



Via Cairoli, 30 57123 Livorno (Italy)
Tel. +39 0586 211646 - Fax +39 0586 21177
memex@memexitaly.it www.memexitaly.it

Requisiti aziendali per la sicurezza delle transazioni in un Sistema di Bigliettazione Elettronica

- ❑ *MemEx* fornisce consulenza sistemistica, capacità di management e servizi tecnici nei settori della Bigliettazione Automatica e dell'Integrazione Tariffaria, del Telecontrollo ed Informazione all'Utenza, dei Servizi Flessibili di Trasporto, dei Servizi Urbani di Mobilità e Controllo del Traffico, della Logistica Urbana.
- ❑ *MemEx* fornisce supporto ed esperienza di management in tutte le fasi del ciclo di vita di un sistema tecnologico: dalla ricerca ed individuazione degli eventuali canali di finanziamento a livello Nazionale ed Europeo, all'analisi dei requisiti e studio di fattibilità, dall'acquisizione, al supporto nella realizzazione/avvio/gestione operativa dei sistemi, al collaudo ed alla stesura del contratto di manutenzione

- ❑ Analisi di sistema, identificazione dei requisiti utente, definizione e redazione delle specifiche tecniche e funzionali, elaborazione di studi di fattibilità
- ❑ Redazione documentazione di gara (capitolati ed allegati tecnici), definizione di metodologie di valutazione delle offerte, valutazione delle offerte
- ❑ Supporto alla fase di negoziazione e redazione documentazione contrattuale
- ❑ Direzione ai lavori, supporto all'introduzione ed alla messa in servizio delle tecnologie, monitoraggio della realizzazione, gestione degli impatti organizzativi ed operativi
- ❑ Definizione delle procedure di collaudo, effettuazione dell'attività di collaudo
- ❑ Redazione del contratto di manutenzione in garanzia e post-garanzia, formazione ed assistenza tecnica/operativa al personale

Enti di Ricerca

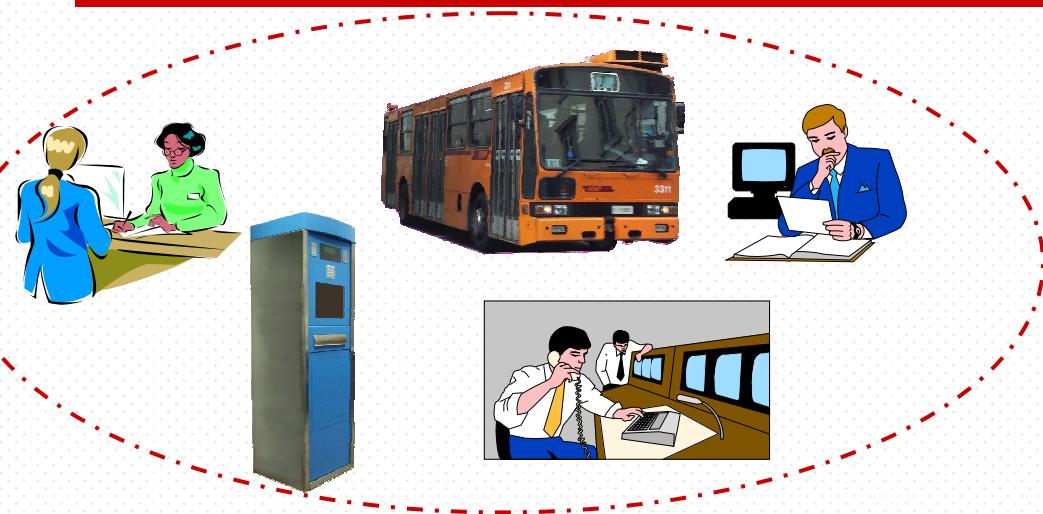
- CNR
- ENEA
- Facoltà Ingegneria Univ. Napoli
- Univ. Pol. de Catalunya (SP)
- Univ. Newcastle upon Thyne (EN)
- FZI Univ. Karlsruhe (DE)

Società di Consulenza

- TRITEL (BE)
- ETTS (IR)

