

# **«La protezione delle Infrastrutture Critiche definizione e normative EN 50131-1 e CEI 79-3»**

# La direttiva CE 114/2008

23.12.2008

IT

Gazzetta ufficiale dell'Unione europea

L 345/75

## DIRETTIVA 2008/114/CE DEL CONSIGLIO

del 8 dicembre 2008

relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione

(Testo rilevante ai fini del SEE)

### Definizione infrastruttura critica:

“un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni”

# Definizione di ECI e Settori Coinvolti

## ECI European Critical Infrastructures

“Infrastruttura Critica Europea”: infrastruttura critica ubicata negli Stati membri dell'UE la cui perturbazione o distruzione avrebbe un significativo impatto su almeno **due Stati membri dell'UE**.

Settore	Sottosettore	
I. Energia	1. Elettricità	Infrastrutture e impianti per la produzione e la trasmissione di energia elettrica per la fornitura di elettricità
	2. Petrolio	Produzione, raffinazione, trattamento, stoccaggio e trasporto di petrolio attraverso oleodotti
	3. Gas	Produzione, raffinazione, trattamento, stoccaggio e trasporto di gas attraverso oleodotti Terminali GNL
II. Trasporti	4. Trasporto stradale 5. Trasporto ferroviario 6. Trasporto aereo 7. Vie di navigazione interna 8. Trasporto oceanico, trasporto marittimo a corto raggio e porti	

# Individuazione ECI Stati Membri

- è critica secondo la valutazione dei criteri settoriali (capacità, dimensioni e distanze)?
- è critica in base alla definizione?
- comporta un impatto trans-frontaliero?
- comporta danni economici, conseguenze per i cittadini?
- c'è il consenso dello Stato membro?

Se queste 5 condizioni sono soddisfatte allora: diventa una ECI

## Dotazione ECI Stati Membri

- Redigere il Piano operativo di Sicurezza dell'Operatore (PSO)
- Instituire il Security Liaison Officer (SLO) che agisce come punto di contatto fra il proprietario/l'operatore della ECI e l'autorità competente dello Stato membro

# Procedure redazione PSO

- l'individuazione degli elementi importanti;
- un'analisi dei rischi basata sulle minacce più gravi, sulla vulnerabilità di ogni elemento e sull'impatto potenziale;
- l'individuazione, la selezione e la "prioritarizzazione" di contromisure e procedure, con una distinzione fra:
  - a) misure permanenti di sicurezza: la **rilevazione**, la protezione e prevenzione, le misure organizzative, le misure di controllo e verifica, le comunicazioni, la crescita della consapevolezza e l'addestramento, la sicurezza dei sistemi informativi;
  - b) misure graduali di sicurezza, che possono essere attivate in funzione dei diversi livelli di rischio e di minaccia.

# **D.Lgs n. 61 dell'11 aprile 2011 l'Italia recepisce la direttiva 2008/114/CE**

- Linee guida per l'individuazione delle Infrastrutture Critiche
- Designazione Nucleo Interministeriale Situazione e Pianificazione (NISIP), integrato dai rappresentanti del:
  - a) Il Ministero dell'interno, il Ministero della Difesa, il Dipartimento della Protezione Civile della Presidenza del Consiglio dei Ministri ed il Ministero dello Sviluppo Economico, per il settore energia
  - b) Il Ministero delle Infrastrutture e dei Trasporti, per il settore trasporti
  - c) A livello locale la responsabilità della protezione delle singole installazioni costituenti le infrastrutture critiche è attribuita al Prefetto territorialmente competente

# CEI 79-3 o EN 50131-1?

- Non sono alternative
- CEI hanno validità solo nazionale e prendono in considerazione l'intero impianto (progettazione, collaudo e manutenzione periodica)
- EN sono norme di prodotto e applicazione

