Modello ISO-OSI – elementi

- ISO-OSI International Standard Organization -Open System Initiative
- Standard internazionale dal 1983.
- Basato sull'architettura a strati (layer) o livelli
- Ogni problema viene scomposto i SOTTOPROBLEMI più semplici
- Rende i vari strati INDIPENDENTI
- Di ogni strato definisce soltanto SERVIZI e INTERFACCE. Ogni livello puo' essere sviluppato indipendentemente dagli altri, e da enti diversi.
- Nell'OSI vengono definiti:
  - Il modello di riferimento (schema, numero degli strati, funzioni di ciascuno strato)
  - I servizi
  - I protocolli e le interfacce

ISO:OSI Modello di Riferimento

- Architettura a 7 strati

7 -Strato di Applicazione – Application
6 - Strato di Presentazione – Presentation
5 - Strato di Sessione – Session
4 - Strato di Trasporto – Transport
3 - Strato di Rete – Network
2 - Strato di Linea – Datalink
1 - Strato Fisico – Physical Layer

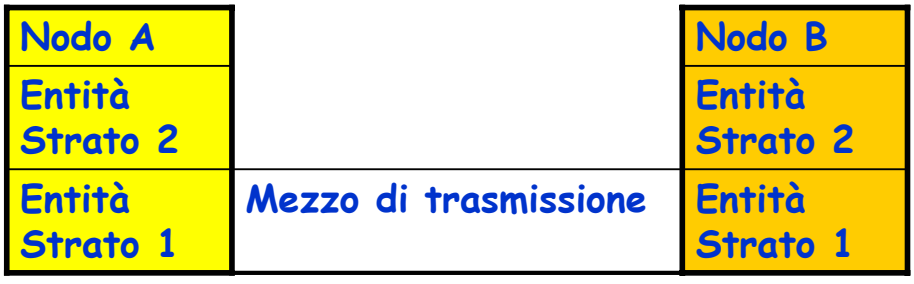
- Gli strati più bassi (1,2,3) sono orientati alla rete (network oriented), nel senso che definiscono la struttura completa della rete.
- Gli strati più alti (5,6,7) sono orientati alle applicazioni (application oriented), nel senso che sono utilizzati dai programmi dell'utente finale della rete (end-to-end).
- Lo strato di trasporto (4) e' uno strato di raccordo

Strato Fisico – Physical Layer – 1 -

- Ha il compito di attivare, mantenere e infine chiudere la connessione tra due entità di strato 2. Un'ENTITA' è l'elemento logico (la macchina a stati) di un nodo della rete attivo su uno specifico strato.
- Specifica le modalità di invio del singolo bit sul mezzo di trasmissione
- Deve specificare le caratteristiche ELETTRICHE, MECCANICHE, PROCEDURALI, FUNZIONALI dei vari segnali
- Lo strato fisico, in particolare, specifica i seguenti aspetti:
  - Velocità di trasmissione
  - Lunghezze dei collegamenti ed estensione della rete
  - Compatibilità con l'ambiente di istallazione
  - Adattabilità su impianti pre-esistenti
  - Mezzo di trasmissione

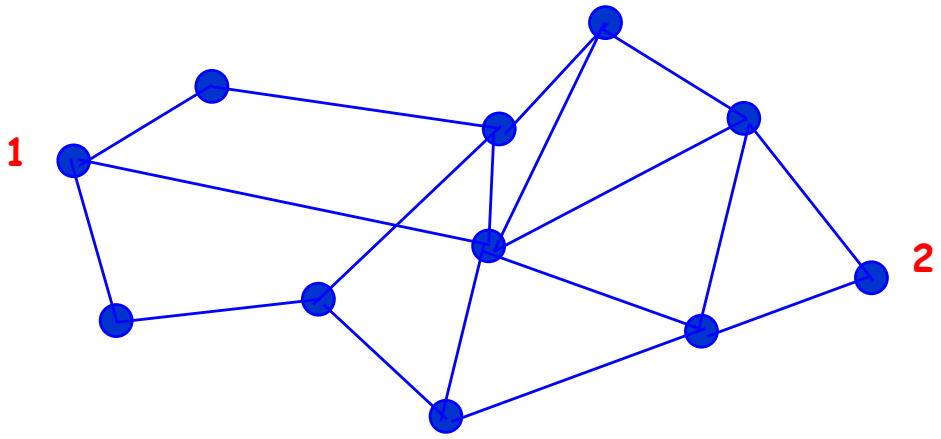
Strato di Linea – Data Link Layer – 2 -

- Deve attivare, mantenere e disattivare la connessione FISICA tra due entità di livello 3.
- Deve rendere affidabile il collegamento (punto-punto) tra nodi adiacenti.
- Struttura il flusso dei dati in "frame" (trame), controlla e gestisce gli errori di trasmissione, controlla il flusso dei dati, e le sequenze trasmesse



Strato di Rete – Network Layer – 3 -

- Deve far giungere i "pacchetti" a destinazione
- Si occupa dell'istradamento ("routing") dei pacchetti cioè di determinare la sequenza di collegamenti punto-punto necessari per trasmettere un pacchetto da un nodo generico della rete a un altro.



Strato di Trasporto – Transport Layer - 4

- Deve fornire un canale sicuro End-to-End per trasferimento di "file".
- Adatta la dimensione dei file forniti agli strati superiori ai pacchetti richiesti dallo strato di Rete (frammentazione/riassemblaggio)

Strato di Sessione – Session Layer - 5

- Assembla il dialogo tra nodi in unità logiche (sessioni)

Relazione
Strato <-> Unità elementare di informazione

- Per i primi 5 strati abbiamo la seguente corrispondenza tra strato e unità elementare di informazione trattata:

Strato di Sessione	Sessione
Strato di Trasporto	File
Strato di Rete	Pacchetto
Strato di Collegamento	Trama
Strato Fisico	Bit

Strato di Presentazione – Presentation Layer - 6

- Adatta la sintassi dei dati di ciascuna applicazione alla sintassi richiesta dalla sessione (sintassi di trasferimento).
- E' lo strato intermedio tra il programma utente vero e proprio e lo strato di sessione. Serve essenzialmente nel caso in cui i dati che vengono usati dal programma applicativo abbiano un formato molto diverso da quello dei dati utili per lo strato di sessione. In molti casi, gli strati 5-6-7 vengono compressi in un unico strato.

Strato di Applicazione– Application Layer - 7

- E' l'utente della rete di calcolatori, e non deve fornire servizi a nessuno. Rappresenta il programma di applicazione che deve comunicare con altri calcolatori remoti.

Concetto di Servizi

- Nel modello ISO-OSI ogni strato fornisce SERVIZI al livello superiore e usa i SERVIZI forniti dal livello inferiore.
- Due strati adiacenti interagiscono solo tramite i servizi.
- Per ogni strato N si puo' definire:
  - N-service provider: cioè un fornitore di servizi a livello N, cioè lo strato N e tutti gli strati inferiori di cui N fa uso.
  - N-service user: è l'entità dello strato N+1 che fa uso dei servizi forniti dal livello N
- I servizi sono descritti da PRIMITIVE DI SERVIZIO, che forniscono una rappresentazione astratta dell'interazione Tra N-service provider e N-service user.
- Le primitive di servizio si dividono in 4 tipi:

  request, indication, response, confirm

Primitive di servizio

SERVIZIO CONFERMATO:

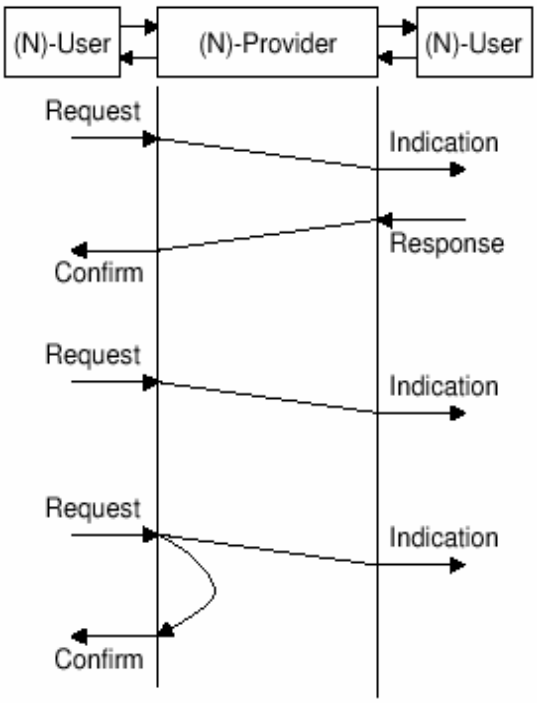
- L'N-User richiede all'N-Provider un servizio (Request).
- L'N-user destinatario riceve la richiesta di servizio dall'N-Provider (Indication).
- L'N-user destinatario conferma la ricezione con la primitiva (Response).
- L'N-user riceve dall'N-Provider la conferma, con la primitiva Confirm.

