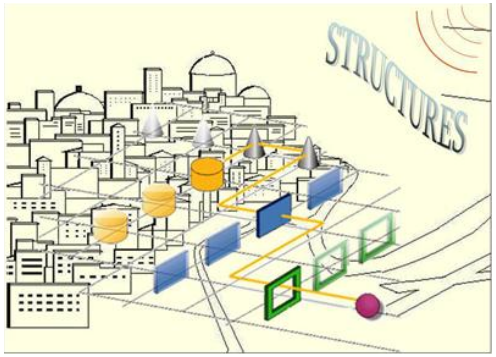
Le radiazioni elettromagnetiche ad alta potenza per la sicurezza e la difesa

29 Ottobre 2015, C.I.S.A.M. - San Piero a Grado (Pisa)



STRUCTURES

Strategies for The impRovement of critical infrastrUCTUres Resilience to Electromagnetic attackS

Mario Antonelli
Computational E.M. and Antenna Design Laboratory
System Engineer / Space Activities & International Services
IDS - Ingegneria dei Sistemi

Sommario

- Introduzione al Problema delle Minacce Elettromagnetiche Intenzionali (IEMI)
- Presentazione al Progetto STRUCTURES
- Definizione ed Analisi dello Scenario
- Procedura di Simulazione
- Stima del Rischio
- Metodi di Protezione

Introduzione

- In applicazioni militari la vulnerabilità dei sistemi elettrici/elettronici a interferenze elettromagnetiche ad alta potenza è nota da diversi decenni

- Attualmente è aumentata la disponibilità di sorgenti che possono produrre radiazioni elettromagnetiche di alta potenza e ad alta frequenza (HPEM)

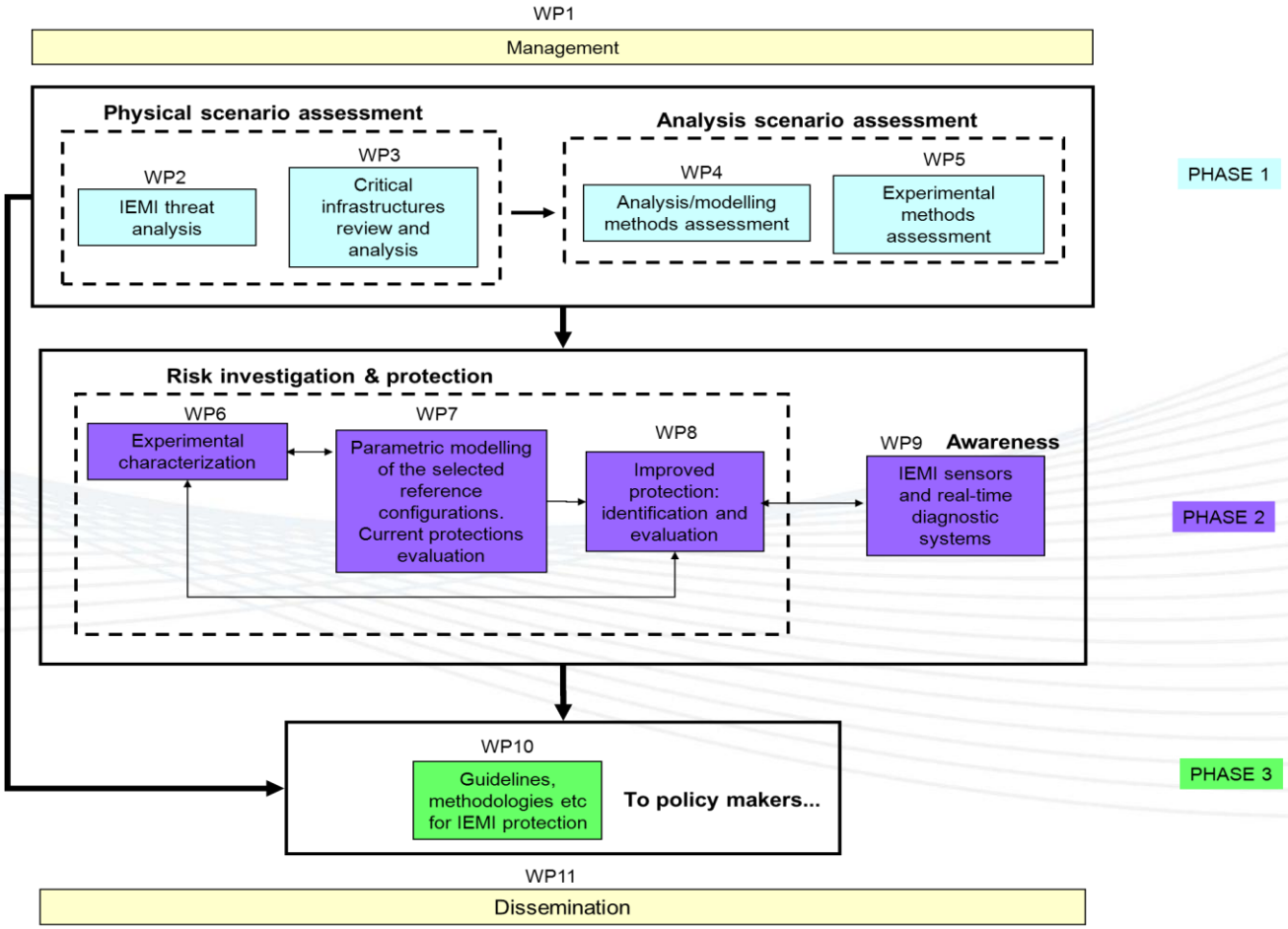
- La crescente dipendenza della società civile da sistemi elettronici ad elevata suscettività e il crescente fenomeno del terrorismo, suggeriscono di prestare adeguata attenzione al problema IEMI (Intentional ElectroMagnetic Interference – Interferenze ElettroMagnetiche Intenzionali)