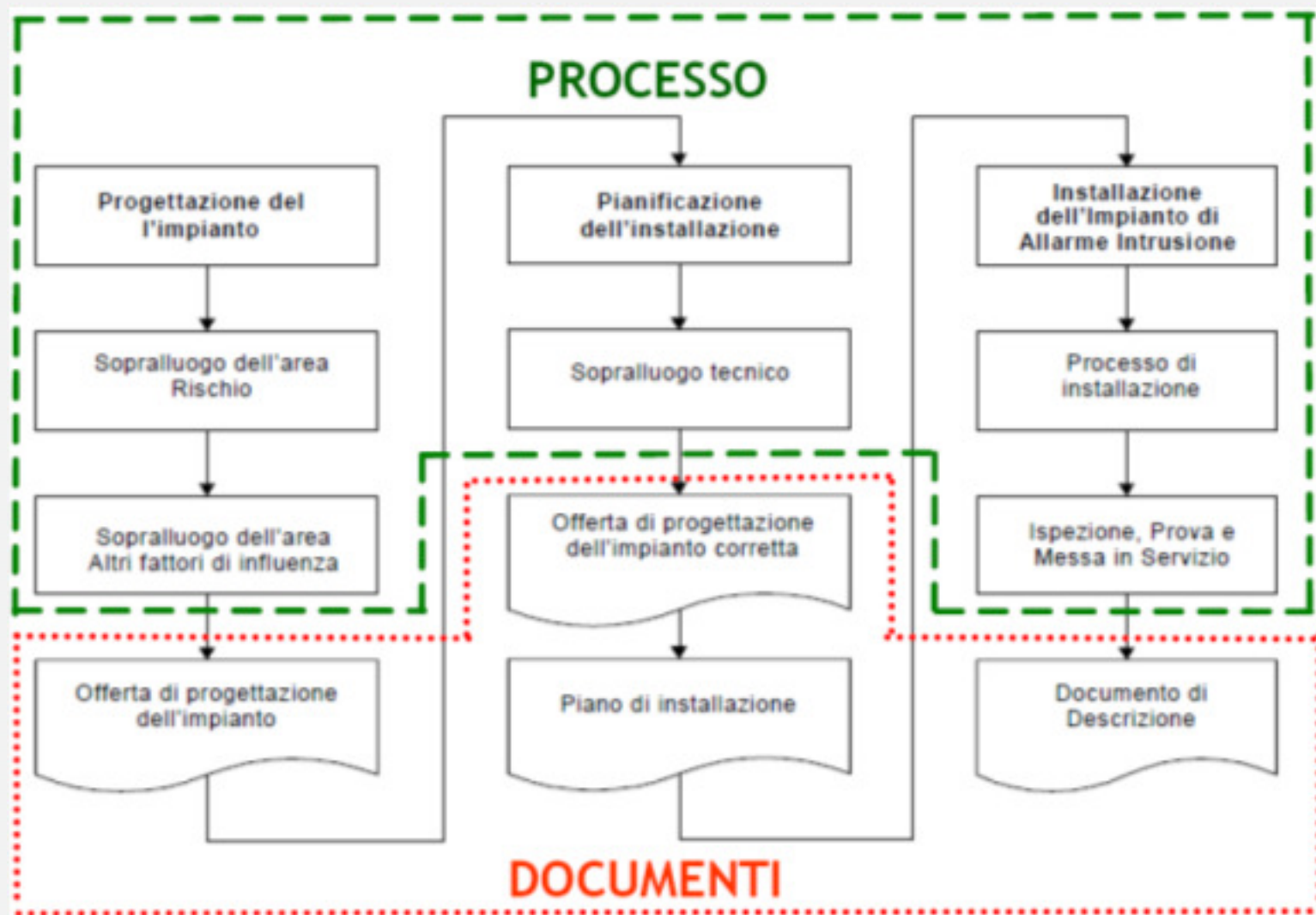
## CEI 79-3 definizione della sequenza

- individuazione dell'area da proteggere
- analisi del rischio e calcolo del livello di rischio
- progettazione dell'impianto
- verifica del livello di prestazione

## CEI 79-3 valutazione dell'area

- unità abitativa non isolata
- unità abitativa isolata
- insediamento industriale
- cassaforte, caveau