SERVIZIO NON CONFERMATO.

Sono usate solo le primitive Request e Indication.

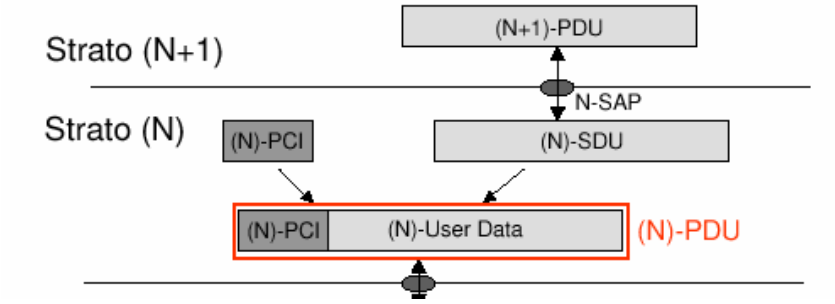
SERVIZIO PARZIALMENTE CONFERMATO

La primitiva confirm viene inviata dal N-service provider, senza che l'N-user di destinazione abbia risposto.



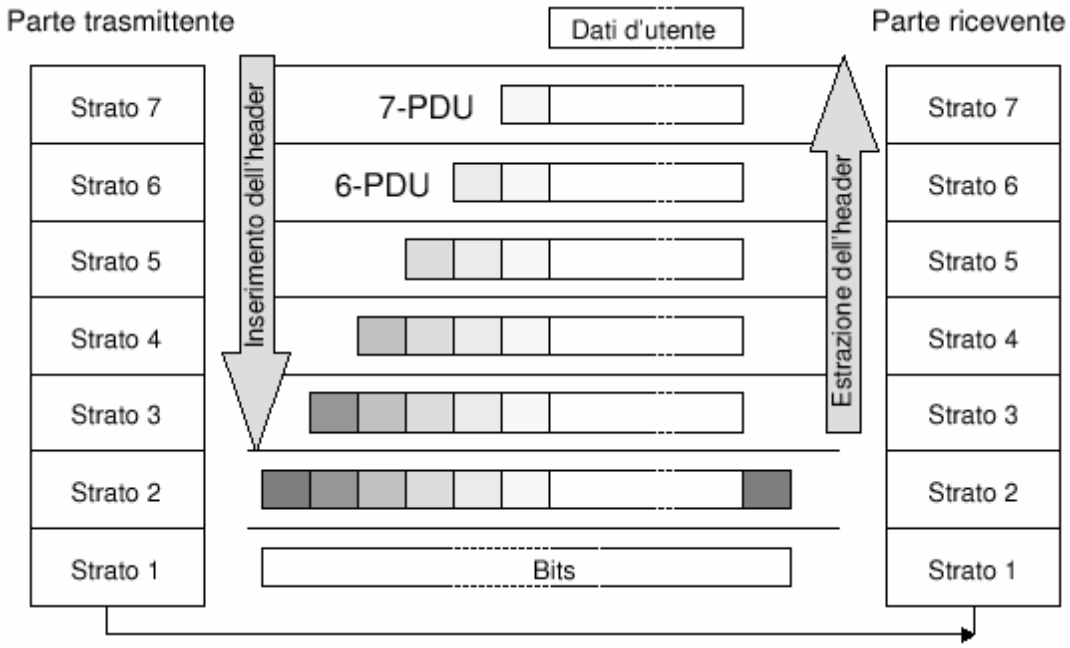
Procedura di Incapsulamento

- Un N-SAP (Service Access Point di livello N) è un l'interfaccia logica tra un entità di strato N+1 e una di strato N attraverso cui viene fornito un servizio.
- (N+1)–PDU (Protocol Data Unit) rappresenta i dati che vengono trasmessi tra entità di pari livello (N+1)
- N–SDU (Service Data Unit) rappresenta i dati passati al livello inferiore (N) attraverso la N-SAP
- La entità di livello N, riceve la SDU, aggiunge la N-PCI, cioè le informazioni di controllo al livello N (Protocol Control Information), e crea la PDU di livello N (N-PDU).



Incapsulamento e Segmentazione

- L'incapsulamento viene eseguito in modo ricorsivo
- Segmentazione: è la procedura inversa all'incapsulamento e consiste di suddividere i dati di una PDU in più SDU.



Modello ISO/OSI e Protocolli reali

- Il modello ISO/OSI è un MODELLO DI RIFERIMENTO, cioè specifica il compito dei vari strati, ma non come ogni strato è fatto in dettaglio.
- Reti di calcolatori: con la diffusione di INTERNET si è diffuso in modo prepotente il protocollo TCP/IP (che ha soppiantato lo strato 3 e 4 del modello ISO OSI: abbiamo
  - un protocollo per lo strato di trasporto (TCP),
  - un protocollo per lo strato di rete (IP)
  - del modello OSI rimane in piedi lo strato fisico e di linea.
  - Gli strati superiori sono praticamente spariti e rimane solo solo strato di applicazione
- Il TCP/IP ha in pratica soppiantato molti altri protocolli definiti sulla base del modello ISO-OSI.
- I sistemi RFID tipicamente prevedono solo:
  - strati fisico (1), di linea (2), di applicazione (7).
- I sistemi BUS gli prevedono gli strati fisico (1), di linea (2) , di rete (3), di trasporto (4), di applicazione (7).

Standard ISO 14443
"proximity coupling contactless smart cards"

- Smart Card a microprocessore
- Accoppiamento di Prossimità (<20 cm)
- Uso principale: biglietti elettronici
- Lo standard si compone di 4 parti
  - Parte 1: Caratteristiche Fisiche
  - Parte 2: Interfaccia RF (segnale e alimentazione)
  - Parte 3: Inizializzazione e Protocollo anticollisione
  - Parte 4: Protocollo di trasmissione
- Parte 1: caratteristiche fisiche:
  - carte in accordo allo standard ISO 7810 (carte di credito): 85.72mm × 54.03mm × 0.76mm.
  - note su resistenza alla torsione, piegamento, raggi UV, X, etc.

