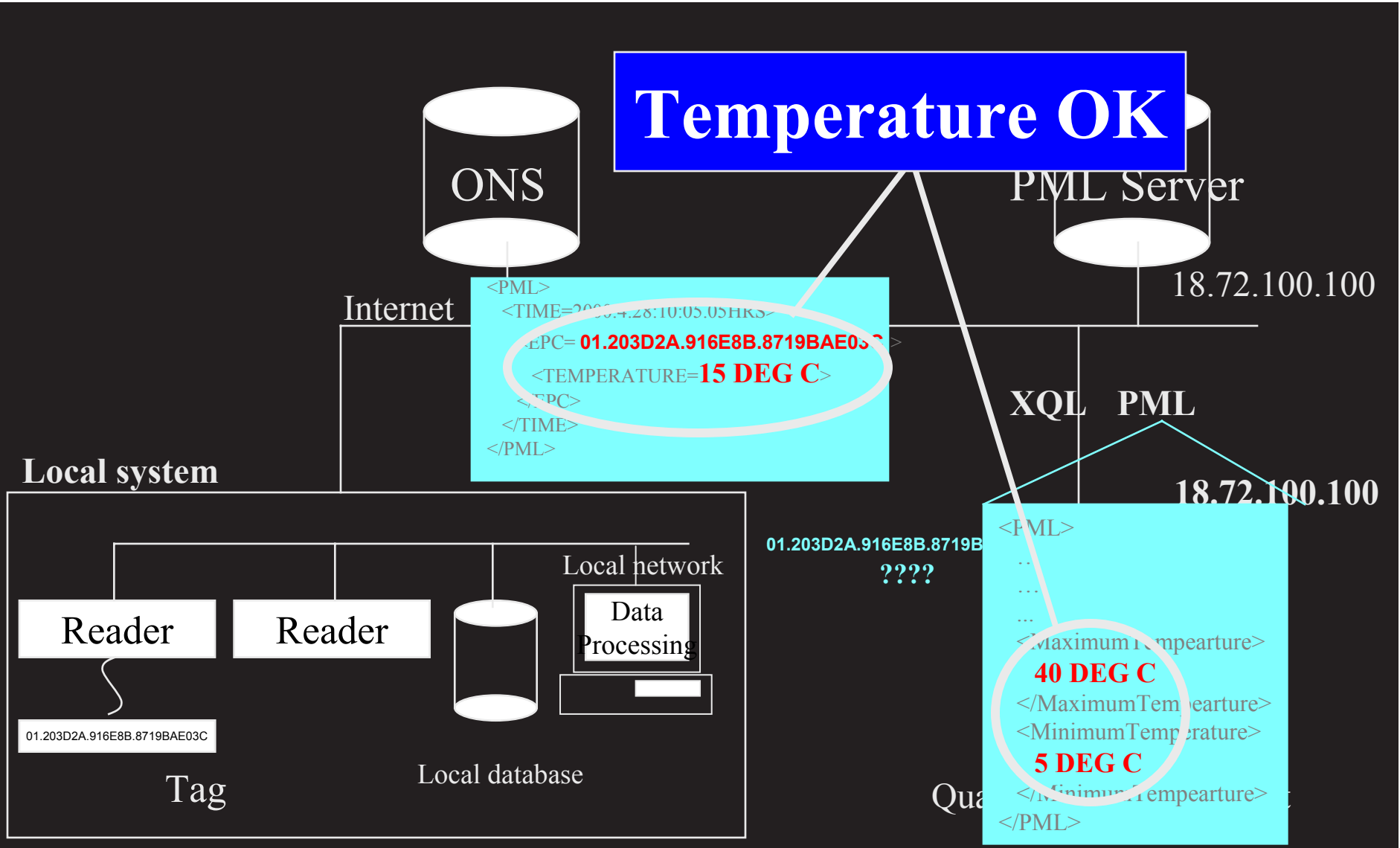
Architecture: Local



Architecture: Global



Inference


Temperature OK
ONS
PML Server
18.72.100.100
Internet
<PML>
<TIME=
EPC= 01.203D2A.916E8B.8719BAE03C
<TEMPERATURE=15 DEG C>
</TIME>
</PML>
XQL
PML
Local system
18.72.100.100
01.203D2A.916E8B.8719B
????
<PML>
40 DEG C
</MaximumTemperature>
<MinimumTemperature>
5 DEG C
</PML>
Local network
Reader
Reader
Data Processing
01.203D2A.916E8B.8719BAE03C
Tag
Local database

AUTO-ID CENTER

outline

- What and why RFID
- The cost issue
- Manufacturing low-cost RFID
- Handling the data