# CEI 79-3 processo realizzazione





## CEI 79-3 livelli di rischio

- Il livello 1 (basso), presuppone che rapinatori e intrusi abbiano una bassa conoscenza dei sistemi e che la strumentazione di cui possono disporre sia limitata ad attrezzi comunemente reperibili.
- Il livello 2 (rischio medio), quando si può presupporre che i malviventi possiedano, oltre ad alcuni strumenti portatili, anche una seppur parziale conoscenza degli apparecchi di difesa attiva.
- Il livello 3 (medio-alto), è rappresentato da potenziali intrusi in possesso di una certa conoscenza dei sistemi antintrusione, oltre a essere dotati di una gamma completa di strumenti e apparati elettronici in grado di violare un impianto.
- Il livello 4 (alto) prevede che entrino in azione autentici professionisti del settore, in possesso di capacità e risorse per pianificare in dettaglio una violazione, sfruttando anche strumenti particolarmente sofisticati.

## CEI 79-3 sottosistemi dispositivi

- rivelatori, hanno il compito di individuare il superamento delle barriere fisiche
- apparati essenziali e opzionali, gestione dei rilevatori (inseritori e centrale)
- dispositivi di allarme, sono quelli che segnalano, localmente e in remoto, una situazione di pericolo (sirene e combinatori)

## CEI 79-3 calcolo (matematico e tabulare) e verifica

- numero di barriere, funzionalmente concentriche e potenzialmente realizzabili, indipendentemente dalla struttura fisica del target da proteggere
- consistenza delle caratteristiche dei componenti installati
- modalità installative dell'impianto

Unità abitativa isolata Sottoinsieme Apparati essenziali ed opzionali				
Impianto	Livello di prestazione 1	Livello di prestazione 2	Livello di prestazione 3	Livello di prestazione 4
Grado di sicurezza delle apparecchiature utilizzate (CIE, ACE, PS e interconnessioni)	Grado di sicurezza 1	Grado di sicurezza 2	Grado di sicurezza 3	Grado di sicurezza 4
Per il sottoinsieme apparati essenziali ed opzionali il livello di prestazione corrisponde al grado di sicurezza delle apparecchiature utilizzate.				

# EN 50131-1 Grado di sicurezza

- Grado 1: Rischio basso: si prevede che gli intrusi o i rapinatori abbiano una conoscenza bassa del sistema di allarme intrusione rapina e dispongano di una limitata gamma di attrezzi facilmente reperibili.
- Grado 2: Rischio medio-basso: Si prevede che gli intrusi o i rapinatori abbiano una conoscenza limitata del sistema di allarme intrusione rapina e utilizzino una gamma generica di utensili e strumenti portatili (es., un multimetro).
- Grado 3: Rischio medio-alto: si prevede che gli intrusi o i rapinatori siano pratici del sistema di allarme intrusione rapina e dispongano di una gamma completa di strumenti e di apparati elettronici portatili.
- Grado 4: Rischio alto: da usare quando la sicurezza ha la precedenza su tutti gli altri fattori. Si prevede che gli intrusi o i rapinatori abbiano le capacità o le risorse per pianificare in dettaglio un'intrusione o una rapina e che dispongano di una gamma completa di attrezzature, compresi i mezzi di sostituzione dei componenti di un sistema di allarme intrusione rapina.