- ATAF - Firenze
- SITA - Firenze
- ATL - Livorno
- ANM - Napoli
- CTP - Napoli
- CAT - Carrara
- ATC - Terni
- ATC - Spezia
- STA - Roma
- ATAC - Roma
- TRAMBUS - Roma
- CTM - Cagliari
- CNA Pisa
- CSST Napoli
- Regione Toscana
- Provincia di Firenze
- Provincia e Comune di Livorno
- Regione Emilia-Romagna
- Comune di Lucca
- Distretto Metropolitano Quito (EC)
- Comune di Cork (IR)
- ICS - Iniziativa Car Sharing
- Comune di Crema
- Provincia di Cremona
- Siena Parcheggi
- Pesaro Parcheggi

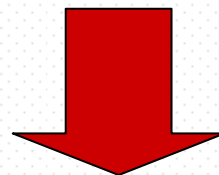
Il concetto di Sicurezza in un Sistema di Bigliettazione Elettronica



"Messa in sicurezza"

come concetto

da considerarsi in senso ampio



Insieme delle attività atte ad individuare e porre in atto le opportune misure di protezione di tipo:

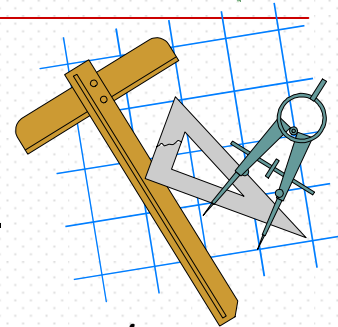
- ✓ *Tecnico*
- ✓ *Organizzativo*
- ✓ *Operativo*

necessarie per tutelare il Sistema nei seguenti ambiti:

- A. Sicurezza Informatica*
- B. Sicurezza di Funzionamento*
- C. Sicurezza Antinfortunistica/Normativa*

Una premessa necessaria

Nessun Sistema risulta totalmente sicuro ed esente da malfunzionamenti/blocchi di qualsiasi natura.

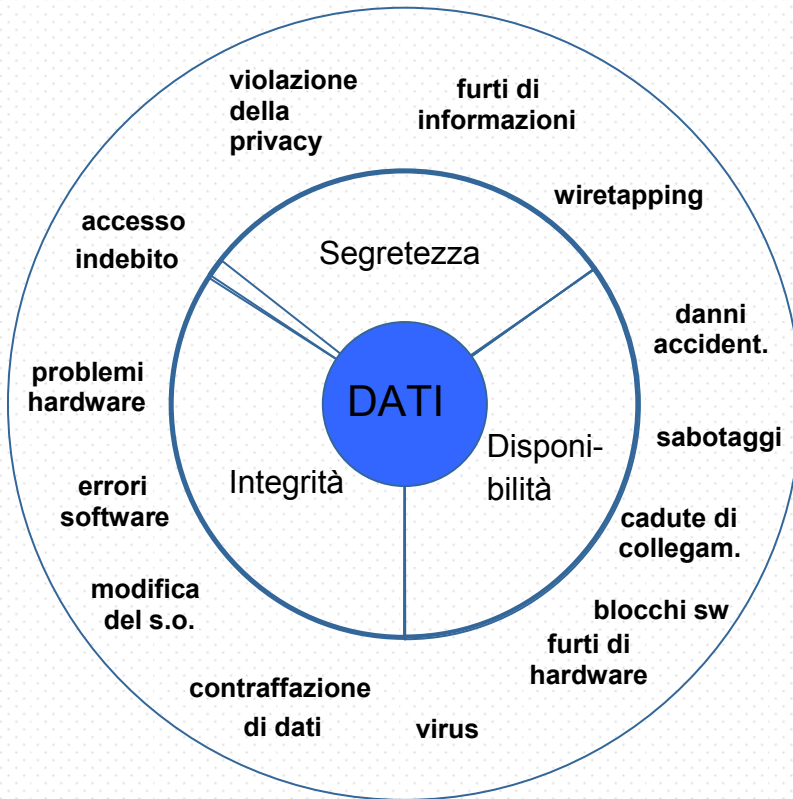


Per stabilire quali protezioni siano adeguate ai requisiti occorre valutare:

- ❖ il livello di sicurezza garantito dalla protezione (*rispetto al livello massimo*)
- ❖ le risorse ed i costi relativi all'attuazione (*rispetto al livello massimo*)
- ❖ la probabilità che abbia luogo l'evento anomalo (di "attacco" alla sicurezza) e la quantificazione degli impatti che ne derivano.