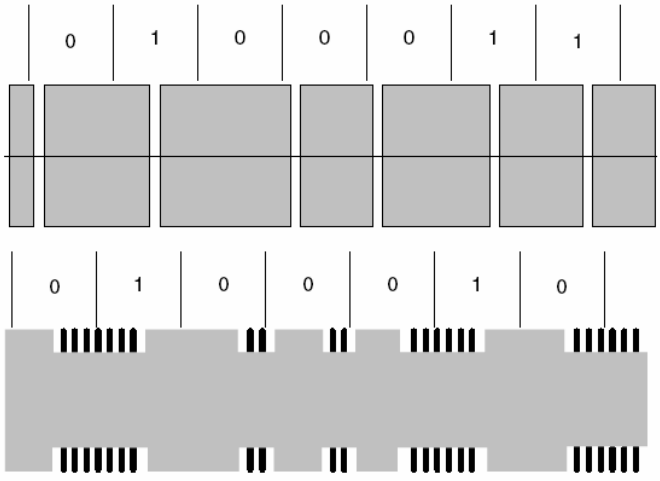
ISO 14443-2: interfaccia RF

- Alimentazione tramite campo magnetico alternato a 13.56 MHz
- Avvolgimento di accoppiamento con 3-6 spire perimetrali
- Campo minimo per il funzionamento del transponder: Hmin = 1.5 A/m
- Campo generato dal lettore: 1.5 A/m ≤ H ≤ 7.5 A/m
- In fase di definizione dello standard non si è riusciti a trovare un accordo su un'unica interfaccia di comunicazione: sono presenti un Tipo A e un Tipo B, significativamente diversi:
  - Una carta conforme allo standard ("compliant") deve supportare un solo tipo di interfaccia
  - Un lettore conforme allo standard deve supportare sia il tipo A sia il tipo B: nel funzionamento normale deve periodicamente commutare tra i due tipi di interfaccia di comunicazione.

ISO 14443-2 – Interfaccia di comunicazione

Tipo A

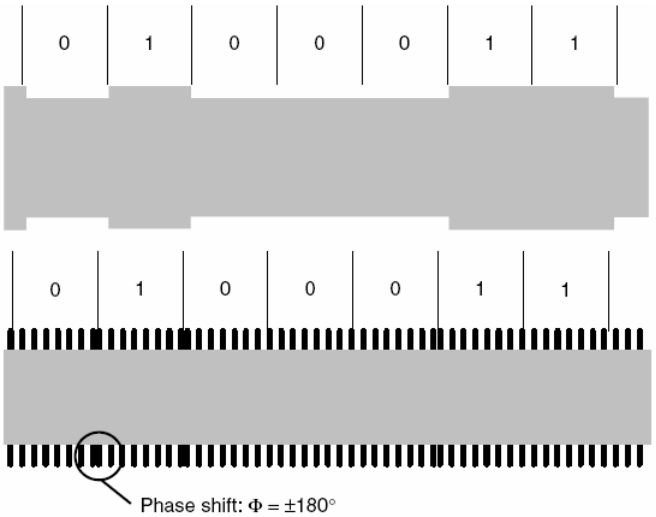
- Downlink: 100% ASK – codifica di Miller modificata
  - gli intervalli di tempo a potenza zero sono lunghi non piu' di 2-3 μs
  - lo standard pone tutti i vincoli sui tempi di salita/discesa
- Uplink: modulazione del carico con sottoportante
  - frequenza sottoportante: f_{sc} = 847 KHz (13.56 MHz/16)
  - modulazione sottoportante: On-Off Keying con codifica Manchester



- Baud rate sia in Uplink sia in Downlink: 106 Kbit/s (13.56 MHz/128).
- Ogni trama ha uno Start_of_Frame e un End_of_Frame

ISO 14443-2 – Interfaccia di comunicazione
Tipo B

- Downlink: 10% ASK – codifica NRZ
  - lo standard definisce tutti i transitori, da cui si ottengono informazioni sulle prestazioni e la banda dell'antenna.
- Uplink: modulazione del carico con sottoportante
  - frequenza sottoportante: f_{sc} = 847 KHz (13.56 MHz/16)
  - modulazione sottoportante: BPSK a 180° con codifica NRZ



- Baud rate sia in Uplink sia in Downlink: 106 Kbit/s (13.56 MHz/128).
- Ogni byte ha un bit di start e un bit di stop

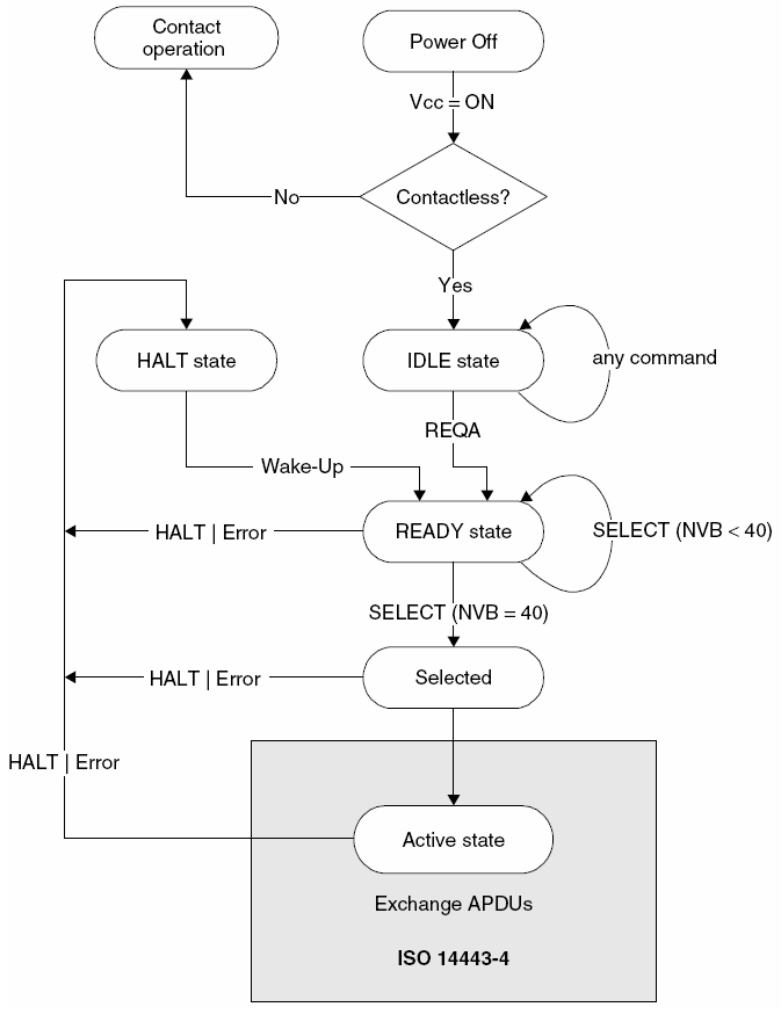
ISO 14443-3 Inizializzazione e Anticollisione
Tipo A (I)

- Appena la carta si trova nella regione di interrogazione di un lettore ed è alimentata il microproc. parte
- Se la carta è "dual interface" verifica se il modo di funzionamento è a contatto o RF
- La carta va nello stato IDLE e lì rimane finche non riceve un comando REQA (Request A) (7 bit di dati), a cui risponde con ATQA (Answer to Request A) (2 byte – trama standard)
- La carta va nello stato READY
- Il lettore capisce che c'è almeno una carta nella regione di interrogazione e comincia la procedura anticollisione, che è una RICERCA AD ALBERO BINARIA DINAMICA
- Il lettore invia comandi SELECT con argomento NVB (number of valid bits, lunghezza del criterio di ricerca)

ISO 14443-3 Inizializzazione e Anticollisione Tipo A (II)

- Il numero seriale della carta è di 4 byte
- Appena il lettore ha rilevato un numero completo invia il comando **SELECT** con argomento NVB=40h e il numero seriale, per selezionare la carta
- La carta selezionata conferma con il comando **SAK** (Select Acknowledge) e va nello stato **ACTIVE** in cui comunica in modo esclusivo con il lettore.
- Lo standard permette anche numeri seriali di 7 o 10 byte. Per esempio nel caso di 7 byte, nell'inviare SAK la carta mette a 1 il bit "cascade" e rimane nello stato READY. Il lettore continua la procedura anticollisione per determinare gli altri bit.

