CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

In collaborazione con

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

"La Strategia Nazionale di Cybersecurity: impatto e prospettive"
Ciclo di webinar a cura del Centro di Competenza Cyber 4.0

SCRUTINIO TECNOLOGICO, CERTIFICAZIONE E VALUTAZIONE DI SICUREZZA

Mercoledì 6 Luglio 2022 ore 16.00

Interverranno:
Leonardo Querzoni *Presidente Cyber 4.0*
Andrea Billet *Direttore del Servizio Certificazione e Vigilanza ACN*
Luisa Franchina *Direttore Generale Prisma*
Andrea Morgagni *Evaluation Facility Technical Manager Leonardo SPA*
Gianluca Ruggieri *Responsabile Laboratorio LVS DigitalPlatforms*
Modera: ***Matteo Lucchetti****, Direttore Operativo Cyber 4.0*

Per info:
comunicazione@cyber40.it
www.cyber40.it

Lo standard Common Criteria, applicazioni pratiche

Gianluca Ruggieri

Responsabile L.V.S. DigitalPlatforms

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Certificazione

Processo attuato dall'Ente di Certificazione

**(Presidenza del Consiglio dei Ministri-DIS o
Ministero dello Sviluppo Economico Telecomunicazioni-OCSI)**

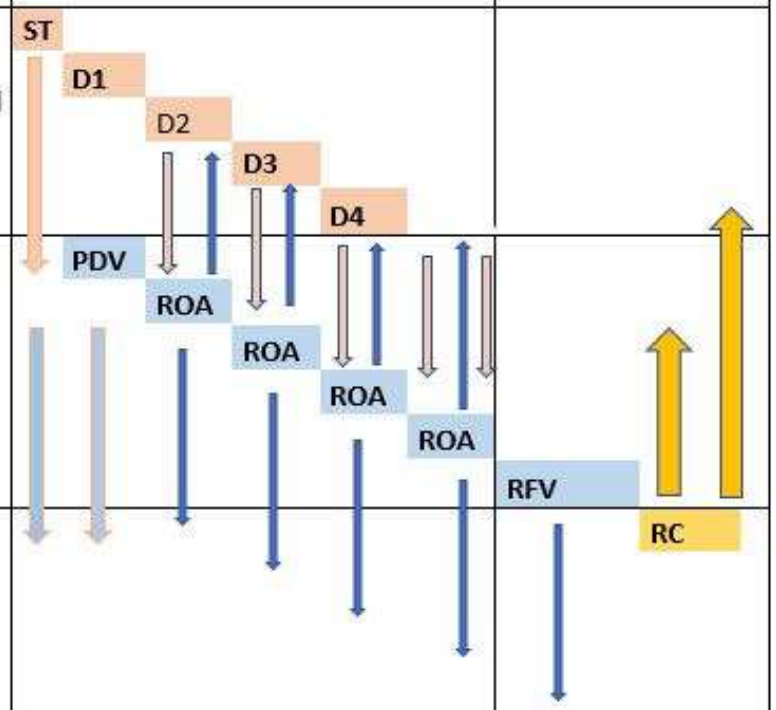
Controlla il processo di valutazione attuato da un laboratorio terza parte (CE.VA. o LVS) ed effettua l'analisi indipendente dei risultati