- ☞ Il Sistema deve essere sufficientemente robusto da **minimizzare gli impatti**
- ☞ La risposta del Sistema deve essere "**tempo-invariante**" per ogni singola tipologia di evento
- ☞ Devono essere **messe a disposizione** le procedure operative di ripristino





Requisiti garantiti dalle protezioni;

- ❖ **Segretezza** → *accessibilità alle risorse del Sistema solo alle figure autorizzate*
- ❖ **Integrità** → *controllo che eventuali modifiche siano effettuate solo da soggetti abilitati*
- ❖ **Disponibilità** → *completa accessibilità per le figure autorizzate o nell'uso delle risorse del Sistema.*

1. Garanzia contro il rischio di perdita dei dati memorizzati ai vari livelli architetturali
2. Garanzia contro la falsificazione ed uso improprio delle informazioni
3. Affidabilità dei flussi informativi tra i vari componenti del sistema (integrità, completezza, univocità dei dati trasmessi, etc.)
4. Tracciabilità delle operazioni effettuate e fruibilità delle informazioni associate a tali flussi



❖ *A livello di Centro:*

- ridondanza nella memorizzazione dei dati
- corretta gestione delle procedure di back-up
- attuazione di una procedura documentata per il ripristino dati in caso di "crash" del sistema



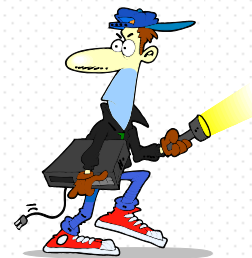
L'Azienda deve definire ed attuare le adeguate procedure operative come attività continuativa nel tempo oppure includerle nel contratto di manutenzione

❖ *A livello di bordo ed ai livelli intermedi:*

- memorizzazione dei dati trasmessi per un certo periodo di tempo (fino ad elaborazione dal Centro) come duplicazione dati di riserva

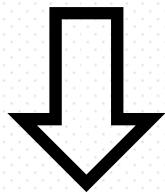
Frenare, rendere oneroso, al limite, rendere impossibile l'eventualità di effettuare frodi o procurare danno manipolando i dati e/o la configurazione del sistema

- ❖ Controllo accesso al sistema centrale
- ❖ Controllo accesso ad hw/sw locale periferico (stazioni di vendita, controllo legittimità nell'esecuzione delle funzioni, etc.)
- ❖ Sicurezza rete da accessi esterni
- ❖ Controllo contraffazione titoli
- ❖ Controllo manipolazione dati relativi ai titoli di viaggio



- ❖ Solamente le entità autorizzate devono poter emettere titoli di viaggio
- ❖ Deve essere estremamente difficoltoso (*e quindi non conveniente per il contraffattore*) creare titoli falsi
- ❖ Deve essere possibile riconoscere titoli falsi
- ❖ Il Sistema non deve basare la propria sicurezza sulla segretezza degli algoritmi utilizzati

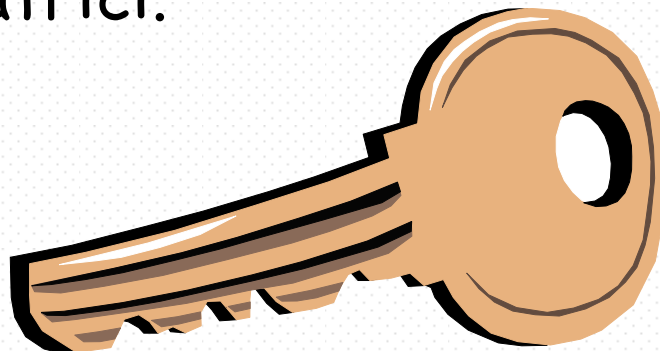
- ❖ Stato dell'arte attuale: **modulo SAM**



- ❖ Sviluppo futuro:
moneta elettronica
interoperabile (*EMV*,
chiave + Hw, etc.)