- Infrastrutture civili e servizi come centrali elettriche, banche, sistemi di trasporto, ospedali, ecc. sono potenziali vittime di interferenze elettromagnetiche

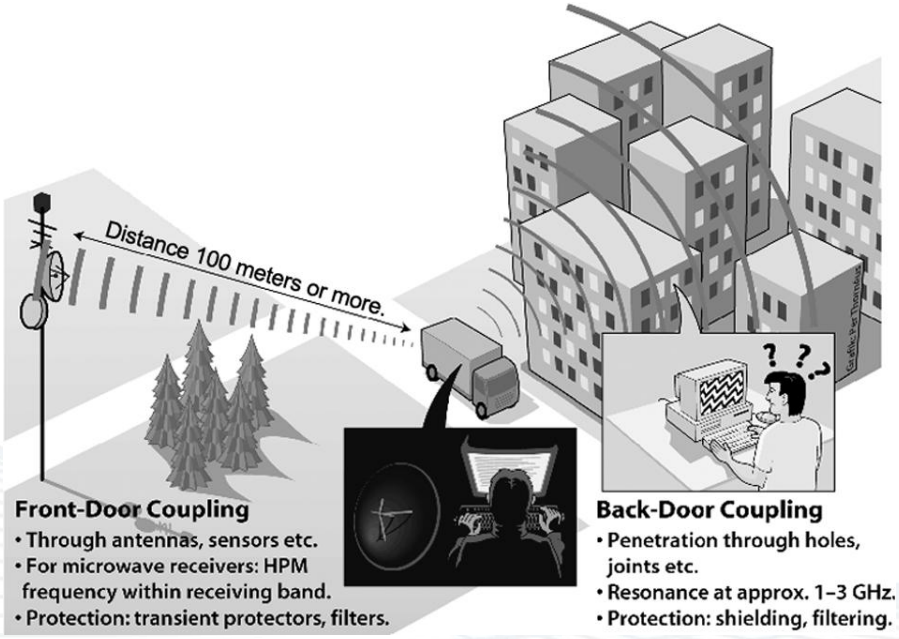
Progetto STRUCTURES

- Una parte significativa del contenuto di questo contributo è legato alle attività svolte nel progetto STRUCTURES (http://www.structures-project.eu/) un progetto di ricerca svolto nell'ambito del Settimo Programma Quadro per la ricerca europea (FP7)
- Il progetto ha coinvolto 12 partecipanti tra cui Università, PMI e Industrie, con il coordinamento di IDS
- I principali obiettivi del progetto sono:
  - identificare le infrastrutture che possono definirsi "critiche"
  - analizzare le possibili minacce elettromagnetiche intenzionali
  - valutare l'attuale livello di protezione delle infrastrutture critiche
  - identificare innovative strategie di protezione
  - fornire ai legislatori un quadro realistico e misurabile sull'effettiva consistenza della minaccia e sulle conseguenze di un attacco elettromagnetico
  - proporre e sviluppare linee guida

Organizzazione del Progetto



Inquadramento del problema



"**Front door**" si manifesta in quelle situazioni in cui l'interferenza entra all'interno dell'infrastruttura attraverso i principali punti di ingresso (ovvero, antenne, porte finestre, ecc.)

"**Back door**" si manifesta in quelle situazioni in cui l'interferenza entra all'interno dell'infrastruttura attraverso involontari punti di ingresso (ovvero, saldature, giunzioni, riduzioni involontarie delle schermature, ecc.)

- Accoppiamento Radiato: avviene quando le vittime sono direttamente illuminate da un campo elettromagnetico prodotto da una sorgente lontana
- Accoppiamento Condotto: il disturbo elettromagnetico è iniettato direttamente in un punto lungo il percorso del cavo, l'accoppiamento condotto può ritenersi significativo nell'intervallo di frequenze che vanno dai kHz ai MHz

Analisi delle minacce elettromagnetiche

- Uno dei primi obiettivi del progetto STRUCTURES è stato quello di fornire una classificazione delle minacce di tipo HPEM per:
  - fornire un input al processo di valutazione del rischio
  - dare evidenza alle Autorità della concretezza del rischio

- Le sorgenti (radiate e condotte) sono state classificate in base alle loro caratteristiche tecniche, ovvero:
  - contributo in frequenza
  - picco del campo elettrico o della tensione
  - forma d'onda dell'eccitazione

Verosimiglianza del Rischio

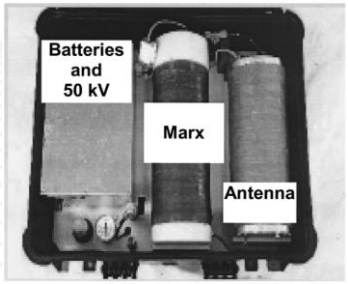
- Per un'attenta valutazione della probabilità di un attacco per mezzo di una determinata sorgente EM, è necessario includere nell'analisi anche caratteristiche non tecniche

- Una prima caratterizzazione del rischio associato alle sorgenti IEMI può essere fatta in base a tre fattori chiave:
  - Disponibilità, ovvero una misura sia del costo e che del livello di conoscenza richiesto per la produzione
  - Mobilità
  - Livello tecnologico della minaccia (basso, medio, alto)