Produce il certificato finale

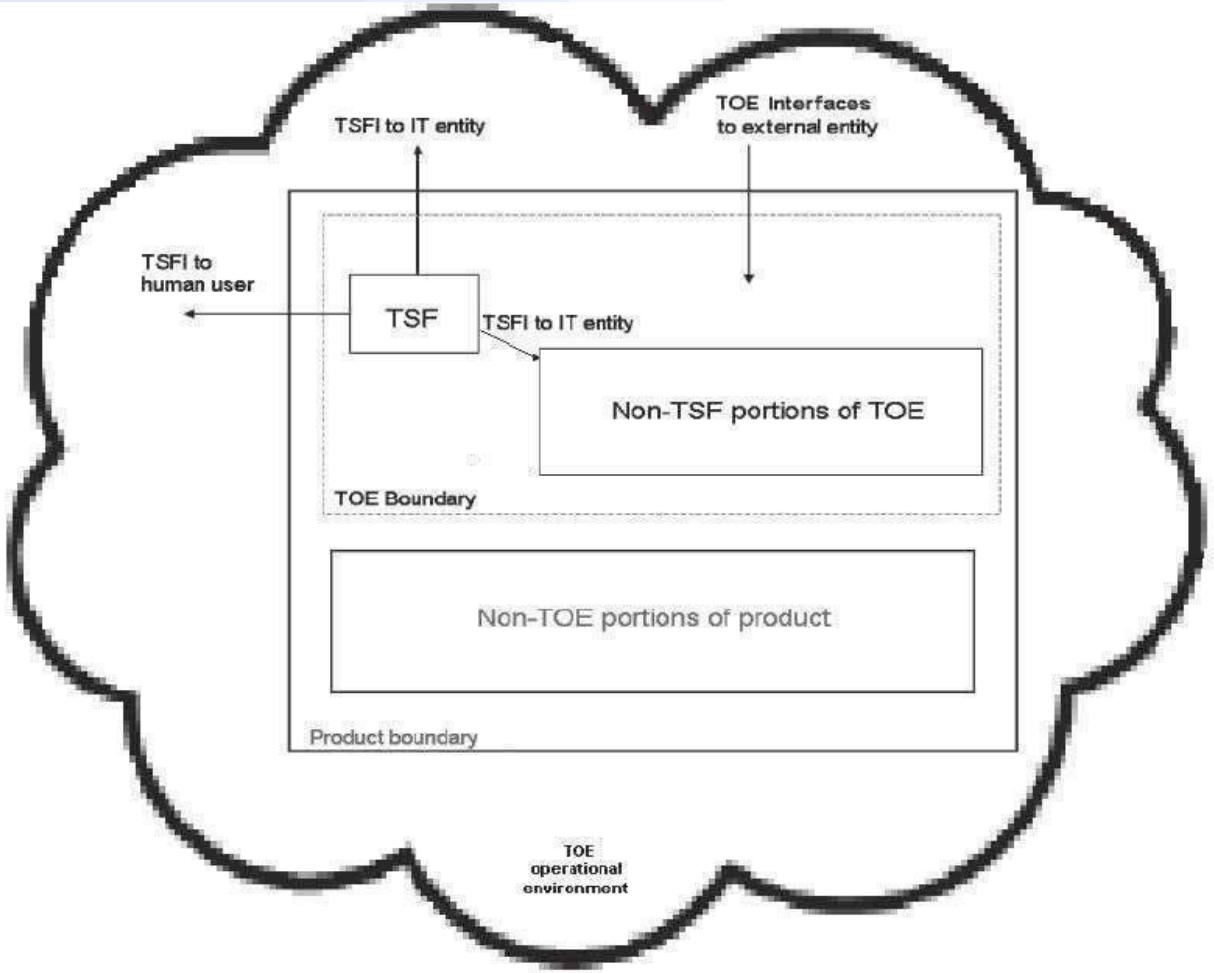
Garantisce maggior coerenza nell'applicazione dei criteri di sicurezza ICT riconosciuti come standard internazionali

Valutazione

	PROGETTAZIONE	VALUTAZIONE	CERTIFICAZIONE
Committente ed LVS in fase di ASSISTENZA	Analisi Preliminare e preparazione del Security Target (ST)		
LVS in fase di VALUTAZIONE			
ENTE DI CERTIFICAZIONE			



Parti dell'OdV (TOE)