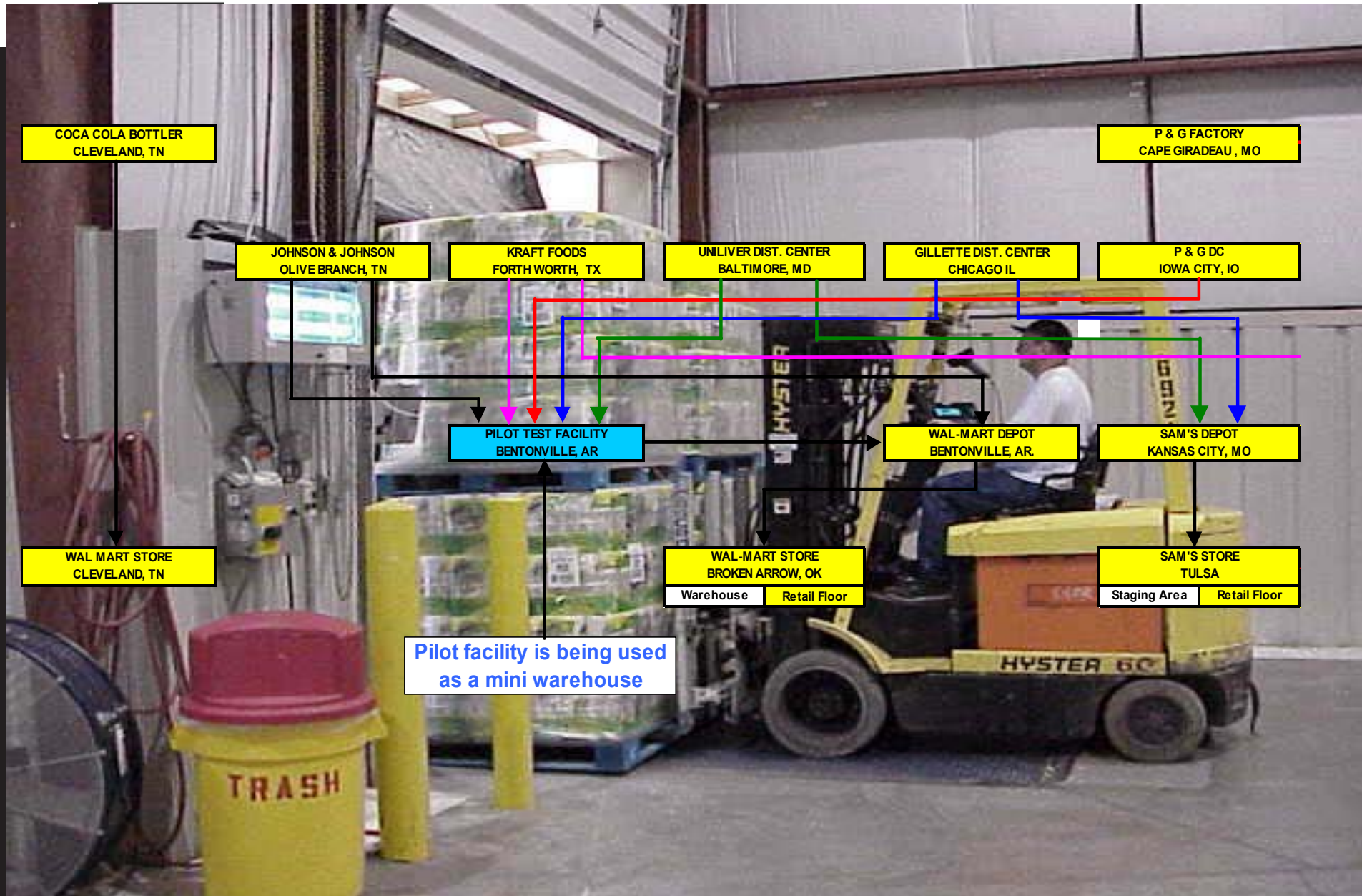
- Current status

Status of center

- Research
  - RFID/routing software technology: MIT & Adelaide
  - Manufacturing /Control Applications: Cambridge
- Standards
  - Air-interface between reader and tags
  - Software for handling/routing data
- Sponsorship
  - 48 sponsors
  - 4 continents

