



STATO MAGGIORE DELLA DIFESA

VI Reparto - Sistemi C4I e Trasformazione

Stato Maggiore Difesa

CONVEGNO

ANUTEI

LA PROTEZIONE DELLE INSTALLAZIONI MILITARI
IN PATRIA

Tema

SICUREZZA NELLA TRASMISSIONE DATI
IN ATTIVITA' DI CUSTODIA ...

Roma, 23 Aprile 2009

*Col. t(tlm) s.SM Enrico BOLOGNA
Capo Ufficio Sistemi Integrati NEC*



Sommario

Stato Maggiore Difesa

- 1. Premessa**
 - a. Classificazione Siti**
 - b. Principi**
 - c. es. Vigilanza & Sorveglianza**
- 2. Implementazioni di Sicurezza ...**
- 3. Uso di Sistemi Tecnicamente Avanzati ...**
- 4. Conclusioni**



Premessa

Stato Maggiore Difesa

Classificazione dei Siti

- **Cat. A1** (Depositi Munizioni ed Esplosivi, Magazzini e Stabilimenti ove siano custodite Armi);
- **Cat.A2** (Caserme e Aerocampi sedi di Enti logistici/scolastici addestrativi con armerie, riserve munizioni ed esplosivi);
- **Cat. B1** (Magazzini, Parchi e Stabilimenti di mezzi efficienti di elevato valore economico, di agevole asportabilità, difficilmente reperibili in commercio, diversi da armi e munizioni);
- **Cat. B2** (sedi di Comandi/Enti vari, non inseriti in Caserme ove siano custodite Armi e munizioni);
- **Cat. C** (Depositi, Parchi di mezzi e materiali efficienti “non appetibili”).



Premessa

Stato Maggiore Difesa

Principi: Difesa / Protezione / Prevenzione

Sicurezza Assoluta non E ... quindi Protezione ...

- **Presenza / Presidio**
- Normativa / Procedure
- **Controllo / Monitoraggio**
- Misure Integrate Σ
- **Approccio Elettromagnetico non \neq Fisico**
- Ruoli, Privilegi, etc ... ma rispettando registrazione, archiviazione, tracciabilità ...
- **Parole d'ordine / Chiavi ... fisiche \neq elettroniche**
- apertura / chiusura forzata ...
- **predisposizioni eventi ... (allagamenti, incendi, calamità naturali, etc)**



Premessa

Stato Maggiore Difesa

ES. Vigilanza & Sorveglianza - attività principali:

- Controllo Accessi, Aree Vitali (sistemi elettronici - centrale di gestione)
- **Controlli Saltuari (su automezzo, giro dell'installazione / percorso fra le recinzioni, ... non ≠ approccio se il sensore non è umano;**
- Disponibilità nucleo di pronto intervento, idoneo ad eseguire procedure di intervento/alertamento dei dispositivi di difesa contro minacce
 - **controllo entrata ed uscita visitatori;**
 - presidio accessi (durante ingresso e uscita personale dipendente);
 - **custodia (registrazione/traccia) chiavi locali ed uffici dell'installazione;**
- Altre predisposizioni di sicurezza ... incendio, etc

USO APPARECCHIATURE ELETTRONICHE O ROBOTIZZATE ???

- **È CAMBIATO LO STRUMENTO, NON LA SOSTANZA!**
- **MINACCIA VIRTUALE AFFRONTATA – PARITETICO APPROCCIO
CONSIDERARE IN AGGIUNTA IL PERCORSO INFORMAZIONI
LA TRASMISSIONE DEI DATI**



Implementazioni di Sicurezza

Stato Maggiore Difesa

SICUREZZA FISICA ed ELETTRONICA DELLE INSTALLAZIONI



IERI



OGGI





Implementazioni di Sicurezza

Stato Maggiore Difesa

Requisiti:

Sicurezza ... Protezione ... Assoluta ?