Test del Laboratorio

Azioni del Laboratorio

- Test funzionali di sicurezza
- Analisi di Vulnerabilità
- Test di penetrazione

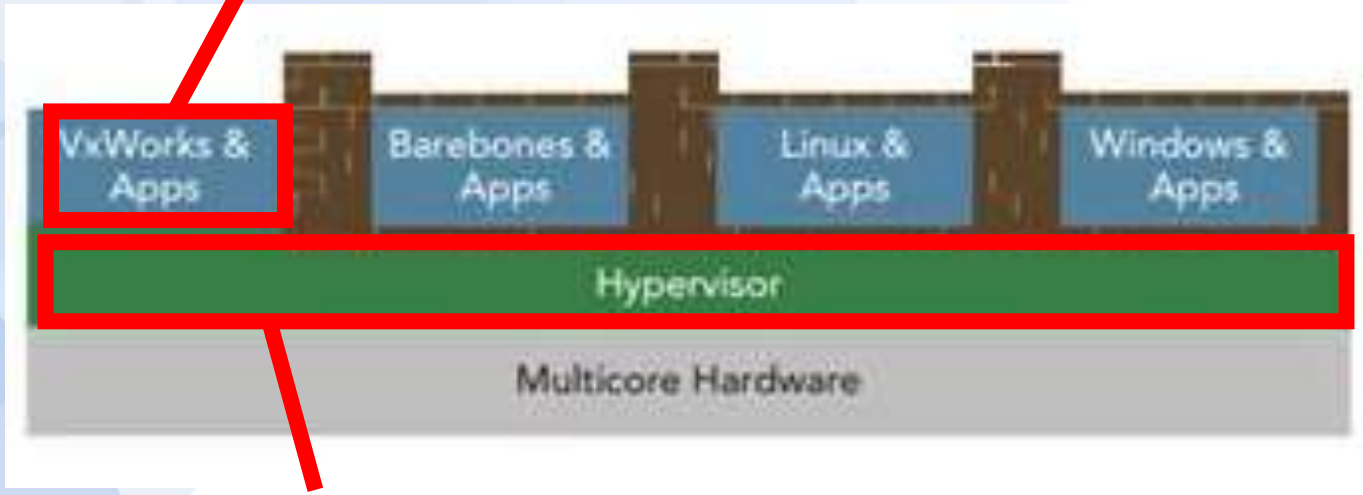
Ambiente di test

- Test bed che rappresenti significativamente il TOE nel suo ambiente
  - Campionamento dei componenti
  - Interconnessioni
  - Simulatori
  - Generatori di input

Test bed e tool documentati nelle evidenze di valutazione

Caso pratico: un prodotto informatico

"Virtual board" abstraction



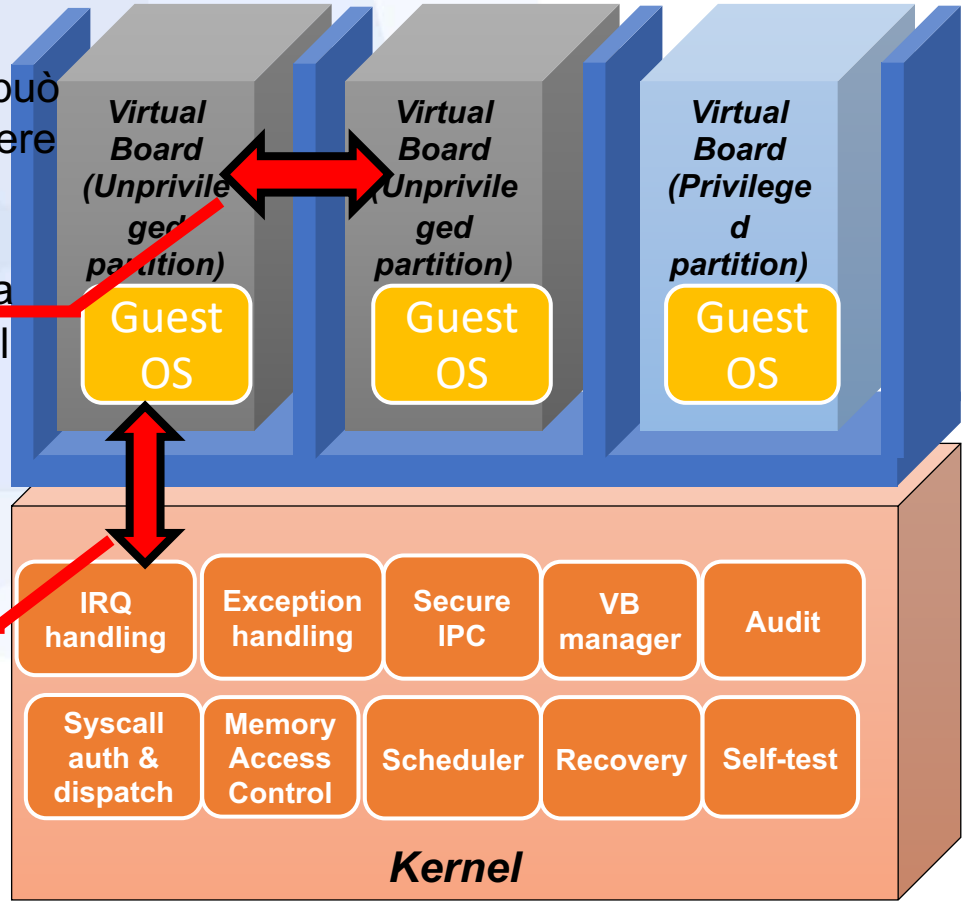
Cornerstone for security!