AUTO-ID CENTER

field trial



outline

- RFID and the Auto-ID Center
- Protocols
- Security issues

AUTO-ID CENTER

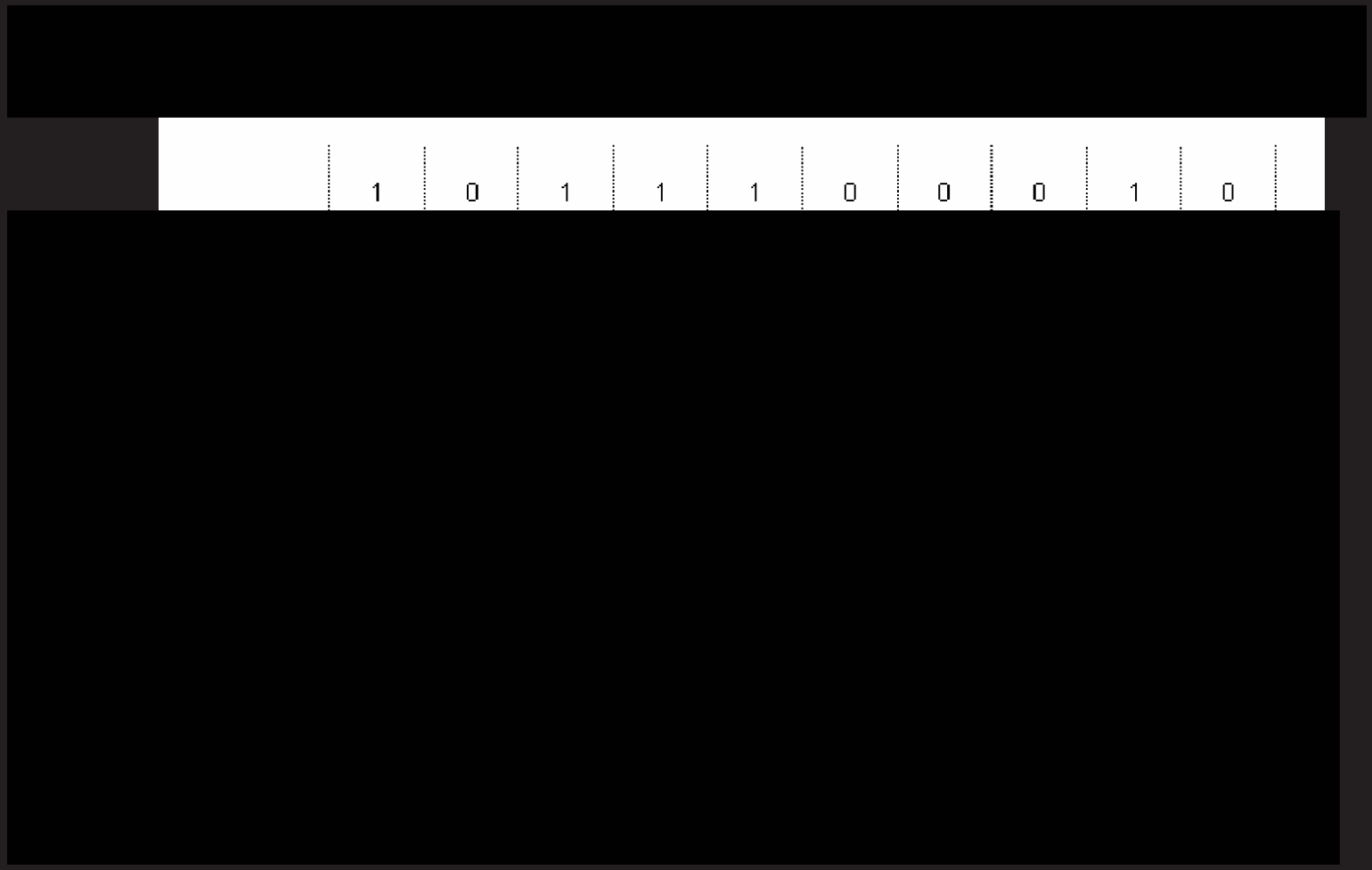
components

- Signaling
- Anti-collision
- Functions

Things to keep in mind

- You will not read one tag: you will read many!
- Bandwidth becomes an issue

Line codes

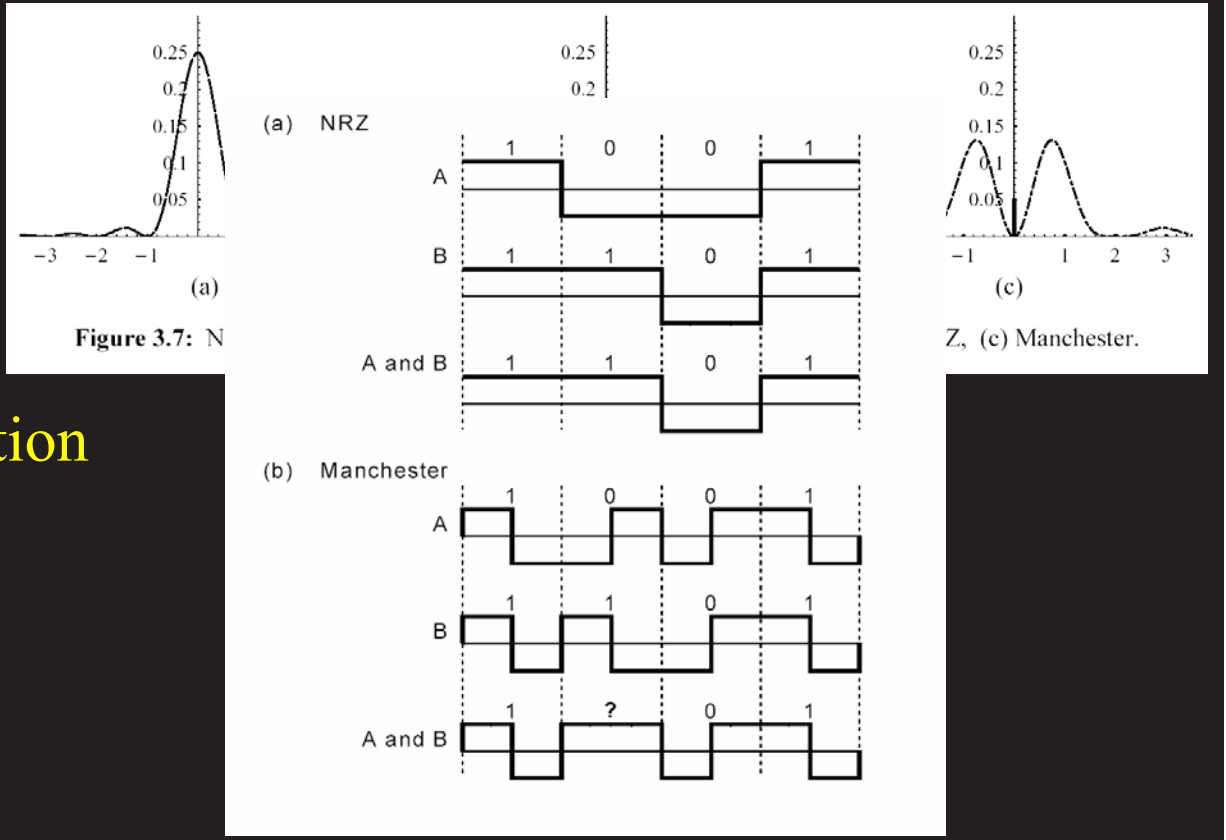


trade-offs

Probability of error

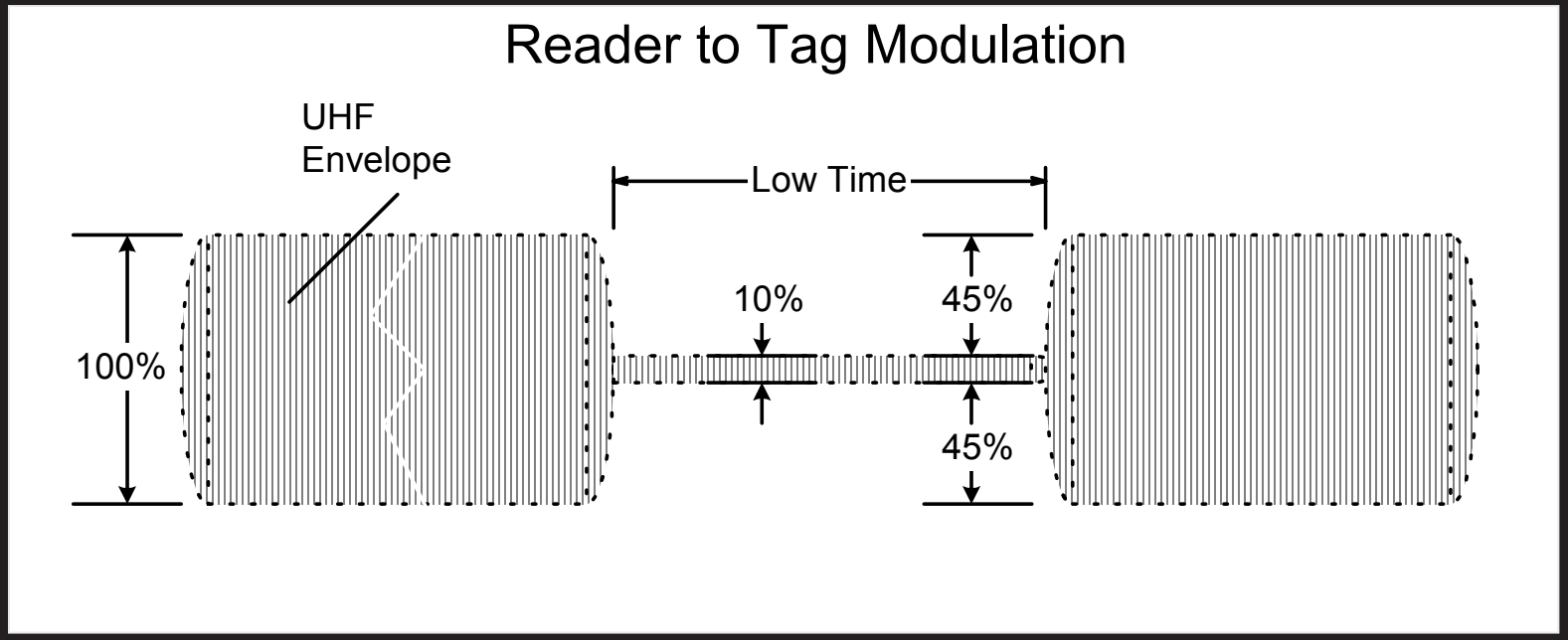
Bandwidth

Collision detection



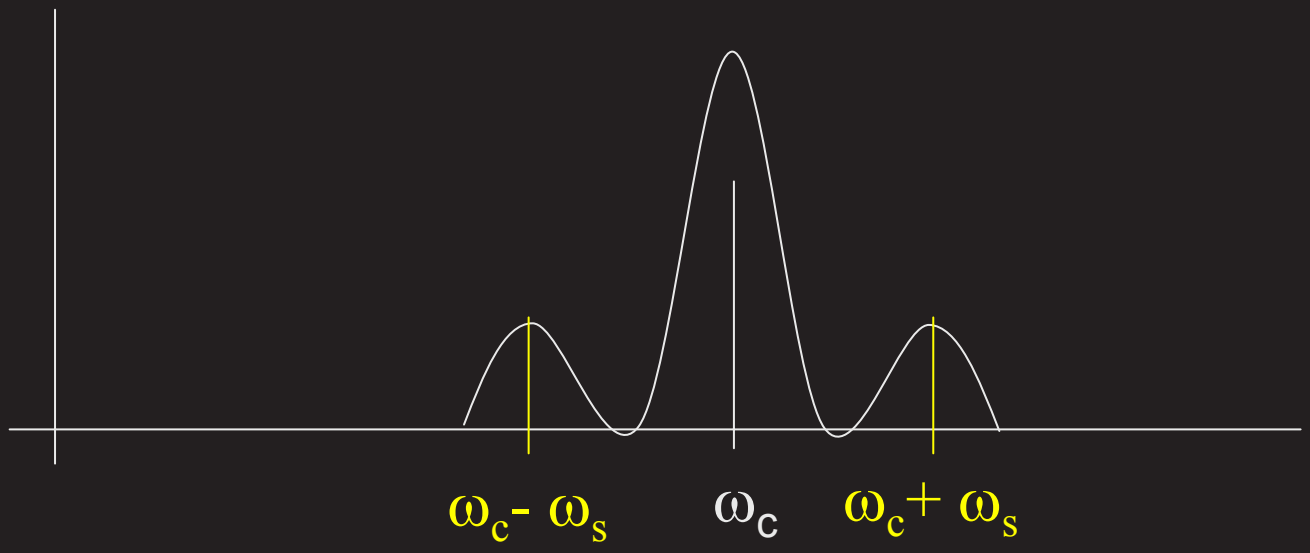