Giuseppe Iannaccone - 2005

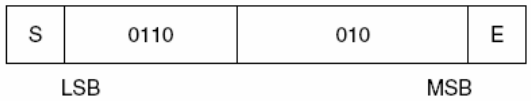


ISO 14443-3 Inizializzazione e Anticollisione Tipo A

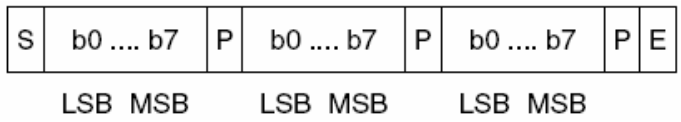
- 2005

ISO 14443-3 Inizializzazione e Anticollisione
Tipo A (III)

- Struttura della trama ("frame"):
- Comando REQA:



- ALtri comandi:

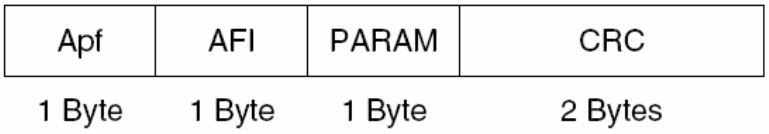


  - S: Start of frame
  - E: End of frame
  - P: Parity bit

- La Sincronizzazione deve essere a livello di singolo bit. La risposta ai comandi deve avvenire dopo un tempo prestabilito:
- Ultimo bit ricevuto '1': $(128\ N + 64)t_{bit}$ - '0': $(128\ N + 20)t_{bit}$
- Comandi REQA, WAKEUP, SELECT: N=9
- Altri comandi: N > 10

ISO 14443-3 Inizializzazione e Anticollisione
Tipo B (I)

- Appena la carta si trova nella regione di interrogazione di un lettore ed è alimentata il microproc. parte
- Se la carta è "dual interface" verifica se il modo di funzionamento è a contatto o RF
- La carta va nello stato IDLE e lì rimane finche non riceve un comando REQB (Request B)
- Il comando REQB ha un parametro AFI (Application Family Identifier) che specifica il tipo di applicazione, e un parametro N (dentro PARAM) che specifica il numero di slot disponibili per la risposta (1,2,4,8,16) (Protocollo Aloha Slotted)



ISO 14443-3 Inizializzazione e Anticollisione
Tipo B (II)

- La carta controlla che l'AFI ricevuto nel REQB corrisponda al proprio. Se sì e se N>1 estrae a caso un numero M tra 1 e N
- Per garantire la sincronizzazione, il lettore trasmette all'inizio di ogni slot un SLOT_MARKER (se il lettore capisce che uno slot rimane inutilizzato, puo' subito inviare lo SLOT_MARKER successivo)

APn	CRC
1 Byte	2 Bytes

- La carta allo slot M trasmette il comando ATQB, che contiene:
  - il numero seriale o un numero random di 4 byte che fa da numero seriale per la sessione (PUPI)
  - Prof. Info: baudrate, lunghezza delle trame, etc,
  - Application data: informazioni sulle applicazioni della carta

Apa	PUPI (Identifier)	Application Data	Prot. Info	CRC
1 Byte	4 Bytes	4 Bytes	2 Bytes	2 Bytes

ISO 14443-3 Inizializzazione e Anticollisione
Tipo B (III)

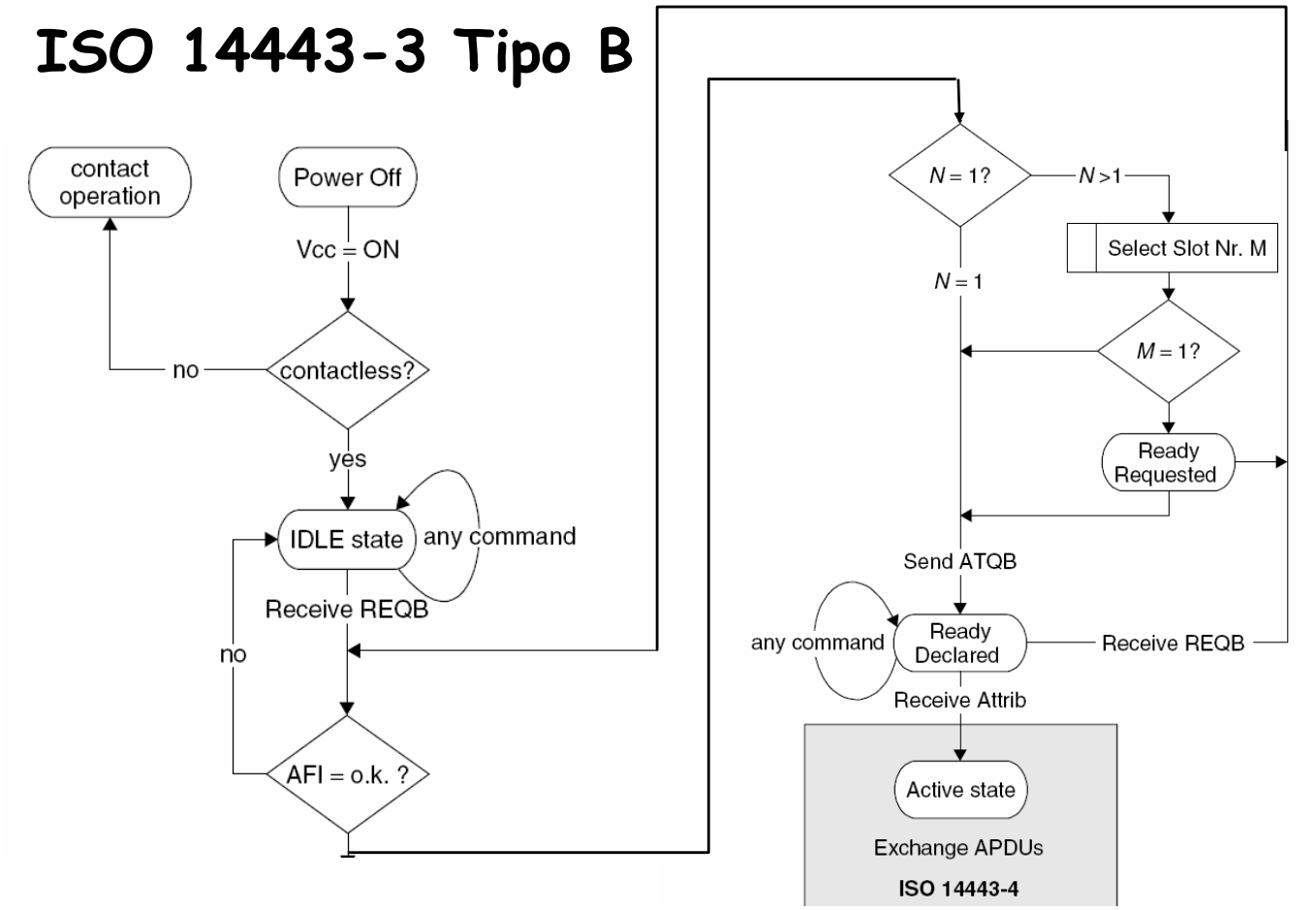
- Appena il lettore riceve un ATQB senza collisioni puo' selezionare la carta, inviando il comando ATTRIB, che contiene l'identificativo della carta, altri parametri della comunicazione (param) e il primo comando della applicazione

ATTRIB-Prefix			Suffix: 1st applicative command		
Apc	PUPI (Identifier)	Param	NAD	Application Data	CRC
1 Byte	4 Bytes	1 Byte	1 Byte	*N* Bytes	2 Bytes

- Struttura della trama degli altri comandi di applicazione (sia downlink sia uplink)

NAD	Data	CRC
1 Byte	*N* Bytes	2 Bytes

ISO 14443-3 Tipo B



ISO 14443-4 Protocolli di trasmissione (I)

- Per le carte di tipo A è necessario che dopo il protocollo anticollisione siano trasferite alcune informazioni dalla carta al lettore (nelle carte di tipo B queste informazioni sono passate con il comando ATQB)
- Inizializzazione del protocollo (Tipo A)
  - Nel comando SAK, la carta specifica se il protocollo è conforme allo standard ISO 14443-4.
  - Se sì, il lettore invia il comando **RATS** (Request Answer to Select) con due parametri:
    - **FSDI** (Frame Size Device Integer): max numero di byte che la carta puo' inviare in un unico blocco
    - **CID** (Card IDentifier): ha validità per la sessione

ISO 14443-4 Protocolli di trasmissione (II)

- La carta risponde con il comando **ATS** (Answer To Select) che ha numerosi argomenti importanti per la definizione del protocollo: FDSI, DS (Datarate Send), DR (Datarate Receive), ...
- Il lettore invia il comando PPS (Protocol Parameter Selection), in cui specifica il baud rate per uplink e downlink.