- A non-privileged domain must not gain access to other domains and the physical board

Architectural Overview

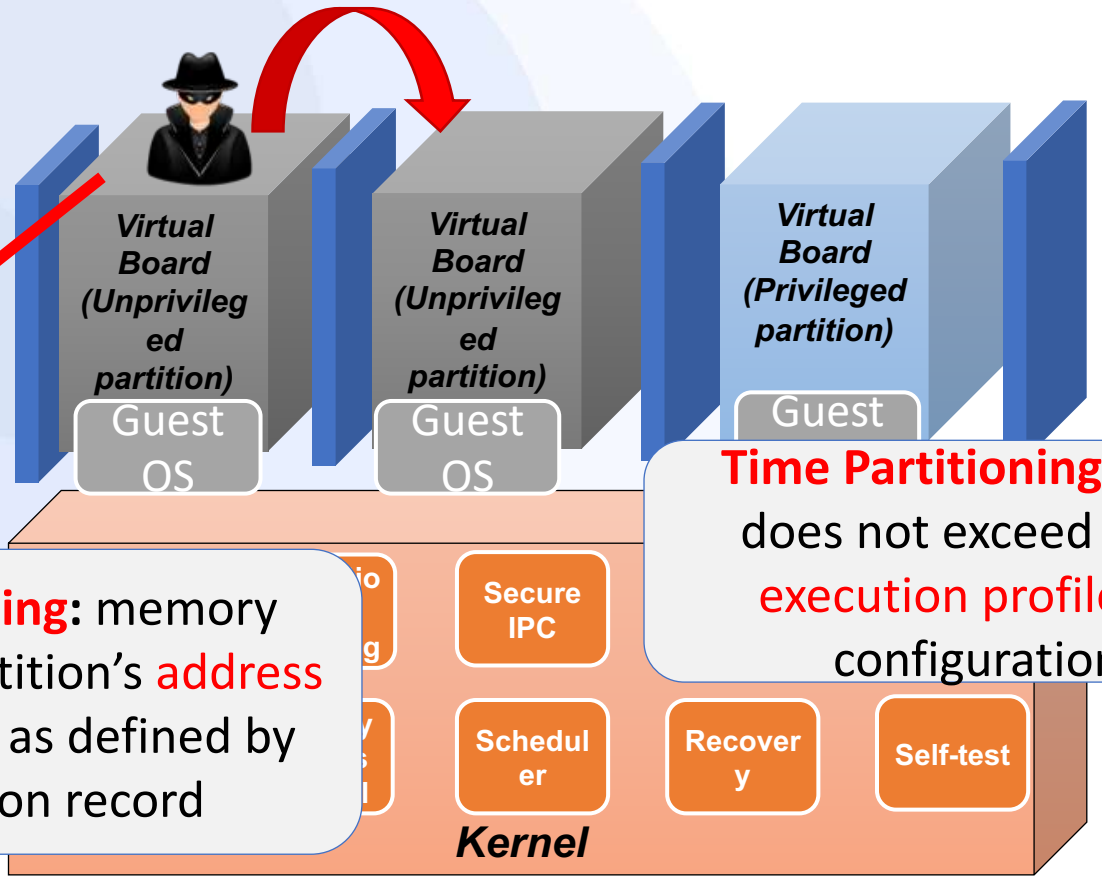
Una Virtual Board può solo inviare o ricevere dati da altre Virtual Board configurate (staticamente) nella **security policy** del sistema

La security policy restringe le **risorse** ed i **servizi** di sistema utilizzabili da ogni Virtual Board