modulation

- Amplitude Shift Keying
- Phase shift keying
- Frequency shift keying

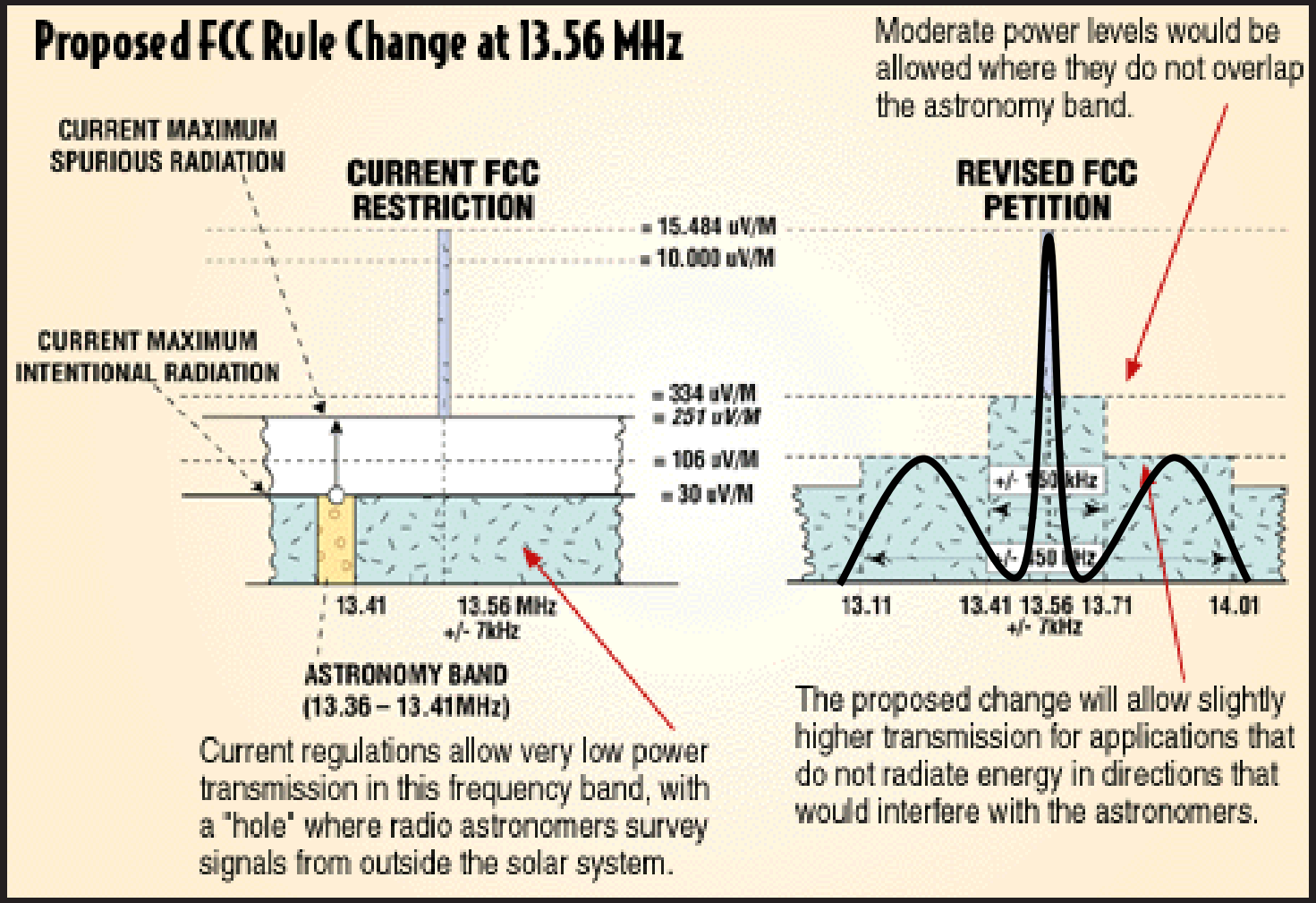


Bandwidth

$$\cos(\omega_c)\cos(\omega_s) = \frac{\cos(\omega_c + \omega_s) + \cos(\omega_c - \omega_s)}{2}$$



bandwidth


Proposed FCC Rule Change at 13.56 MHz
Moderate power levels would be allowed where they do not overlap the astronomy band.
CURRENT MAXIMUM SPURIOUS RADIATION
CURRENT FCC RESTRICTION
= 15.484 uV/M
= 10.000 uV/M
CURRENT MAXIMUM INTENTIONAL RADIATION
= 334 uV/M
= 251 uV/M
= 106 uV/M
= 30 uV/M
13.41
13.56 MHz
+/- 7kHz
ASTRONOMY BAND
(13.36 – 13.41MHz)
Current regulations allow very low power transmission in this frequency band, with a "hole" where radio astronomers survey signals from outside the solar system.
REVISED FCC PETITION
13.11
13.41 13.56 13.71
+/- 7kHz
14.01
The proposed change will allow slightly higher transmission for applications that do not radiate energy in directions that would interfere with the astronomers.