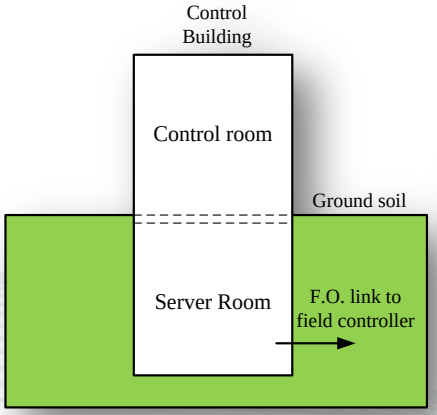
Alcuni (allarmanti) esempi

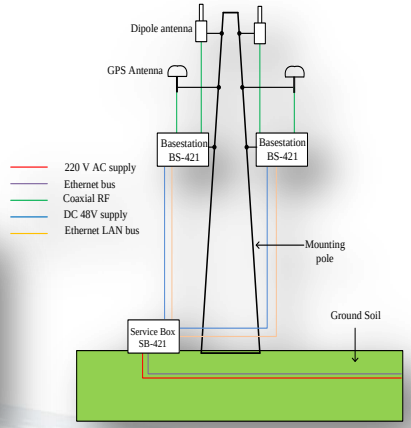
Diehl Munitions System.

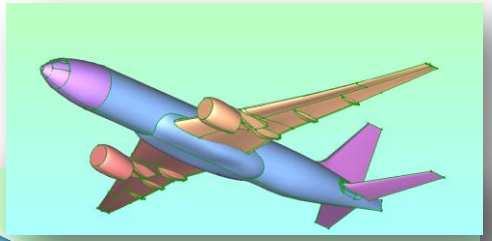
- 350 MHz damped sine field
- Peak electric field at 1m: 125 kV/m.
- 50x40x20 cm
- 30 minute continuous operation (5 pulses per seconds or 3 hours in bursts

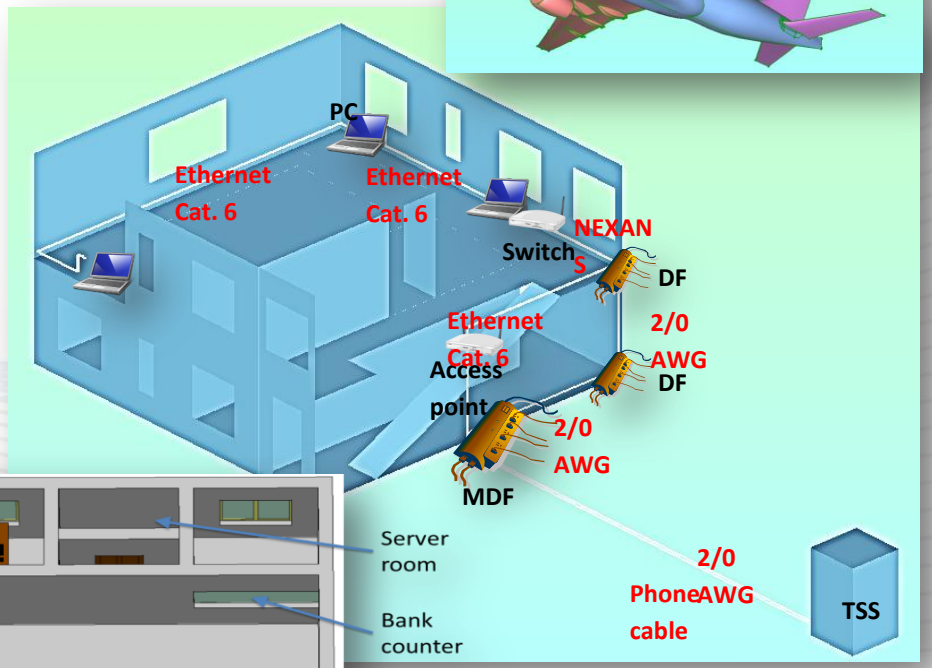


Infrastrutture Critiche Selezionate

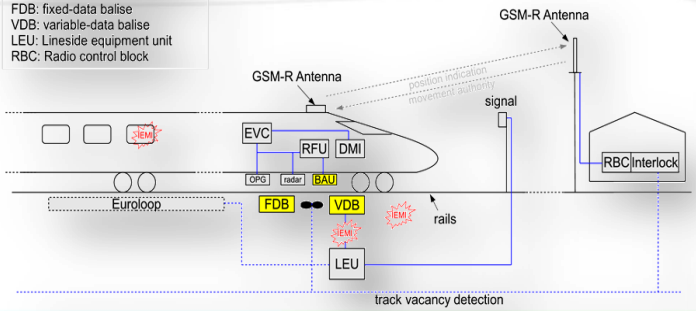


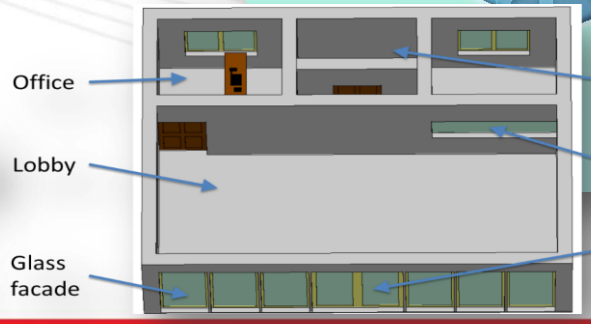






EVC: European vital computer
RFU: receive-&-forward unit
DMI: driver-machine interface
OPG: odometer pulse generator
BAU: balise antenna unit
FDB: fixed-data balise
VDB: variable-data balise
LEU: Lineside equipment unit
RBC: Radio control block