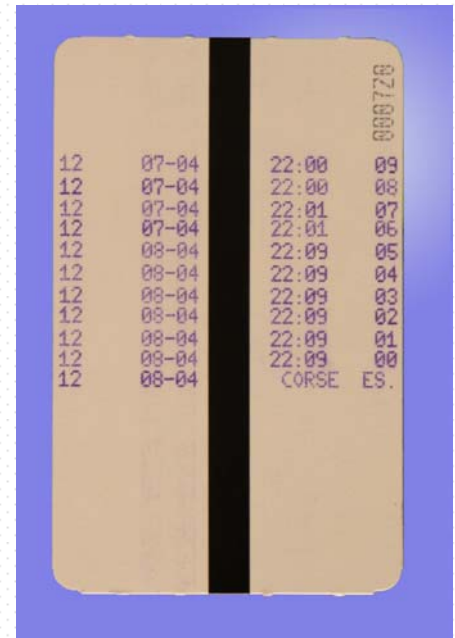


- ❖ Le **chiavi** devono essere possedute dall'Ente terzo garante della sicurezza e non dal Fornitore.
- ❖ E' opportuno che i **moduli SAM** siano acquistati direttamente da parte dell'Ente terzo a ciò proposto e che siano consegnate al Fornitore per l'installazione nelle validatrici.