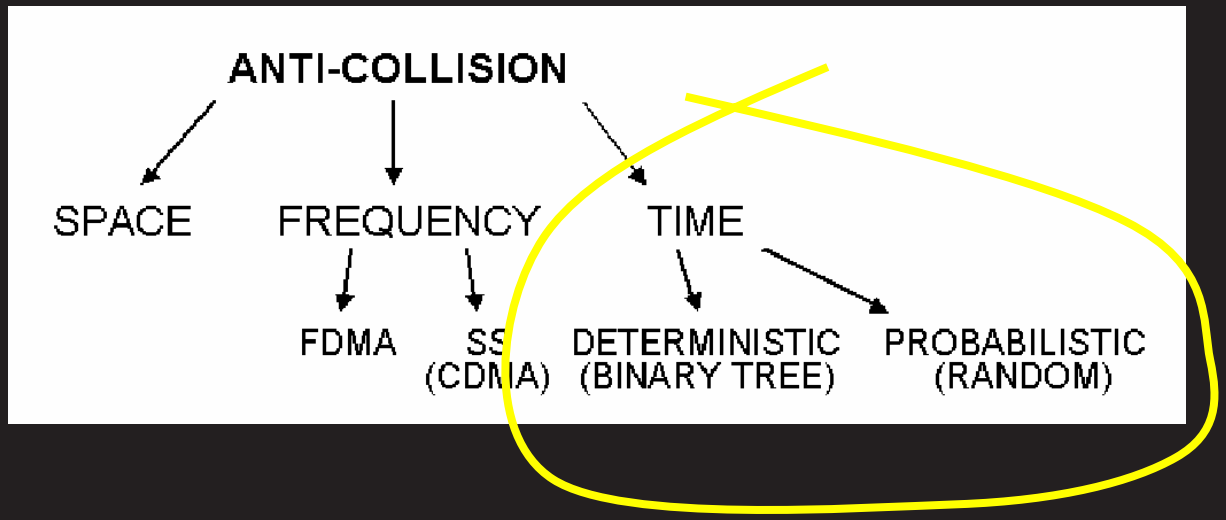
AUTO-ID CENTER

components

- Signaling
- Anti-collision
- Functions

anticollision

- Multiple tags in the field
- Need to be sorted
- Tags relatively dumb



aloha protocols

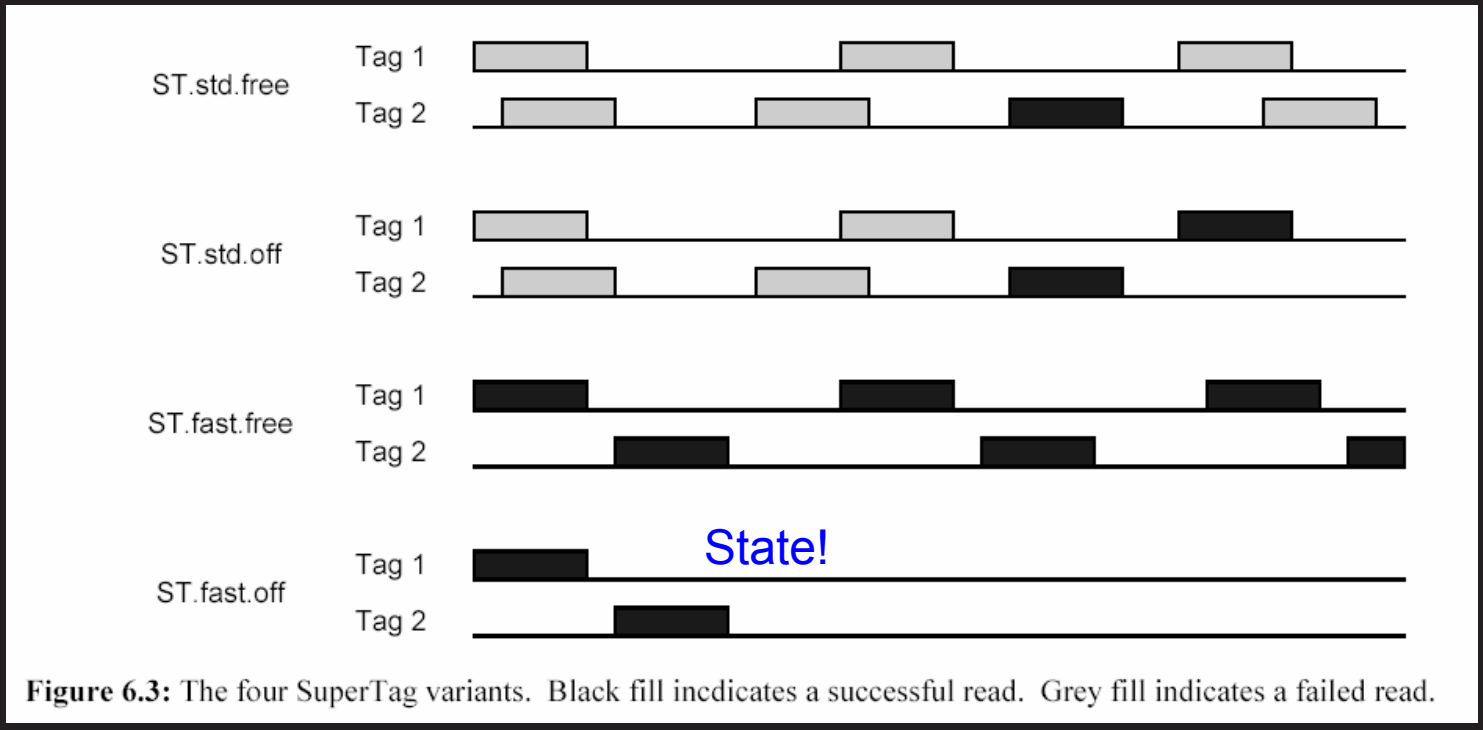
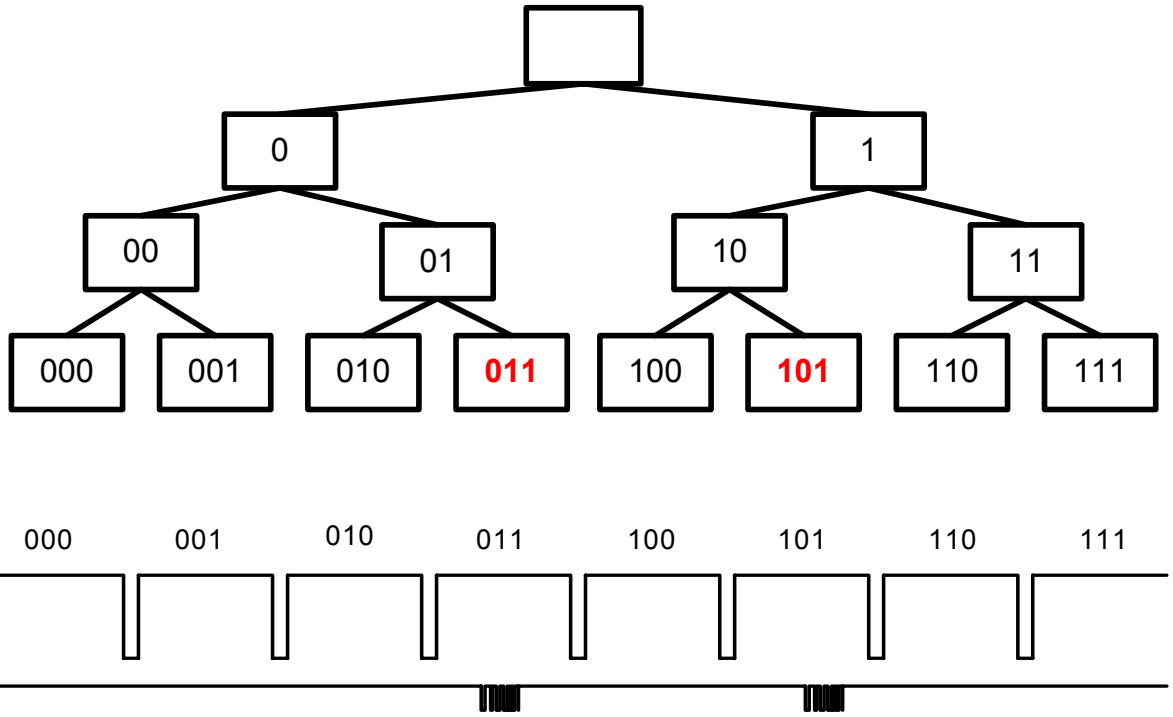


Figure 6.3: The four SuperTag variants. Black fill incdicates a successful read. Grey fill indicates a failed read.

tree walking

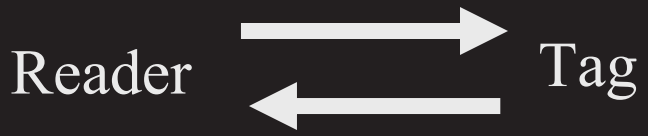


Aloha vs tree-walking

Asymmetric

Aloha schemes
13.56 MHz ISM

Symmetric



Tree schemes
915 MHz ISM

AUTO-ID CENTER

anticollision

- The backbone function
- Extract unique ID
- Must leverage for any security scheme

AUTO-ID CENTER

components

- Signaling
- Anti-collision
- Functions

Functions

One time

- Write address
- Lock address
- Pointer
- Read ID (anti-collision)
- Read payload
- Write payload
- Sleep
- Wake
- Destroy

How to interpret standards

RFID Technologies Using the 13.56MHz Frequency (Proposed Methods)