Procedura di Simulazione

- Nel WP7 è stata effettuata l'analisi dei rischi per ognuno dei sei tipi di infrastruttura critica individuati
- Per ogni infrastruttura, è stata definita una configurazione di riferimento, la quale comprende:
  - CAD 3D (geometria struttura e routing dei cavi)
  - materiali
  - un elenco delle apparecchiature vittime
  - sono stati individuati i livelli di suscettività dei dispositivi vittime

- E' stata identificata una procedura di modellazione adeguata ad un'efficace gestione dei problemi IEMI considerando budget e tempi limitati e mantenendo al tempo stesso la possibilità di applicare le più precise tecniche di analisi (allo stato dell'arte)

Stima del Livello di Interferenza

- L'analisi numerica è stata usata in maniera estensive per la valutazione del livello di interferenza

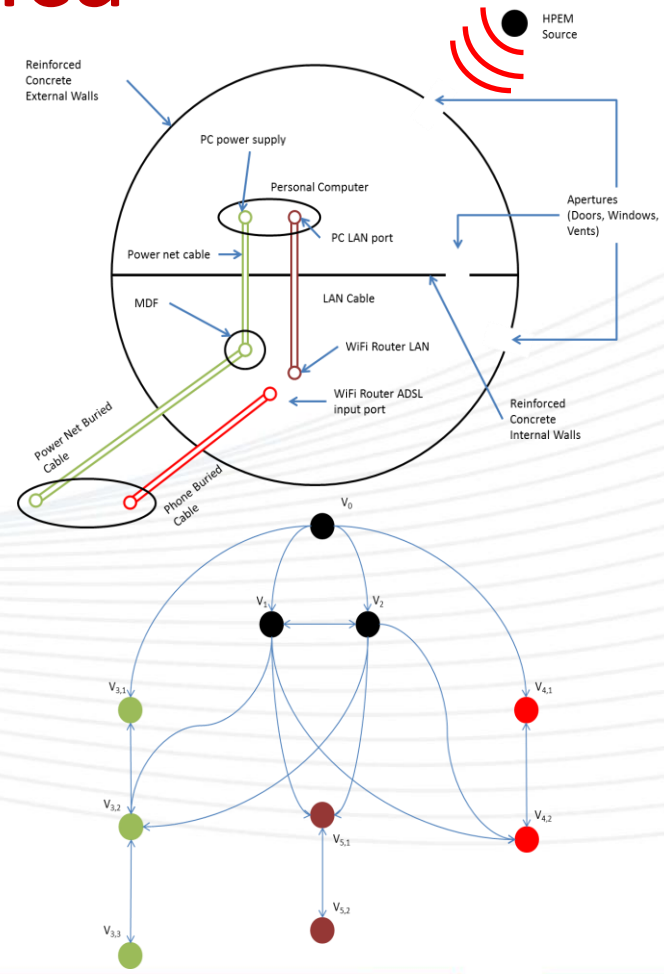
- L'approccio proposto si basa su due passi sequenziali:
  - Analisi Topologica:
    - Decomposizione dello scenario in volumi elementari
    - Definizione del digramma di interazione → percorsi di accoppiamento tra i volumi
  - Analisi dettagliata:
    - Metodi nel dominio della Frequenza o del Tempo

Analisi Topologica

- L'analisi topologica (C. Baum) è un passo preliminare che consiste nel chiarificare il problema totale allo scopo di semplificare il modellamento numerico per l'analisi di dettaglio focalizzando l'attenzione sui principali punti critici

- In questa fase vengono identificati:
  - Elementi dello scenario: stanze, e dispositivi suscettibili
  - Percorsi di accoppiamento: pareti, finestre, porte, cavi, antenne

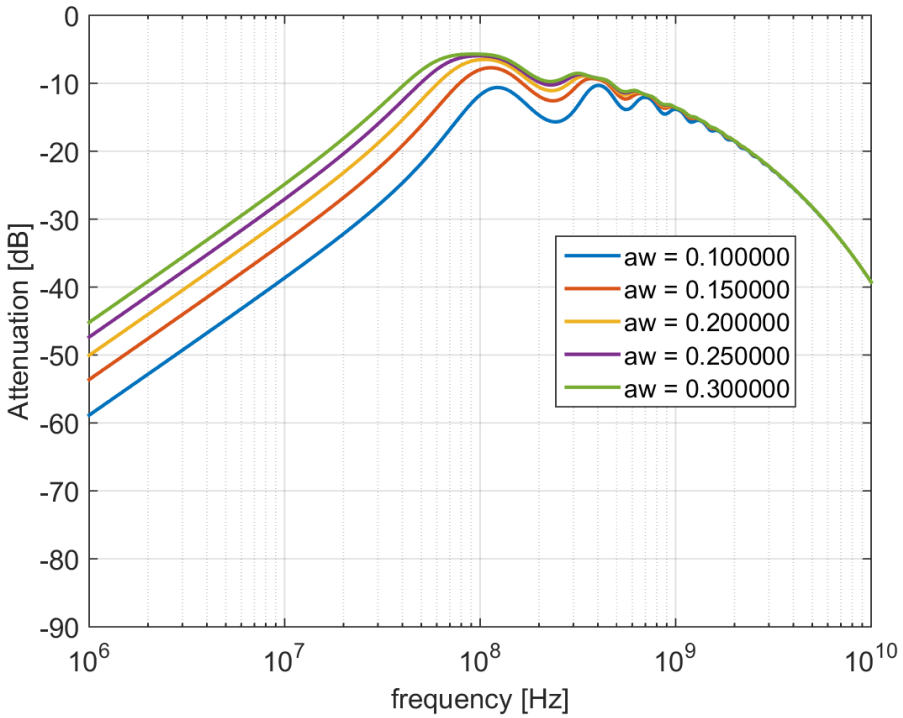
- Vengono trascurate interazioni multiple tra gli elementi