ISO 14443-4 Protocolli di trasmissione (III)

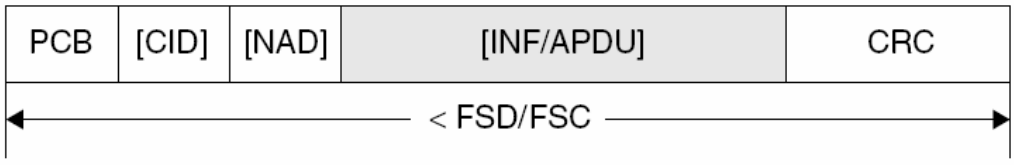
- Il protocollo supporta la trasmissione di APDU (Application Protocol Data Units) tra carta e lettore.
  - APDU possono essere dati, comandi, risposte
- E' fortemente basato sul protocollo ISO 7816-3 (smart card a contatto) per semplificare l'uso di carte "dual interface".
- La trasmissione dati nel protocollo ISO 14443 si puo' descrivere nel quadro del modello a strati OSI
  - ISO 14443 Parti 1,2 → Livello fisico
  - ISO 14443 Parti 3,4 → Livello di collegamento
    - Controlla i dati tra lettore e carta, correttezza dei dati indirizzati, gestione degli errori di trasmissione, lunghezza dei blocchi di dati.
  - I livelli da 3 a 6 del modello OSI non sono usati nelle smart card
- Il livello 7 gestisce i dati delle applicazioni, ed è comune alle carte a contatto: e.g. ISO 7816-(4-7)

ISO 14443-4 Protocolli di trasmissione (III)

- La comunicazione lettore-carta segue la struttura master-slave:
  - La carta si pone in attesa di un comando dal lettore
  - Il lettore invia un comando alla carta, che esegue e risponde
- Al livello 14443-4 l'infomazione viene trasmessa da data block, che possono essere di tipo
  - I (information): dati delle APDU
  - R (recovery): gestione degli errori di trasmissione
  - S (supervisory): controllo superiore del protocollo

ISO 14443-4 Protocolli di trasmissione (III)

- Struttura



- PCB Protocol Control Byte (tra le altre cose specifica il tipo di data block)
- CID Card IDentifier (opzionale):
- NAD (introduce compatibilità con ISO 7816-4
- INF (sono le APDU se non ci sono errori),

Infrastruttura di "contactless ticketing" per trasporti pubblici

- Consente l'accesso a bus, treni, tram, parcheggi
- Contactless ticketing (dagli anni '90)
  - un biglietto contactless puo' rimpiazzare biglietti di carta o con banda magnetica in diversi modi:
    - "event ticket": convalidato una volta sola e consente l'accesso a un certo numero di tratte interconnesse.
    - carta ricaricabile (eventualmente contenente informazioni personali importanti per la tariffa).
    - carta multi-applicazioni (+ fidelizzazione, controllo accesso a parcheggio, altri acquisti).
- Vantaggio per il viaggiatore: biglietto flessibile, unico,facile da usare e con funzionalità aggiuntive
- Vantaggio per la società di trasporto: costi di manutenzione ridotti, protezione da frodi, monitoraggio + semplice

Vantaggi di un infrastruttura di "Contactless ticketing" (I)

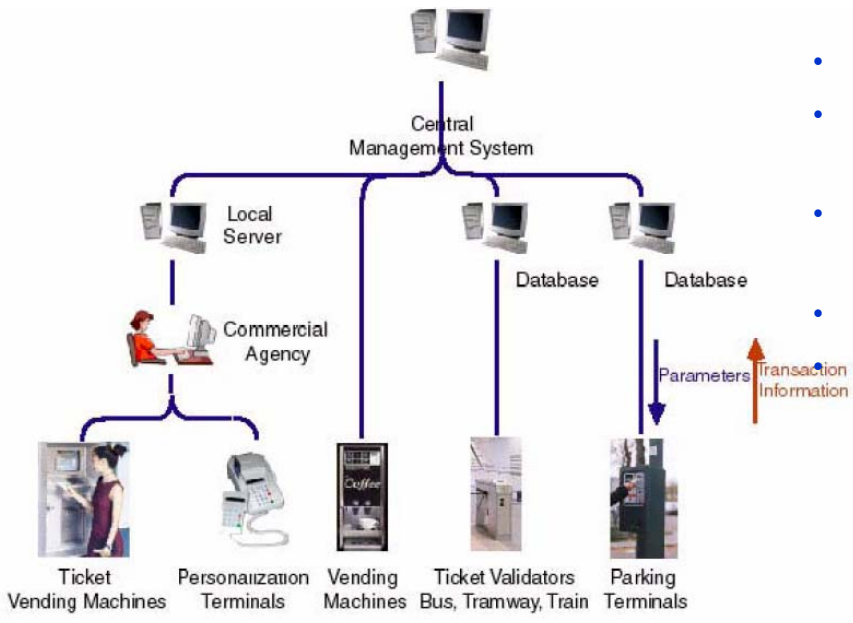
1. Alta velocità delle transazioni (tip. 150 ms)
   - Più adatta ad alti volumi di traffico della tecnologia a contatto o banda magnetica
2. Ridotti costi di manutenzione
   - 10 volte più affidabile di un sistema basato su carte magnetiche.
   - In media un lettore magnetico deve andare in manutenzione ogni 20 K carte. Una stazione metro trafficata ha tipicamente più di 2000 passeggeri al giorno per cancelletto → Una richiesta di manutenzione ogni 10 giorni. Rapporto dei costi di manutenzione sui costi di esercizio: 12-15% for sistemi "magnetici", 8% per sistemi "contactless"

Fonte: Axalto

Vantaggi di un infrastruttura di "Contactless ticketing" (II)

3. Frode
   - L'alta velocità di transazione permette un passaggio stretto (uno alla volta).
   - Più difficili da duplicare delle strisce magnetiche
4. Maggiore flessibilità nella struttura dei prezzi
   - Permette di applicare tariffe diverse a seconda dell'ora del giorno e a seconda delle stazioni di partenza e arrivo con la stessa carta
5. Espandibile a nuovi servizi:
   - per esempio: si possono aggiungere schemi di fidelizzazione, o altre combinazioni di servizio (borsellino elettronico, carta sconti, raccolte punti)

Infrastruttura di "contactless ticketing" per trasporti pubblici



Source: STM TA262

- biglietti/carte "contactless"
- vending machines
- terminali di personalizzazione
- validatori dei biglietti (bus, tram, treni)
- terminali di parcheggio
- sistema di gestione centrale (online/offline):
  - controllo dell'accesso al sistema
  - gestione account individuali
  - statistiche

Requisiti generali del sistema

- Sicurezza da duplicazione o riprogrammazione non autorizzata
- Robustezza per ridurre i costi di manutenzione
- Investimento iniziale adattabile al volume di vendita
- Transazioni veloci per facilitare l'accesso e attirare clienti
- Riduzione dei costi e servizi migliori
- Interoperabilità

Requisiti della tecnologia contactless:

- Piccola portata
  - 0-10 cm per le carte
  - 0-20 cm per i biglietti
- Compatibilità con ISO14443 tipo B
- Offerta variabile tra biglietti/lettori a basso costo a carte di fascia alta
- Offerta di caratteristiche di sicurezza adeguate all'applicazione (one-time write, crittografia, sistemi anticontraffazione).