Format		Proximity type			Vicinity type	
ISO		14443			15693	
Type		Type A	Type B	Type C	Type X	Type Y
Communication Distance (cm)		>10 cm	>10 cm	>10 cm	>10 cm	>10 cm
Transfer from reader/writer to card (Downlink)	Carrier Frequency (fc)	13.56MHz	13.56MHz	13.56MHz	13.56MHz	13.56MHz
	Digital Modulation Type	ASK	ASK	ASK	ASK	ASK
	Modulation (Modulation Level)	AM100%	AM10+/-2%	AM10%	AM100%	AM10%
	Power Pause Time	2.95 µs	0 µs	0 µs	11.1 µs	0 µs
	Subcarrier Frequency	None	None	None	None	None
	Required Bandwidth	+/-(1/Power Pause Time)	+/- communication speed x 1	+/- communication speed x 2	+/-(1/Power Pause Time)	+/- communication speed x 2
	Data Rate (kbps)	105.9375(fc/128) 211.875(fc/64)	105.9375(fc/128) 211.875(fc/64)	105.9375(fc/128) 211.875(fc/64)	6.2 to 9	1.6 to 26.5
	Bit Coding	Modified Miller	NRZ	Manchester	Pulse Width	Pulse Position
	Self-clock in Data	Self-clock	No self-clock	Self-clock	Self-clock	Self-clock
	Peak Difference between Main and Sideband	Approx. 14 dB	Approx. 28 dB	Approx. 28 dB	Approx. 14 dB	Approx. 28 dB
Transfer from card to reader/writer (Uplink)	13.56MHz transmission from reader/writer	Load Modulation	Load Modulation	Load Modulation	Load Modulation	Load Modulation
	Communication with reader/writer	Reader/writer Talk first *1	Reader/writer Talk first *1	Reader/writer Talk first *1	Reader/writer Talk first *1	Reader/writer Talk first *1
	Digital Modulation Type	ASK Subcarrier	BPSK Subcarrier	ASK	FSK Subcarrier	ASK Subcarrier
	Subcarrier Frequency	847.5kHz(fc/16)	847.5kHz(fc/16)	None	423.75kHz(fc/32) 484.2857kHz(fc/28)	423.75kHz(fc/32)
	Data Rate (kbps)	105.9375(fc/128) 211.875(fc/64)	105.9375(fc/128) 211.875(fc/64)	105.9375(fc/128) 211.875(fc/64)	26.7	1.6 to 26.5
	Bit Coding	Manchester	NRZ	Manchester	Manchester	Manchester

outline

- RFID and the Auto-ID Center
- A peek at the protocol
- Security issues

- Discussions with: Dan Engels, Peter Cole, Steve Weiss, Ron Rivest

AUTO-ID CENTER

Does protocol compromise privacy?

Not necessarily. Your choice.

You can destroy the tag and opt out

or

You can keep tag for later use
(physics is your friend)

AUTO-ID CENTER

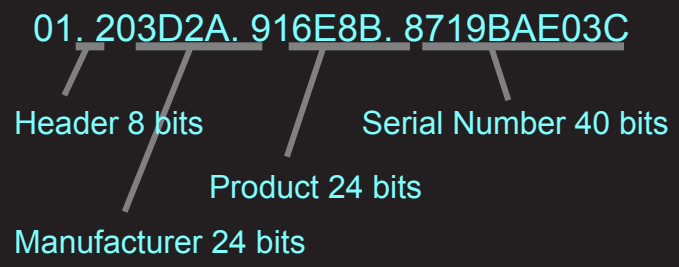
mass hijack of tags

- Could happen in destroy or re-programming
- Physics our friend
  - Bandwidth limited: 200 tags a second anti-collision
  - Destroy must be individually addressed
  - So it takes time to kill
  - Surveillance

For the future: issues

- Tags are light-weight

- Anyone can read the tags (promiscuity)
- The same number shows up all the time
- Channel is open and shared



AUTO-ID CENTER

problem: unique and promiscuous

Kill Serial number?

- Product still readable
- Person can be tracked by constellation

Personalize the number?

- Repeated reads yield same number
- You could still be tracked by constellation

AUTO-ID CENTER

using keys – iteration 1

- Tag, reader share a key
- They challenge each other
- They establish trust
- The communicate

But wait:

There still needs to be a unique number for anticollision

Key management problem

rolling number

$Temporary\_number = Key\{ID|nonce\}$

Perform anticollision on $Temporary\_number$

Extract ID

Advantages:

- Promiscuous, but who cares
- Can't track
- No privacy issue

Disadvantage:

- Still a key management problem

Acknowledgement: Peter Cole, Ron Rivest

keyless approach

$lock = hash(key)$

Tag knows *hash* and *lock*
Lock used as ID and for anticollision

Administrative functions

Reader provides *key*
Tag computes *computed_lock*
If *computed_lock* == *lock*,

then tag unlocked,
ready for administration until new *lock*

AUTO-ID CENTER

administering the tag

Problems

- Air interface always vulnerable
- Grey area of ownership in retail

Solutions

- Physical contact for reprogramming
- Physical contact reset of memory

(Resurrected duckling, University of Cambridge)

AUTO-ID CENTER

conclusions

- RFID is here
- As more functionality goes on RFID, security challenges
- 0.2 milli-cents per gate, cost is paramount
- Minimize data on tag