Analisi preliminare basata sui modelli semplificati

- I modelli semplificati sono stati utilizzati nel contesto dell'analisi topologica per una prima valutazione del livello di rischio
  - modelli analitici di antenne
  - modelli di aperture
  - modelli di accoppiamento cavo-campo
  - modelli analitici di muri, ecc.

Coefficiente di trasmissione per diverse spaziatura dell'armatura del cemento armato



Analisi Dettagliata: Catena Computazionale

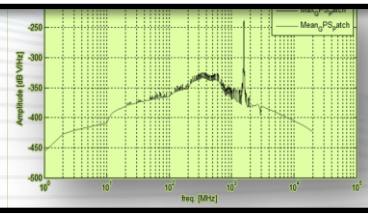
Valutazione Funzione Trasferimento (FT)

Minaccia esterna: Onda Piana
Minaccia Interna: Dipolo

Antenna Minaccia (Reale)

FT Processamento: Minaccia Reale→ Diagramma di radiazione & Forma d'onda

Segnale interferente nel dominio della frequenza (livello di campo o tensione alle porte)



FFT $^{-1}$

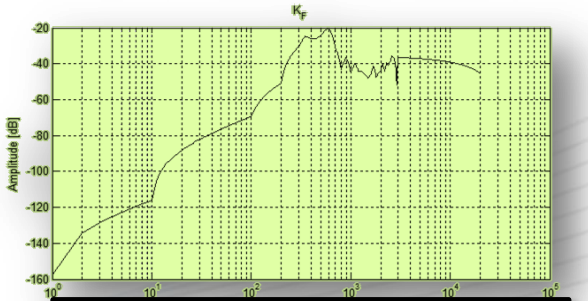
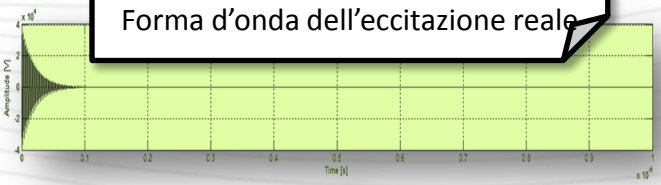
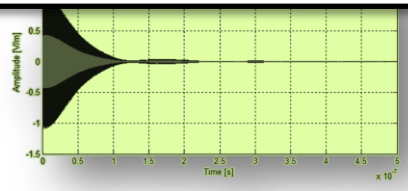


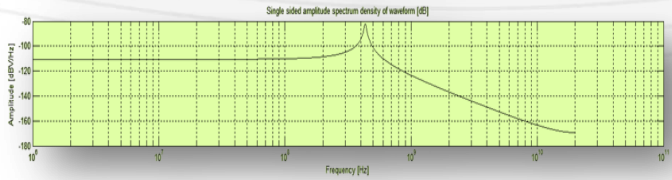
Diagramma di Radiazione Antenna Reale
Forma d'onda dell'eccitazione reale



Segnale interferente nel dominio del tempo (livello di campo o tensione alle porte)



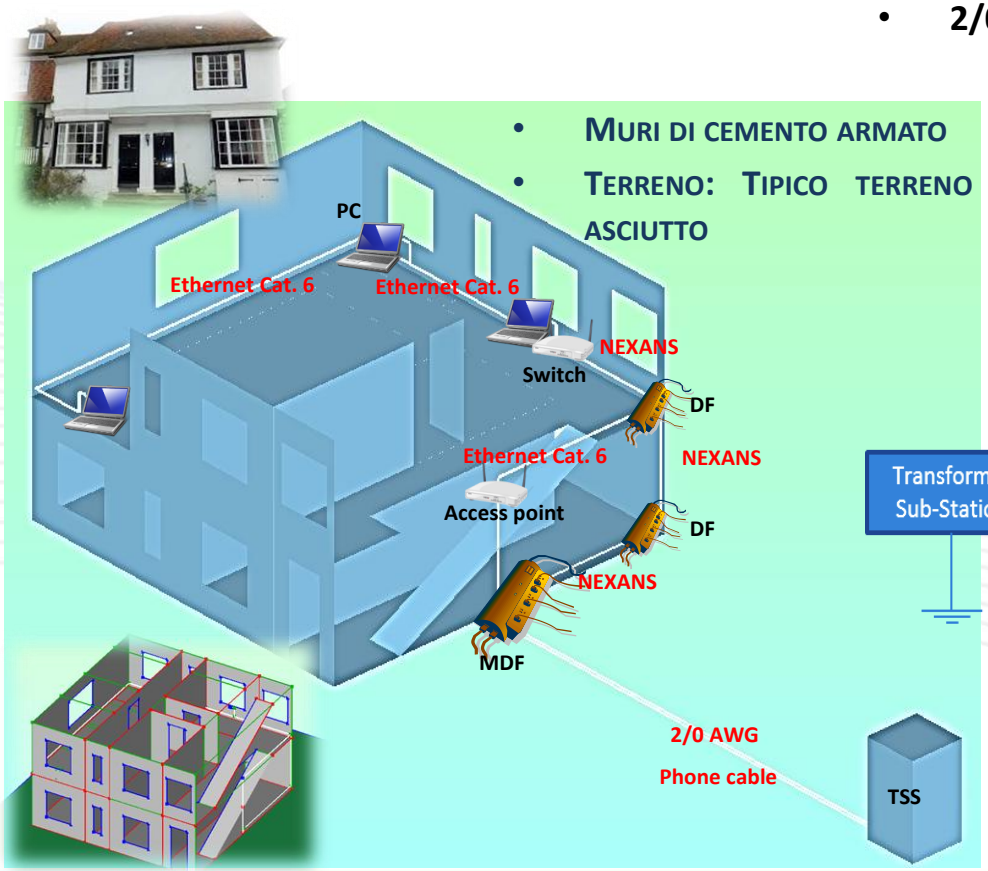
Valutazione della potenza o dell'energia