Standard Calypso

- Associazione di imprese nel settore del trasporto urbano (iniz. francesi) per definire uno standard di "teleticketing"
- Tecnologia Aperta = Specifiche pubbliche
- Carte a microprocessore compatibili con
  - ISO 14443 B per l'interfaccia contactless
  - ISO 7816-4 per l'organizzazione memoria e la struttura file
  - CEN ENV 1545 per la definizione dei dati del trasporto
- Interoperabilità: ciascun lettore puo' gestire carte di altre reti Calypso
- multiapplicazione: a seconda del bisogno la carta puo' gestire borsellino elettronico, accesso a musei, congressi, eventi sportivi, parcheggio
- 40 citta: Parigi, Lisbona, Venezia, Capri, ...
- Crittografia: DES (64 bit), XDES (128 bit), tripleDES (64bit)
- www.calypsonet-asso.org

Standard Calypso

	Layer	International Standard	Calypso Status
7	Security Management and Architecture		Calypso Security Architecture
6	Terminal Applicative Software		Calypso API
5	Data Model		Calypso Data Model
4	Card and SAM Security Mechanisms		Calypso card application
3	Card Data structure	CEN ENV 1545	
2	Card OS and Files structure & Commands	ISO 7816-4	
1	Contact and Contactless Communication Interface	ISO 7816 1-3 ISO 14443 B 1-4	

Soluzioni STM x standard Calypso (I)

- **Biglietti: ISO 14443 B - f=13.56 MHz – data rate 106 Kb/s**
  - **fascia bassa (low end) – CTS256**
    - **"event" ticket e biglietti giornalieri.**
    - **32 bit UID**
    - **256 bit EEPROM (codice attività, ID emittente, scadenza, prezzo pagato, regione di validità)**
    - **sicurezza:**
      - **possibilità di "write-lock" di una zona di memoria**
      - **possibilità di autenticazione in linea mandando alla sistema di gestione centrale un *certificato passivo***
  - **"secure SRIX contactless memories" - SRIX512 e SRIX4K**
    - **+ memoria → biglietti multigiornalieri + carte ricaricabili**
    - **controllato in linea *dal* sistema di gestione centrale attraverso protocollo di challenge-response**

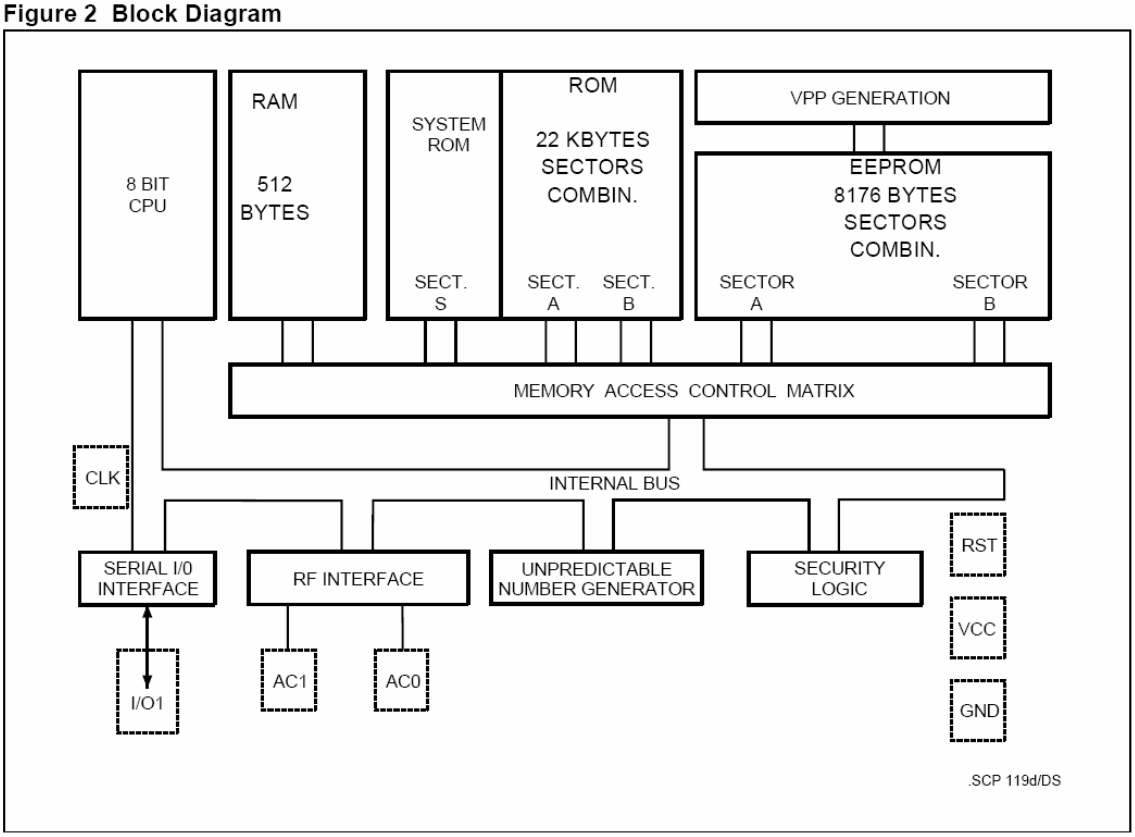
Soluzioni STM x standard Calypso (II)

Dual Interface Smart Cards:

- Per carte multifunzionali o biglietti stagionali
- Interfacce:
  - contactless ISO 14443B (e-ticketing)
  - contact interface (parking, borsellino elettronica (e-purse), fidelizzazione (loyalty cards))
- ST16R820, ST16RF52 e ST16RF58 (piattaforma ST16)
  - fino a 22KByte ROM, 8KByte EEPROM, 512 Byte RAM.
- ST19RF08 (piattaforma ST19)
  - ha in più un processore crittografico (DES) e 32KByte di ROM per il codice dell'applicazione

ST16RF58

Figure 2 Block Diagram



Axalto Cards (www.axalto.com)

- **Carte a MicroProcessore:**
  - cryptoflex 32K: +100: 16$ (+2000: 12$)
    - ISO 7816, Coprocessore crittografico DES
  - micropayflex S 4K: +100: 4.19$ (+2000: 3.19$)
    - transazioni sicure, EEPROM 450 byte
- **Lettori:**
  - Reflex 20 v. 2 (PCMCIA): 60$ (+2000 30$)

ASK C.ticket: disposable paper tickets

	CTS256B	CTS512B	CTS512A	CTM512B	CTM8KA
RF Interface	ISO14443B	ISO 14443 B	ISO 14443 A	ISO 14443 B	ISO 14443 A
EEPROM	256 bits	512 bits	512 bits	512 bits	1024 bytes
OTP area	12 bits	128 bits	32 bits	Variable	Variable
Unique S/N	64 bits	64 bits	56 bits	64 bits	32 bits
Memory Write protection	Yes per sector	Yes per sector	Yes per pg or block	Yes per sector	Yes per sector
Authentication	Simple static	Simple static	Simple static	Simple dyn.	Mutual dynamic
Key length	-	-	-	80 bits	48 bits
SAM	Optional	Optional	Optional	YES/Optional	MFRC500
Anticollision	No	Yes	Yes	Yes	Yes
Trans. time	100 ms	< 150ms	< 150ms	< 200 ms	< 300ms
distance	10 cm	10 cm	10 cm	10 cm	10 cm
Other features				One way counter	Random generator

www.ask.fr

C.ticket application: CAPRI

- Progetto Unico Capri,
- Operatori di trasporto: SIPPIC Funicolare di Capri - SIPPIC Trasporti - STAIANO Autotrasporti
- Integratore di Sistema: ASCOM MONETEL
- Cifre significative:
  - 2.5 milioni di carte ASK C.ticket® fornite nel 2002
  - 8500 smart card GTML fornite nel 2002
  - 2 funicolari and 33 bus:
    - 169.758 treni x Km / anno,
    - 1.004.082 bus x Km / anno
  - Popolazione di Capri: 13100
  - Visitatori in estate: 1.3 milioni
  - 7.6 milioni viaggiatori/anno
  - 0.1 s/passeggero per la validazione
- Progetto Unico Campania