# EN 50131-1 Classe ambientale

- Classe ambientale I – Interno -- Influenze ambientali normalmente presenti in ambienti chiusi, quando la temperatura è ben controllata (es.: in una proprietà residenziale o commerciale). +5 e +40 , con un'umidità 75% senza condensazione.
- Classe ambientale II – Interno – Generale Influenze ambientali normalmente presenti in ambienti chiusi, quando la temperatura non è ben controllata (es.: nei corridoi, atri o scale, dove si può formare condensa sulle finestre e nelle aree non riscaldate adibite a deposito o nei magazzini nei quali il riscaldamento è intermittente).-10 C e +40, con un'umidità 75% e senza condensazione.
- Classe ambientale III – Esterno – Riparato o interno in condizioni estreme Influenze ambientali normalmente presenti all'aperto, quando i componenti non sono completamente esposti agli agenti atmosferici o all'interno, quando le condizioni ambientali sono estreme.-25 e +50, con un'umidità 75% senza condensazione. Per 30 giorni all'anno si prevede che l'umidità vari tra l'85% e il 95% senza condensazione.
- Classe ambientale IV – Esterno – Generale Influenze ambientali normalmente presenti all'aperto, quando i componenti sono completamente esposti alle intemperie. NOTA Si prevede che la temperatura vari tra -25 e +60, con un'umidità del 75% e senza condensazione. Per 30 giorni all'anno si prevede che l'umidità relativa vari tra l'85% e il 95% senza essere soggetta a condensazione.