Confronto con i livelli di suscettività

Funzione di Trasferimento: Computer Network

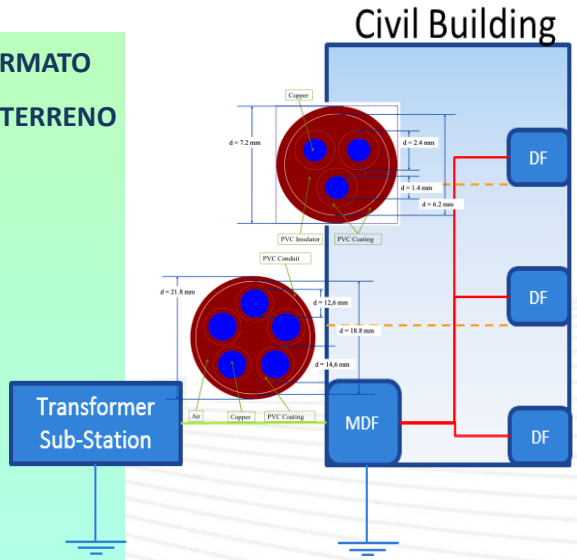
- **DEFINIZIONE SCENARIO**



- MURI DI CEMENTO ARMATO
- TERRENO: TIPICO TERRENO ASCIUTTO

DISTRIBUZIONE ELETTRICA

- **2/0 AWG + NEXANS CABLES (BD)**



WIRED LAN NETWORK

- ETHERNET CAT.6
- CAVO TELEFONICO / ADSL

WIRELESS LAN NETWORK

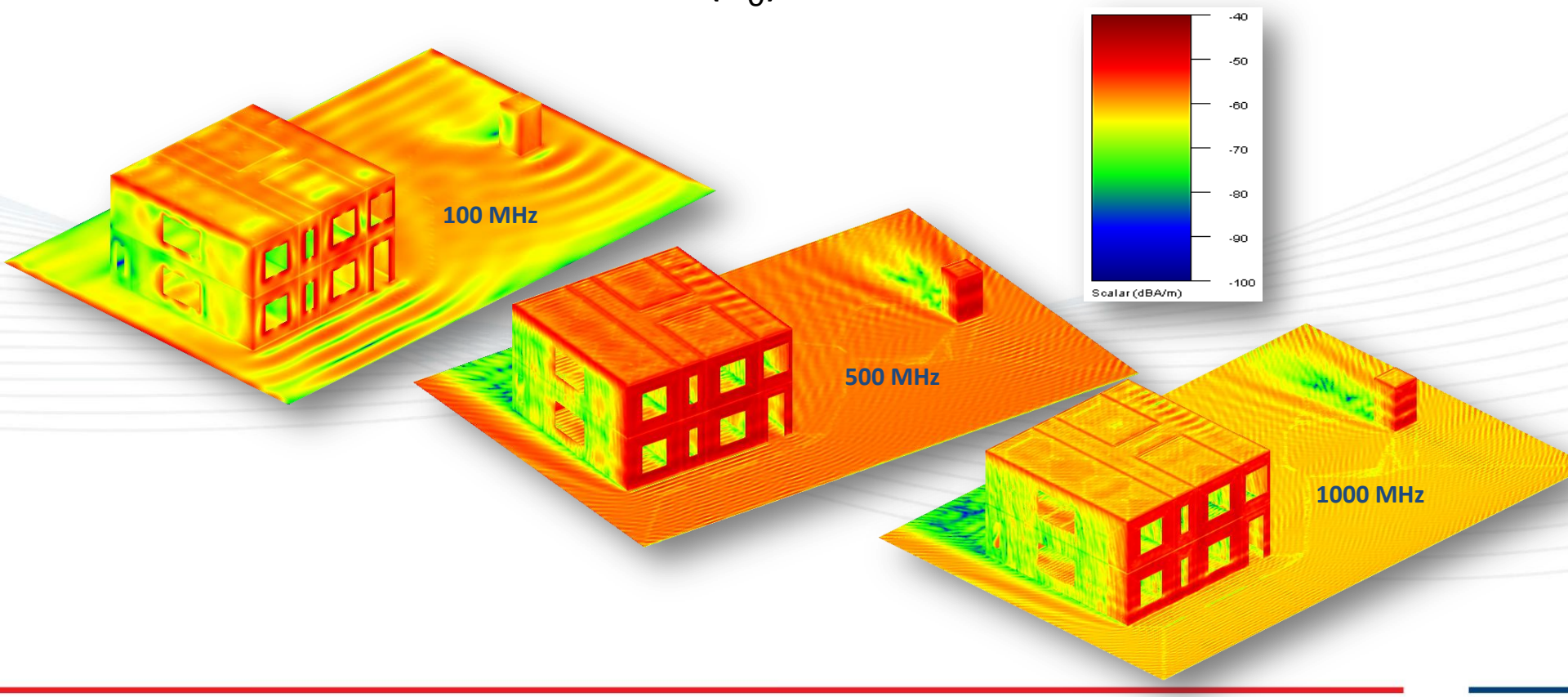
- ANTENNE WIRELESS, (802.11 WLAN)
- RICEVITORE WIRELESS CON FILTRO PRE-SELETTORE