Standard ISO 18000
(Rilasciato nel 2004)

- Parte 1: Architettura di Riferimento
- Parte 2: f < 135 KHz
- Parte 3: f = 13.56 MHz
- Parte 4: f = 2.45 GHz
- Parte 5: f = 5.8 GHz
- Parte 6: UHF Frequency band 860-960 MHz
- Parte 7: f = 433 MHz

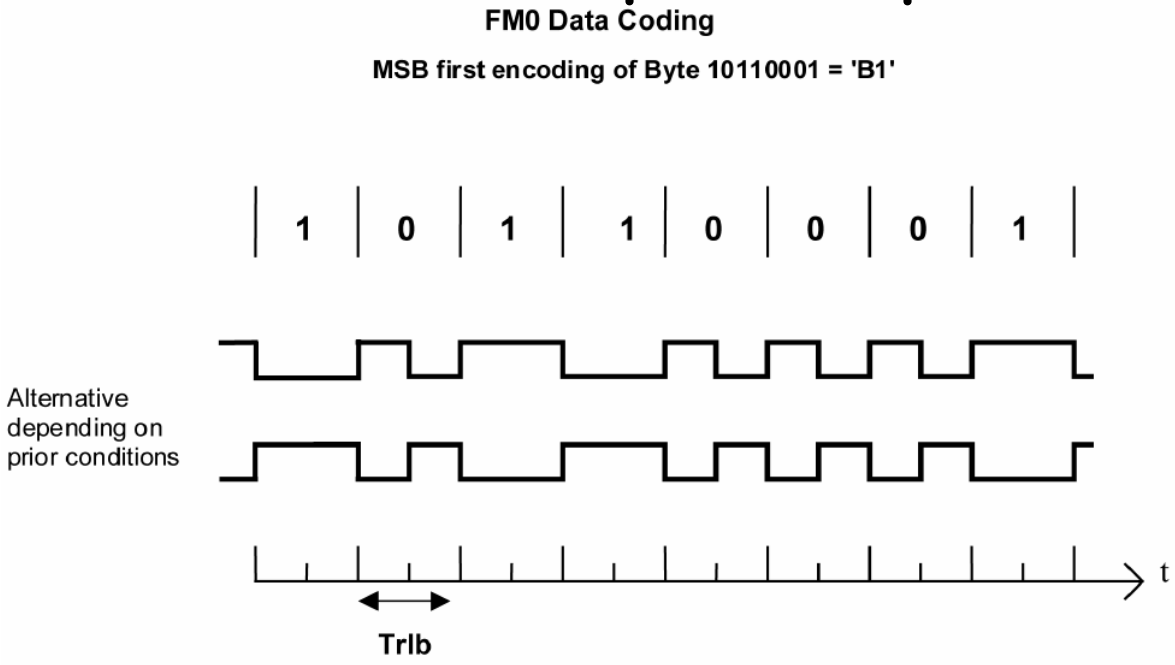
- Parte 6:

  Definisce un sistema con tag a radiazione retrodiffusa nella banda 860-960 MHz con:
  - Protocolli anticollisione
  - Selezione di un sottogruppo di tag
  - Lettura/scrittura su tag
  - Possibilità di proteggere il tag in scrittura (write lock)
  - Rivelazione d'errore uplink/downlink
  - Protezione per l'integrità dei dati
  - Supporto per tag passivi e semi-passivi.

ISO 18000 – Tipo A e Tipo B

Parametro	Tipo A	Tipo B
Downlink	Modulazione ASK Pulse Interval Encoding	Modulazione ASK Manchester
Indice di Modulazione	30%-100%	18%-100%
Data rate	33 kbit/s	10-40 kbit/s
Uplink	FM0	FM0
Prot. Anticollisione	ALOHA Slotted	Albero Binario
Identificatore	64 bit (40 Sub UID)	64 bit
Ind. Memoria	Blocchi fino 256 bit	Blocchi 1-4 byte
Riv. Errore donwlink	CRC 5 bit (16xlunghi)	CRC 16 bit
Riv. Errore uplink	CRC 16 bit	CRC 16 bit
Linearità Anticollisione	Fino a 250	2^256

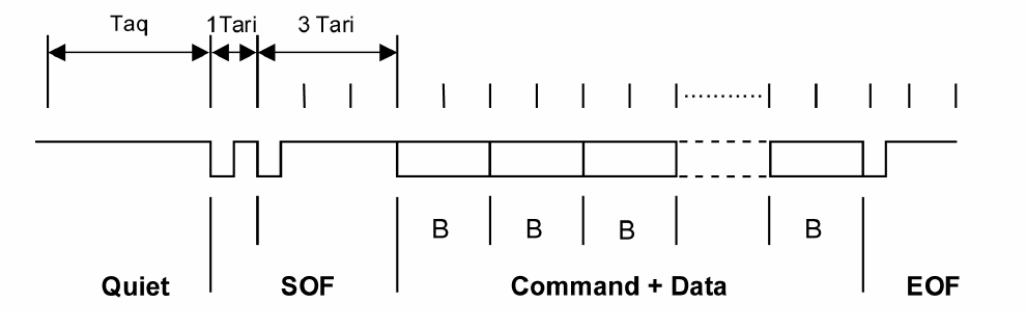
ISO 18000
A comune tra Tipo A e Tipo B



- CRC 5 bit - Polinomio Generatore x^5+x^3+1
- CRC 16 bit - Polinomio Generatore $x^{16}+x^{12}+x^5+1$

ISO 18000 – Tipo A

- Downlink Frame Format: SOF Start of Frame --- EOF End of Frame --- RFU (per usi futuri) -- SUID



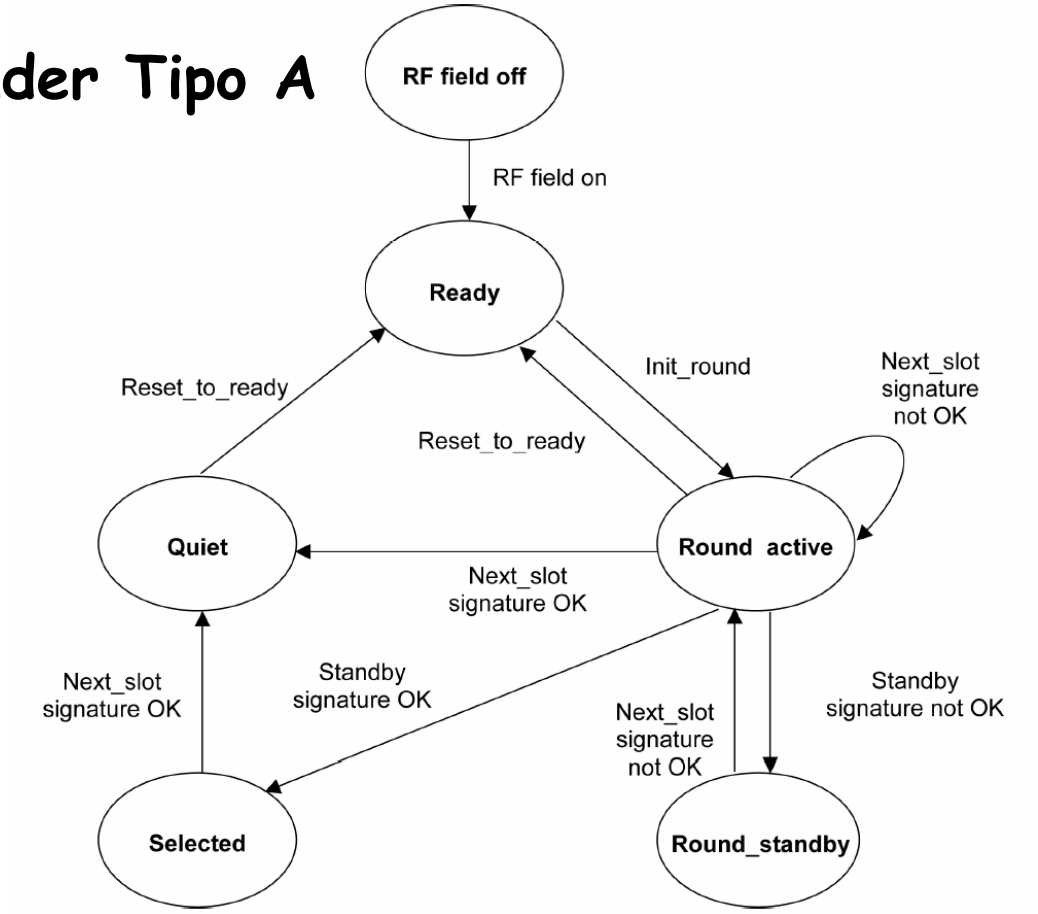
SOF	RFU	Command code	Parameters/Flags	CRC-5	EOF
	1 bit	6 bits	4 bits	5 bits	