Attack Model

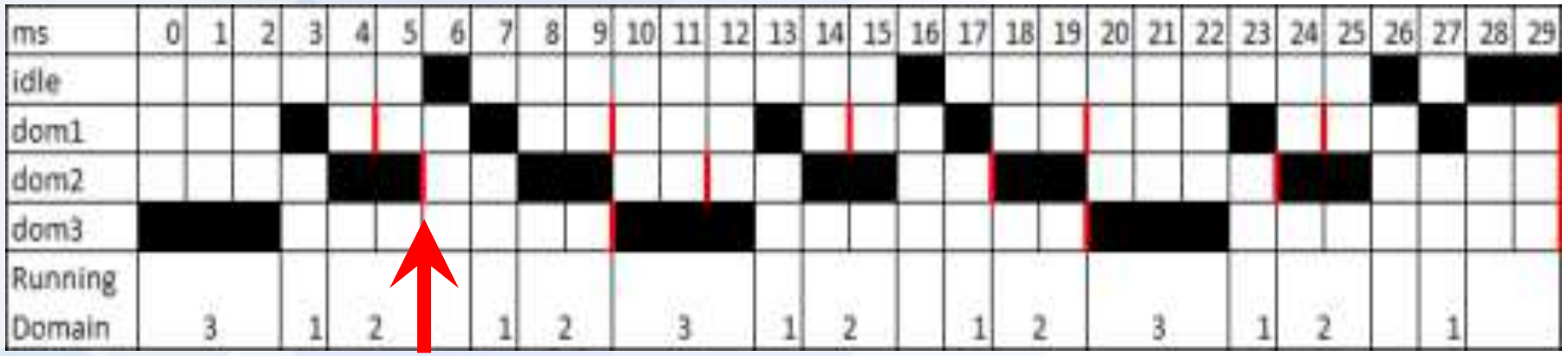
Il software di una VB (incluso il guest OS) è compromesso e tenta di sovvertire le proprietà di **partizionamento robusto**



Memory Partitioning: memory access beyond a partition's address space is prohibited as defined by the configuration record

Time Partitioning: a partition does not exceed its allotted execution profile as in the configuration table

Deterministic Scheduling



Delay between switch-out (VB_{i-1}) and switch-in (VB_i)

The kernel enforces periodic, deterministic CPU scheduling

A context switch occurs between the time frames

Timing covert channels

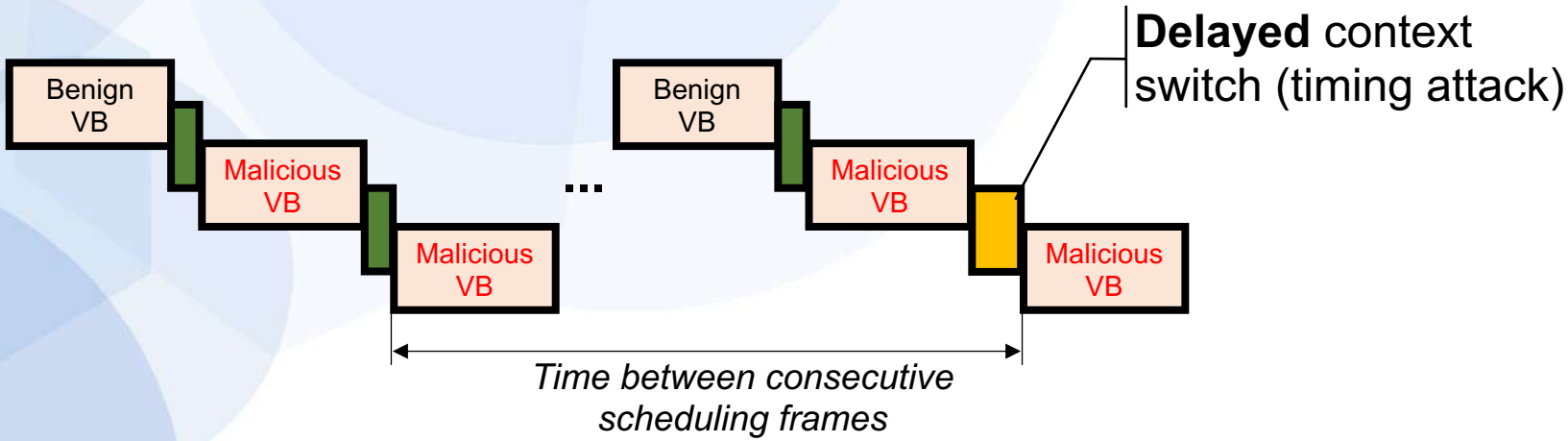
- **Una virtual board non deve essere in grado di alterare il tempo di context switch per trasmettere informazioni (presenza/assenza di ritardo)**
- **Lo scheduler impone che il tempo di context-switch sia fisso, introducendo un ritardo compensativo**