MINACCE

- ESTERNA: ONDA PIANA (DIVERSE DIREZIONI)
- INTERNA: ELICA

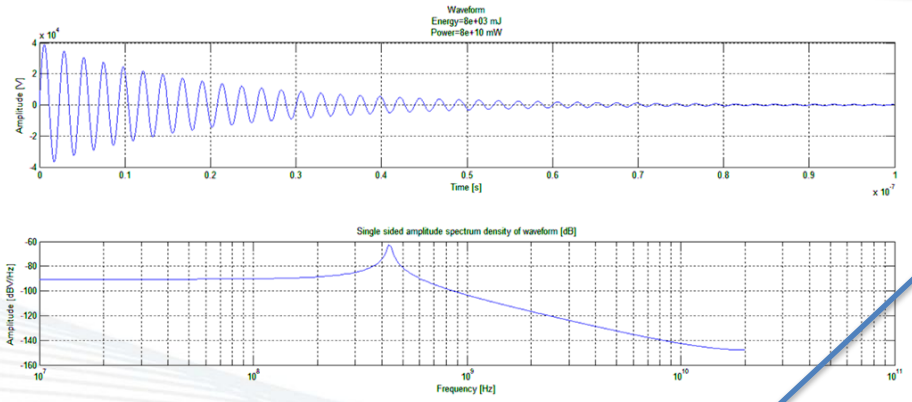
Distribuzioni delle correnti

Funzione di Trasferimento: $I = F(E_0)$



Valutazione Livello di Interferenza

Forma d'onda



Livello di Interferenza,
Frequenza → Tempo

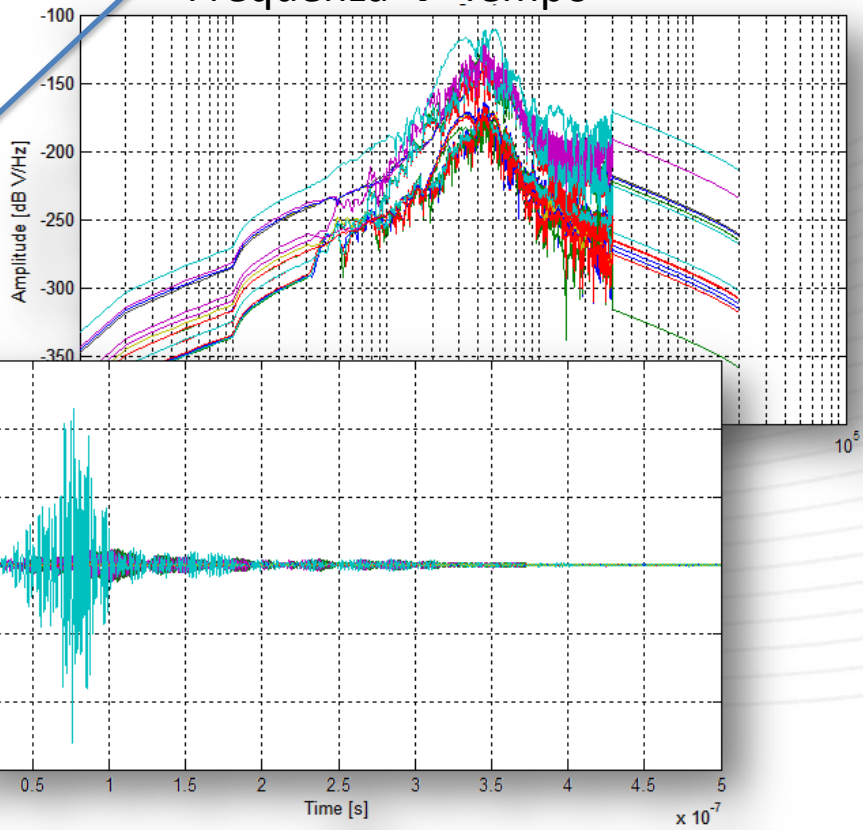
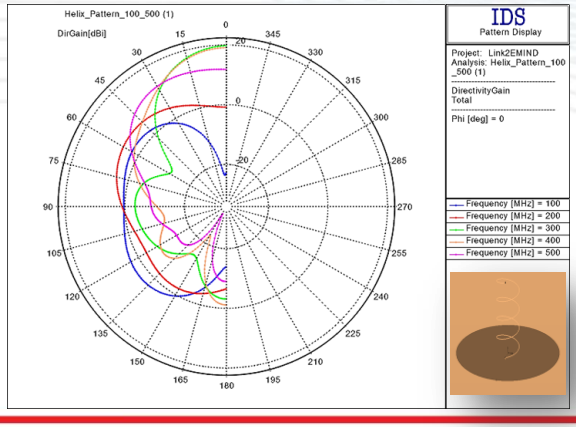
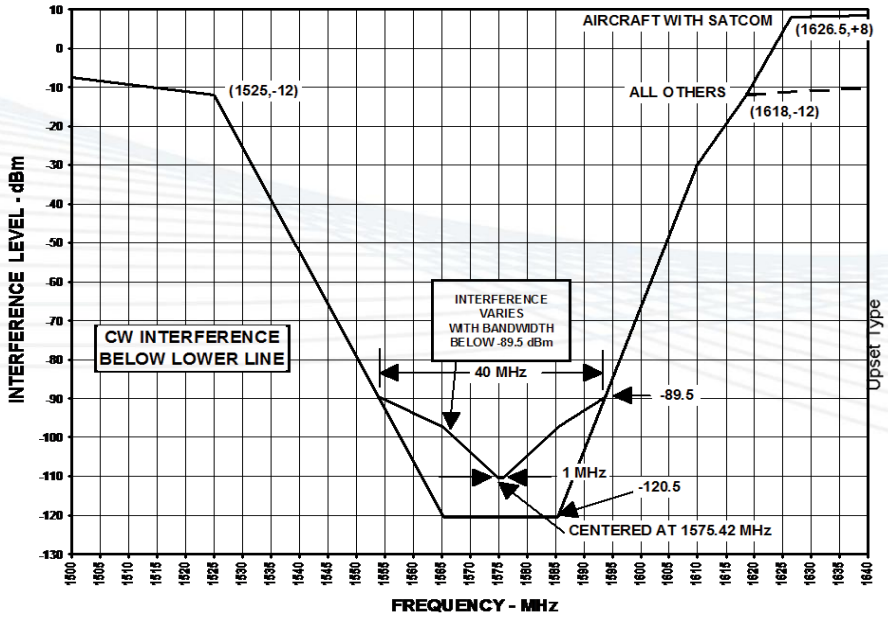