- **Presenza / Presidio**
- Normativa / Procedure

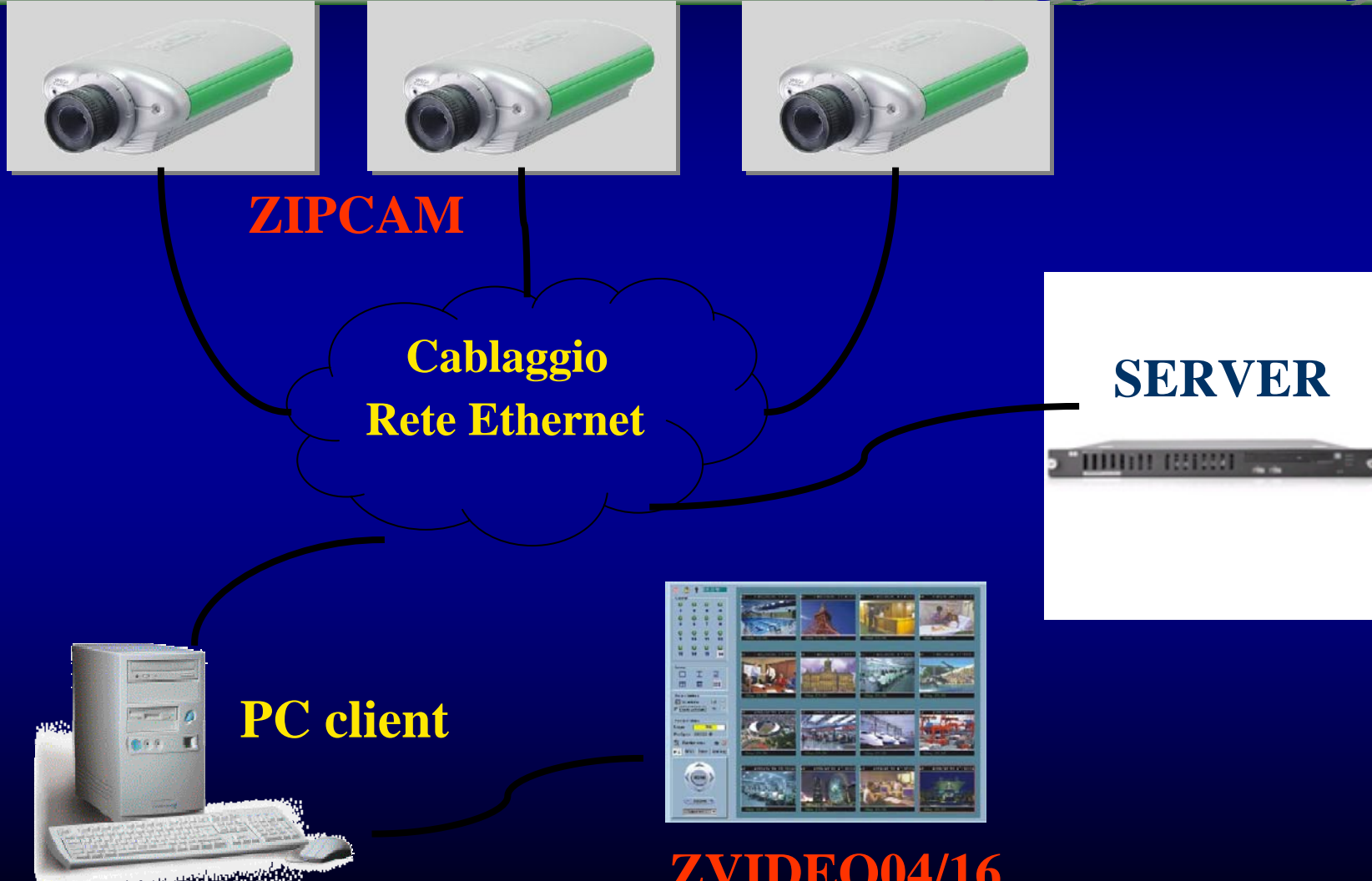
... cosa viene offerto o considerato dal mercato?