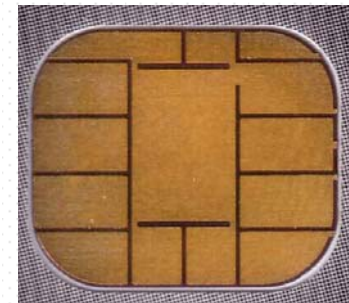
Titoli a banda magnetica

- ❖ *Minore* livello di sicurezza
- ❖ *Maggiore* diffusione



Smart-Card

- ❖ *Maggiore* livello di sicurezza
- ❖ *Minore* diffusione



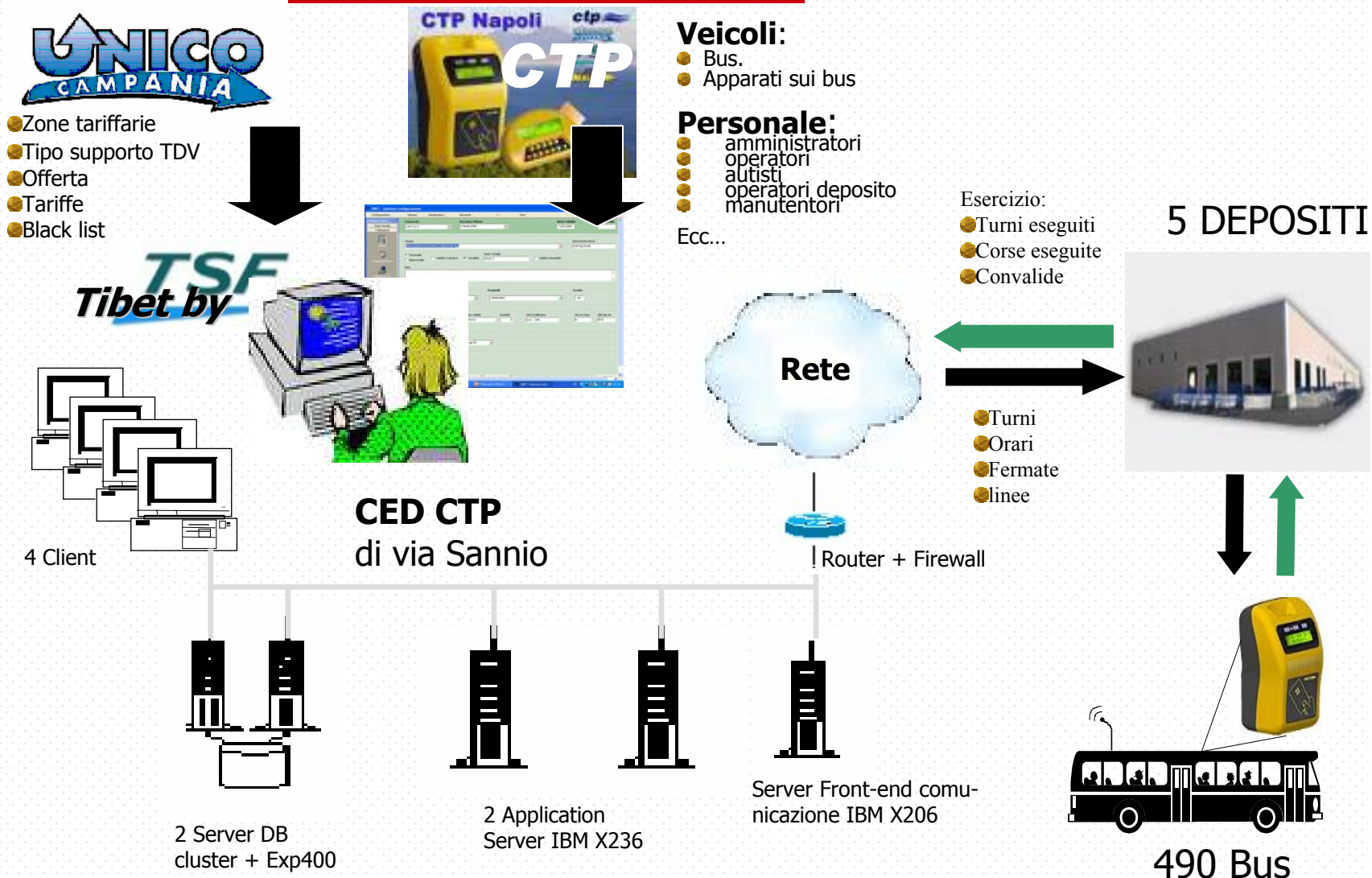
Attualmente si contano alcune esperienze di sperimentazione/realizzazione di carte integrate per il pagamento ("*Carte Trasporti*")