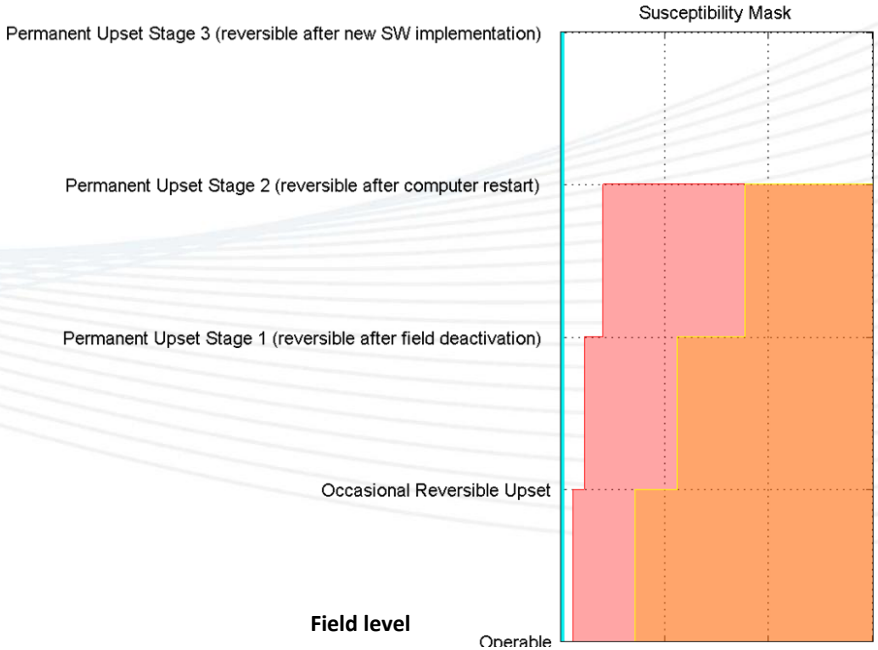
Diagramma di radiazione



Valutazione del livello di Rischio

- I livelli di interferenza valutati vengono confrontati con ii livelli di suscettività delle apparecchiature vittime





Tecniche di protezione: Back Door

- Back Door
  - Schermaggio:
    - Materiali di costruzione possono essere sfruttati per fornire un grado limitato di schermatura (un'analisi caso per caso è richiesta)
    - Metallo può essere utilizzato per bloccare completamente campi elettromagnetici
    - Una gabbia metallica completa: gabbia di Faraday
    - Costosi e non sempre applicabili
  - Filtri
  - SPD (Surge Protection Devices)

Tecniche di protezione: Front Door

- Come proteggersi da attacchi IEMI di tipo Front-Door preservando al tempo stesso il servizio?
  - Nel contesto di STRUCTURES è stata progettata una nuova tecnica “a basso costo” per la detezione e localizzazione di minacce IEMI:
    - Localizzazione basata su analisi delle differenze dei tempi di arrivo dei segnali raccolti una sensoristica distribuita
    - Identificazione della sorgente basata sulla analisi del segnale ricevuto
  - Smart Antennae
  - AFSS: Superfici selettive in frequenza, BP or BS

Conclusioni

- La realizzazione del progetto STRUCTURES rende disponibili per utilizzatori finali, strumenti utili per la difesa da attacchi elettromagnetici intenzionali
- Sono stati proposti metodi di modelling innovatovi
- Sono definiti metodi di protezione e rilevamento minacce
- La conoscenza dei livelli di vulnerabilità potrà aiutare nella definizione di un quadro normativo rinnovato per una migliore protezione delle IC