- **decodifica Software senza bisogno Hardware aggiuntivo**
- Registrazione manuale, programmata e su allarme
- **Ricerca video tramite data e ora;**
- Esportazione immagini in formato bitmap;
- **Password di protezione ... Chiavi elettroniche**
- Capacità di Compressione;
- **Controllo remoto di Dome Camera**



Un ESEMPIO ?

Stato Maggiore Difesa





Implementazioni di Sicurezza

Stato Maggiore Difesa

Misure Integrate Σ

Applicazione concetto “difesa in profondità” (DID)

tradizionali difese perimetrali necessitano ancor di più di misure aggiuntive

- > livello rischio: più si innalza il livello guardia
- > ambizioni difesa: più le capacità / strumenti specializzati, altamente affidabili o proprietari, etc.

La massima sicurezza ottenibile si raggiunge con la concorrenza di un insieme di strumenti ciascuno dei quali agisce su un livello di possibile rischio ...



Sistemi Tecnicamente Avanzati

Stato Maggiore Difesa

REQUISITI

- Livello di protezione del Sistema
- Attivazione/Disattivazione da remoto
- ...
- **Misure aggiuntive ed integrate protezione** (Protezione in profondità – comporre minimo tre misure, innalzando al max la sicurezza dei dati di gestione del sistema ...)
- **Connettività** (protezione del back-bone, org SMI, etc.) **non può essere solo WEB protection ...**



Sistemi Tecnicamente Avanzati

Stato Maggiore Difesa

Livello di protezione del Sistema

La sicurezza della trasmissione dei dati del Sistema dovrà essere la stessa di quella del sito.

Attivazione/Disattivazione da remoto

Sia del sistema che degli allarmi



Sistemi Tecnicamente Avanzati

Stato Maggiore Difesa

Misure aggiuntive di protezione (Protezione in profondità)

- **1° livello: warning**



- **2° livello: dissuasion**

- **3° livello: action**





Implementazione di Sicurezza

Stato Maggiore Difesa

NECESSITÀ DI SICUREZZA NELLA TRASMISSIONE DATI

I livelli di sicurezza (MSL) si individuano in:

- Perimetrale: Separazioni HW & SW (Firewall, BPD, ...)
- Sicurezza nelle interconnessioni (VPN, NMI – NOC, SOC)
- Sicurezza Client e Server (antivirus, serverlock, ...)
- **Monitoraggio continuo, automatico ed attivo, notifica incidenti e prevenzione intrusioni, procedure di reazione (automatica o attraverso le organizzazioni SMI - CERT ... IDS, IPS, etc)**
- Il mantenimento del livello di aggiornamento continuo dei sistemi di sicurezza (Live – Security, ...)



Sistemi Tecnicamente Avanzati

Stato Maggiore Difesa

Connettività

Su protocollo IP con “*Back-bone*” protetto.

Ai fini di poter impiegare il minimo di banda ed aumentare di conseguenza le misure di protezione dei dati, i sistemi futuri dovranno essere dotati di “*Motion Detector*” ovvero di dispositivi in grado di attivare la registrazione non appena viene rilevato del movimento, variazione ...

E poi

Valgono sempre i Principi di Riservatezza, Integrità, Disponibilità ... (CIA + NR, AAA)



CONCLUSIONI

Stato Maggiore Difesa

Sistemi elettronici di sorveglianza sostituiranno sempre di più sensori e controllori umani

Personale potrà essere maggiormente impiegato per misure di protezione attiva/decisione di intervento/reazione

Ma i principi e l'approccio

devono essere esattamente gli stessi

La sicurezza nella trasmissione dei dati in attività di custodia delle installazioni militari

affrontata stessa maniera / misure ed utilizzando le stesse capacità ed organizzazioni comprese in una più complessa e moderna

INFOSTRUTTURA



SICUREZZA NELLA TRASMISSIONE DATI IN ATTIVITA' DI CUSTODIA DELLE INSTALLAZIONI MILITARI

Stato Maggiore Difesa

DOMANDE ?



STATO MAGGIORE DELLA DIFESA

VI Reparto - Sistemi C4I e Trasformazione

Stato Maggiore Difesa



Grazie per l'attenzione