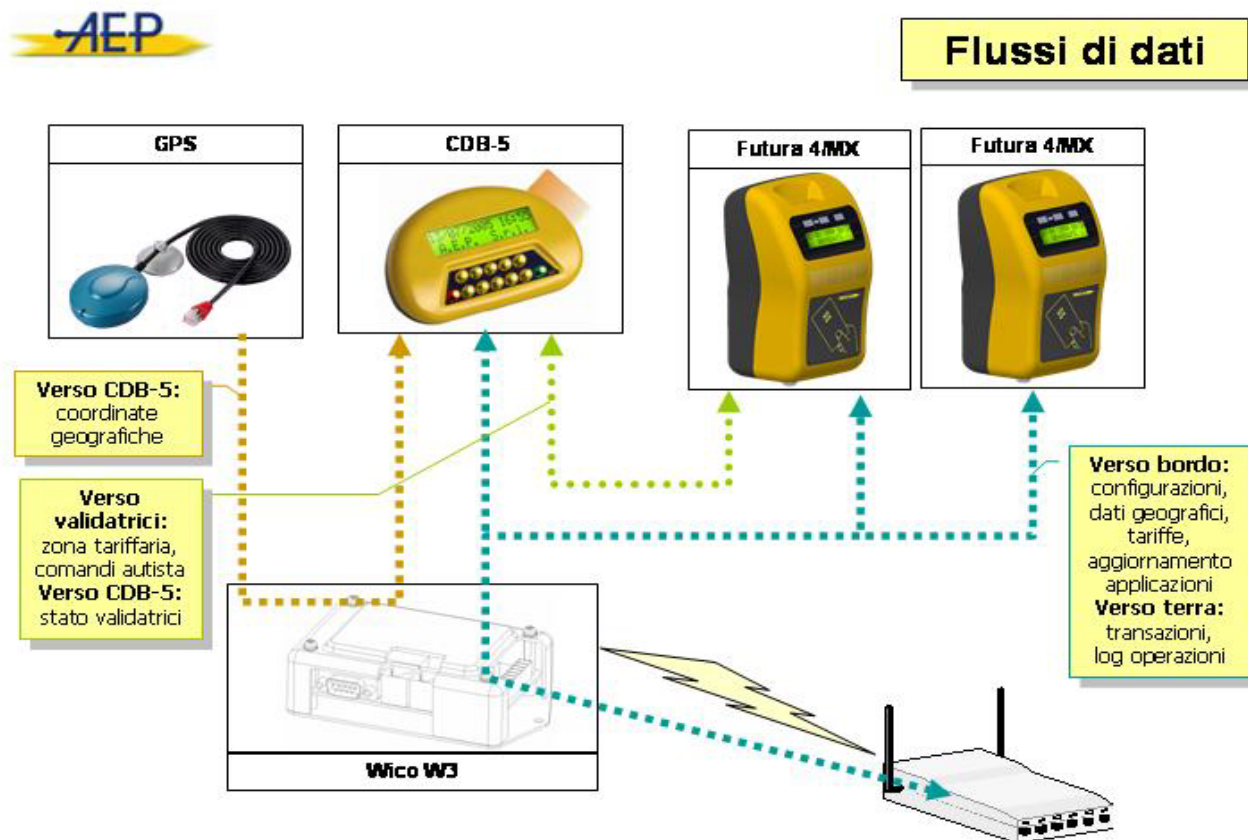
☞ *Le Aziende sono "sensibili" ai criteri di autorizzazione nella gestione dei dati sulla carta ed alle regole di condivisione delle operazioni di lettura/scrittura delle aree dedicate ai trasporti nel caso di carte multifunzionali*

- ❖ Definire, in maniera univoca e chiara, per ogni condizione operativa di funzionamento, gli stati logici e fisici dei vari apparati coinvolti
- ❖ Stabilire regole di comportamento ben precise (protocollo) e documentate per l'Azienda (specifiche progettuali)
- ❖ Garantire la possibilità di adottare le opportune procedure operative di gestione (*per esempio procedure operative del personale di deposito per la movimentazione dei mezzi*)



L'esempio CTP: "Sistema automatico di validazione dei titoli di viaggio integrato con UnicoCampania"





Per gentile concessione di TSF e AEP

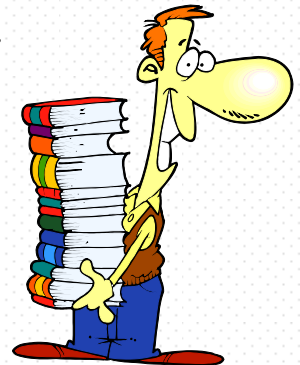
- ❖ Utilizzo di file log per la registrazione degli eventi che risultino facilmente fruibili ed immediatamente interpretabili ai fini manutentivi (*per esempio diagnostica apparati*)

Garanzia della continuità (affidabilità) di servizio in caso di anomalia nel tempo
(*rottura Hw, malfunzionamento Sw, etc.*)

- ☞ Importante la qualità della fornitura, ma anche la manualistica, la formazione degli operatori in base alle procedure operative definite ed i livelli di servizio garantiti dal servizio di manutenzione
- ☞ **ATTENZIONE:** alla valutazione dei livelli di servizio

Esiste un gran numero di normative applicabili agli apparati

- ☐ Non sempre sono tutte di facile comprensione ad un lettore "non specializzato"
- ☐ E' una materia sempre in evoluzione che richiede continui aggiornamenti
- ☐ Verificare il contesto di attuazione e riferimento
- ☐ Evitare "copia ed incolla" nelle specifiche tecniche e nei capitolati
- ☐ Non solo rispetto delle normative ma anche regola d'arte nell'installazione degli apparati a bordo e delle infrastrutture di terra



GRAZIE PER L'ATTENZIONE !