SOF	RFU	Command code	Parameters or flags	CRC-5	SUID (optional)	Data	Data (optional)	CRC-16	EOF
	1 bit	6 bits	4 bits	5 bits	40 bits	8 bits	8 to n	16 bits	

ISO 18000 Tipo A - Transponder

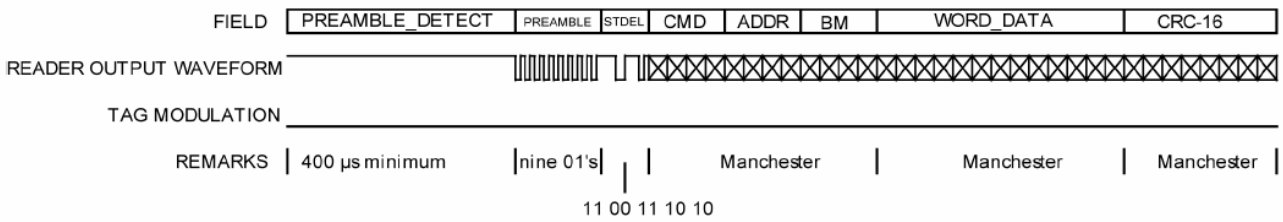
- Memoria: 256 blocchi di 256 bit.
- Per ogni blocco:1 bit user lock e 1 bit factory lock
- Stati del Transponder:
  - RF Field Off: tag passivi OFF, tag attivi Stand by
  - Ready: Il tag processa solo i comandi non indirizzati a un tag particolare
  - Quiet: Il tag processa i comandi in cui SUID corrisponde a quello del tag
  - Selected: Il tag processa i comandi in cui il SUID non è presente
  - Round_active: il tag partecipa al protocollo anticollisione
  - Round_standby: il tag NON partecipa al protocollo anticollisione

Transponder Tipo A



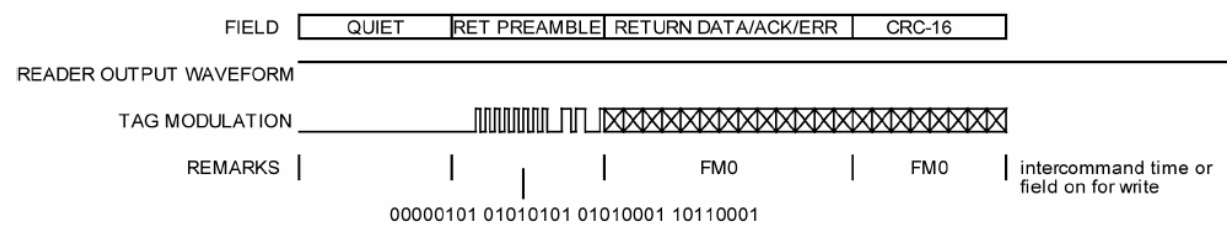
ISO 18000 Tipo B

- Anche in questo caso "Interrogator Talks First":
  - Il lettore invia un comando
  - Il trasponder invia una risposta
- Formato di un Comando = 1 frame
  - Preamble Detect: 400 us di portante non modulata
  - Preamble: 9 bit di zeri in codifica Manchester = 0101010101010101
  - Delimiter (4 tipi): tipo 1 in formato NRZ: 1100111010 (codifica non Manchester)
  - CRC 16



ISO 18000 Tipo B

- **Formato di una risposta:**
  - Quiet: 16/(Uplink data rate) - 0.75/(Downlink data rate)
  - Return Preamble (non Manchester)
  - CRC 16



ISO 18000 Tipo B – Macchina a Stati Tag

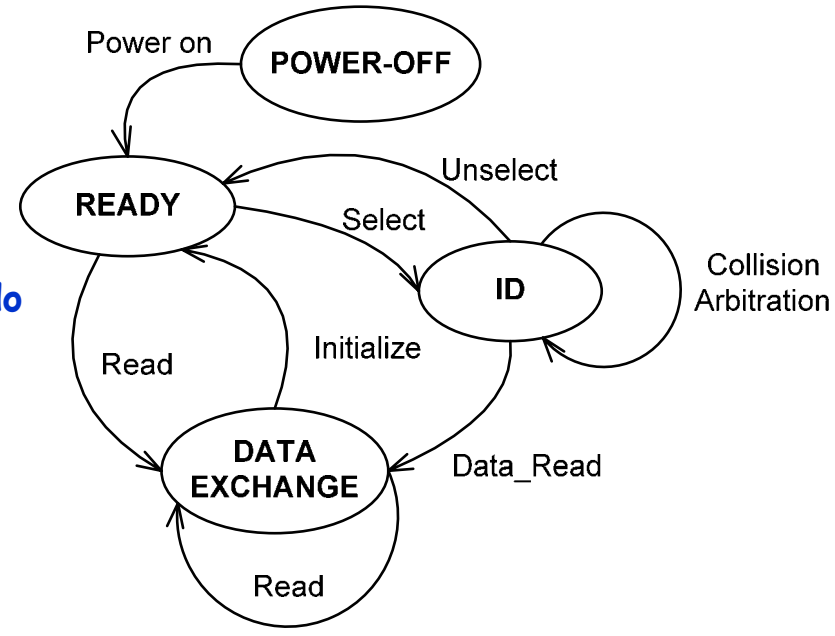
Stati:

POWER OFF
(non alimentato)

READY:
aspetta un comando Select o Read

ID:
Gestione delle collisione

DATA EXCHANGE:
transponder selezionato



Tipo B – Procedura Anticollisione (I)

- Il tag deve avere a bordo
  - generatore random di 1 bit
  - contatore a a 8 bit (COUNT)

1. Quando i tag ricevono un comando di GROUP_SELECT passano nello stato ID e resettano il contatore (COUNT := 0)
2. Se arriva un comando SELECT tutti i tag con COUNT = 0 rispondono
3. Il Lettore puo':
   - Rivelare una collisione
   - Ricevere la risposta di un unico tag
   - Non ricevere nessuna risposta

Tipo B – Procedura Anticollisione (II)

Se il lettore rivela una collisione,

4 invia il comando FAIL

- Quando un tag nello stato ID riceve il comando FAIL:
  - Se COUNT > 0 → COUNT = COUNT + 1
  - Se COUNT = 0 → Estrae un bit random R → COUNT = COUNT+R
- Si torna al punto 2

Se il lettore non riceve niente,

5 invia il comando SUCCESS

- Tutti i tag decrementano il COUNT=COUNT–1 → goto 2

Se il lettore riceve solo la risposta di un tag si va al punto 6

6. Il Lettore Trasmette READ_DATA con argomento l'ID del tag
7. Il tag si sposta nello stato DATA_EXCHANGE e comincia a comunicare con il transponder
8. Il lettore invia il comando SUCCESS e torna al punto 2