Pen Test Timing Covert Channel

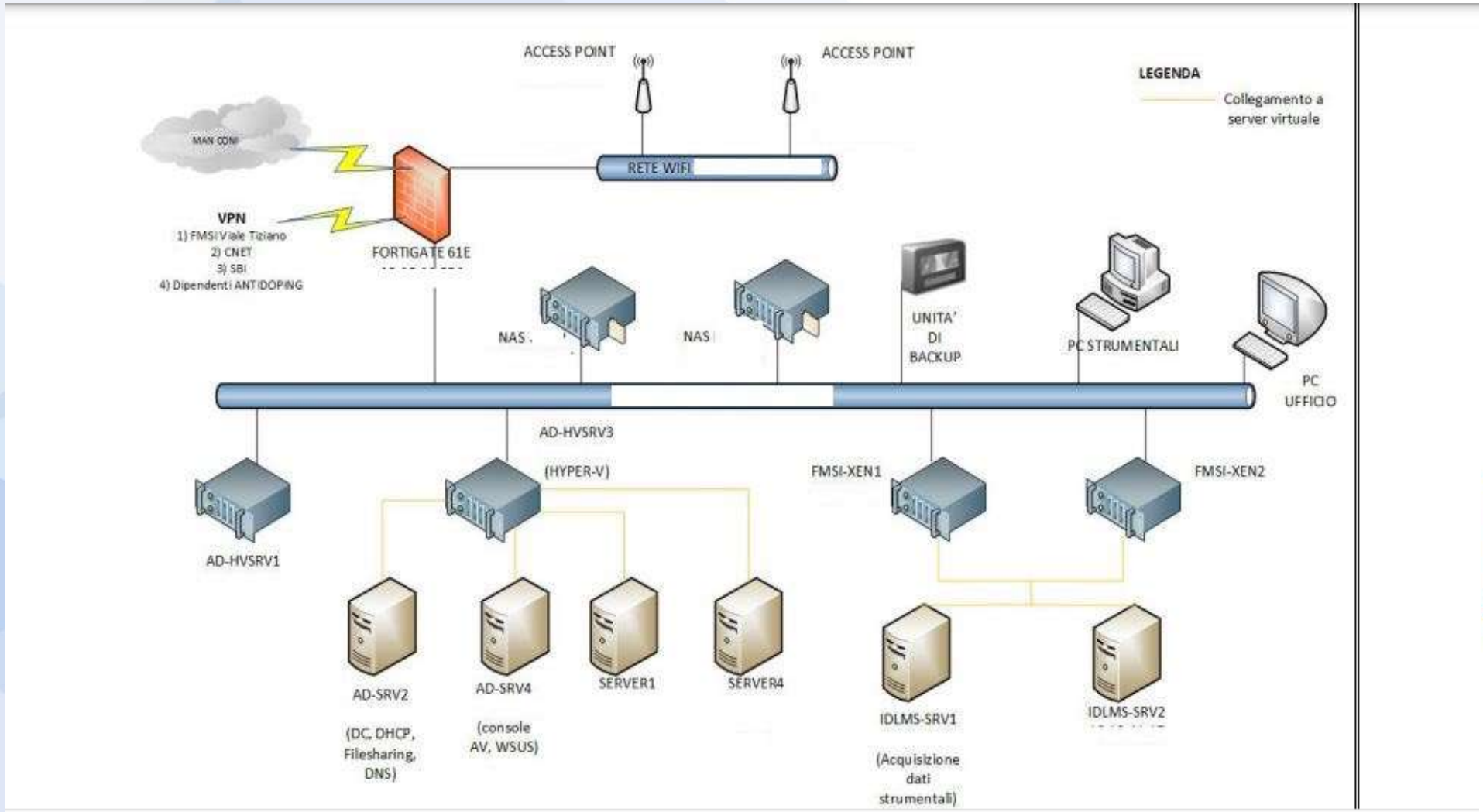
We challenge deterministic CPU scheduling with a **virtual board that performs stressful activity**,

The VB aims to **delay the time-between-scheduling-frames**

Delays can be used to transmit confidential information to the other virtual board



Caso pratico: un sistema informatico



Caso pratico: un sistema informatico

- Funzionalità di sicurezza “distribuite” tra i vari applicativi che costituiscono il sistema
- Vulnerability Assessment e Penetration tests realizzabili con i classici tools già presenti sul mercato
- Suddivisione in sottosistemi coincidente il più delle volte con la suddivisione fisica dei vari apparati
- Problematiche diverse da affrontare rispetto ad una valutazione di prodotto
- Ricorso a COTS certificati per l’espletamento di alcune funzionalità di sicurezza (tipicamente il controllo accessi demandato ai Sistemi Operativi)

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Your Innovation will come true with us!

Grazie.