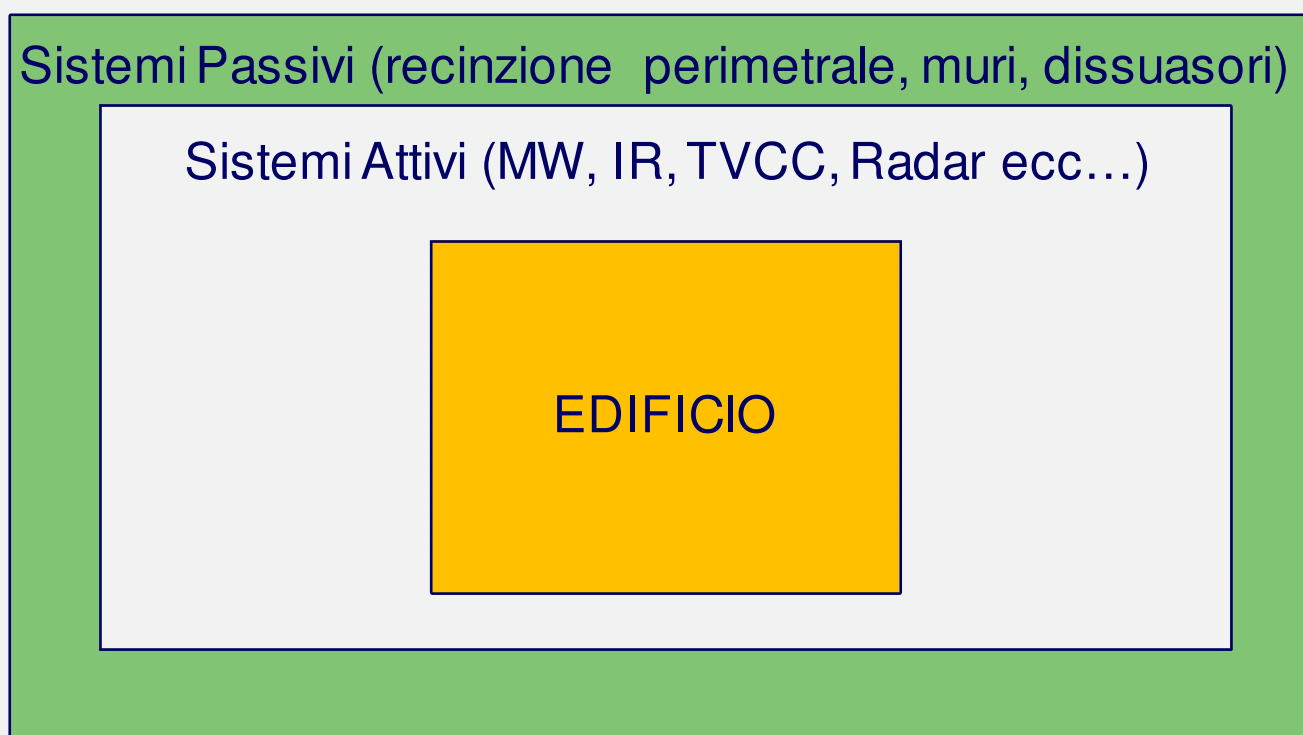
# EN 50131-1 Livelli di accesso

- “Livello di accesso 1”, include tutte le azioni e le indicazioni per “chiunque” senza che vi sia necessità di interazione
- «Livello di accesso 2» livello normale di operatività tramite richiesta di log-in compiere le azioni di consultazione o comando
- “Livello di accesso 3”, livello manutenzione o installazione e deve essere autorizzato ad operare da parte dell’utente (Livello 2)
- “Livello di accesso 4”, associata ad interventi effettuati dal “Costruttore” o su sua delega tipo aggiornamento del firmware o sostituzione di una scheda che può essere fatta fisicamente dall’installatore, che però in questo caso agisce come delegato del costruttore

# Sicurezza Fisica: componenti attivi e passivi

La sicurezza fisica è l'insieme di misure che prevengono o dissuadono gli attaccanti dall'accedere a un locale, a una risorsa o a informazioni e delle linee guida su come progettare strutture in grado di resistere ad atti ostili. Il fine della Sicurezza Fisica è quello di proteggere persone e beni coinvolti nel funzionamento del processo aziendale.

**Non vi è Sicurezza Fisica completa se non si combinano sistemi attivi e passivi**





# Il tempo raggiungimento obiettivo

$$Tobi \geq Tril + Tint + Trall$$

**Tobi**: tempo di raggiungimento obiettivo

**Tril**: tempo di rilevazione dovuto alla difesa elettronica

**Trall**: tempo di rallentamento dovuto alla difesa fisica

**Tint**: tempo di intervento per attuare le contromisure



# Prestazioni dei sensori utilizzati

## **Probabilità di Rilevazione PD = Probability of Detection**

Rappresenta la probabilità di rilevare un intruso all'interno della zona di rilevamento coperta dal sensore

Si esprime come la % di tentativi di intrusione rilevati rispetto al totale di quelli effettuati

## **Numero di Falsi Allarmi FAR = False Alarm Rate**

Rappresenta il numero degli allarmi non validi causati da fattori sconosciuti

Tipicamente si esprime in giorno/i-mese/i-anno/i

Normalmente è associato al rumore intrinseco del sensore stesso

## **Numero di Allarmi Impropri NAR = Nuisance Alarm Rate**

Rappresenta il numero degli allarmi non validi causati da fattori che non possono essere considerati minacce

Tipicamente si esprime in giorno/i-mese/i-anno/i

Normalmente tali allarmi sono causati da sorgenti esterne (condizioni climatiche, animali, vegetazione, ecc.)

## **Vulnerabilità al Sabotaggio VD = Vulnerability to Defeat**

Rappresenta la probabilità che il sensore possa essere sabotato (bypass, mismatch, masking ecc.)

Specifica di ciascuna tecnologia utilizzata

**MTBF (Mean Time Between Failures)** tempo medio tra il verificarsi di un guasto ed il successivo (deve essere di diversi anni)

**MTTR (Mean Time To Repair)** tempo medio di riparazione (deve essere il più breve possibile dell'ordine di un'ora o meno)



# TCO, ROI e la responsabilità morale della progettazione



Qualunque soluzione o tecnologia venga scelta per la realizzazione del sistema di sicurezza, presenta vantaggi e svantaggi, sia di natura tecnica che economica. Per questo motivo nella valutazione devono essere pesati anche due fattori di tipo economico:

**TCO** Total Cost of Ownership che definisce il costo totale (acquisto, installazione, gestione, manutenzione/aggiornamento e il suo smaltimento)

**ROI** Return on Investment che definisce il ritorno sull'investimento (dato dal rapporto tra risultato operativo e capitale investito)

Spesso la gestione e la manutenzione (che influisce sul risultato operativo) vengono trascurati nella fase di progettazione e così in breve tempo l'impianto viene messo fuori servizio e il ROI inevitabilmente si abbatte.

**Il sistema di protezione progettato dovrebbe essere: efficace (in qualunque condizione meteo), efficiente (con pochi guasti) ed avere costi di manutenzione limitati**

# *L'azienda CIAS*

Moving to IP, heading to future!

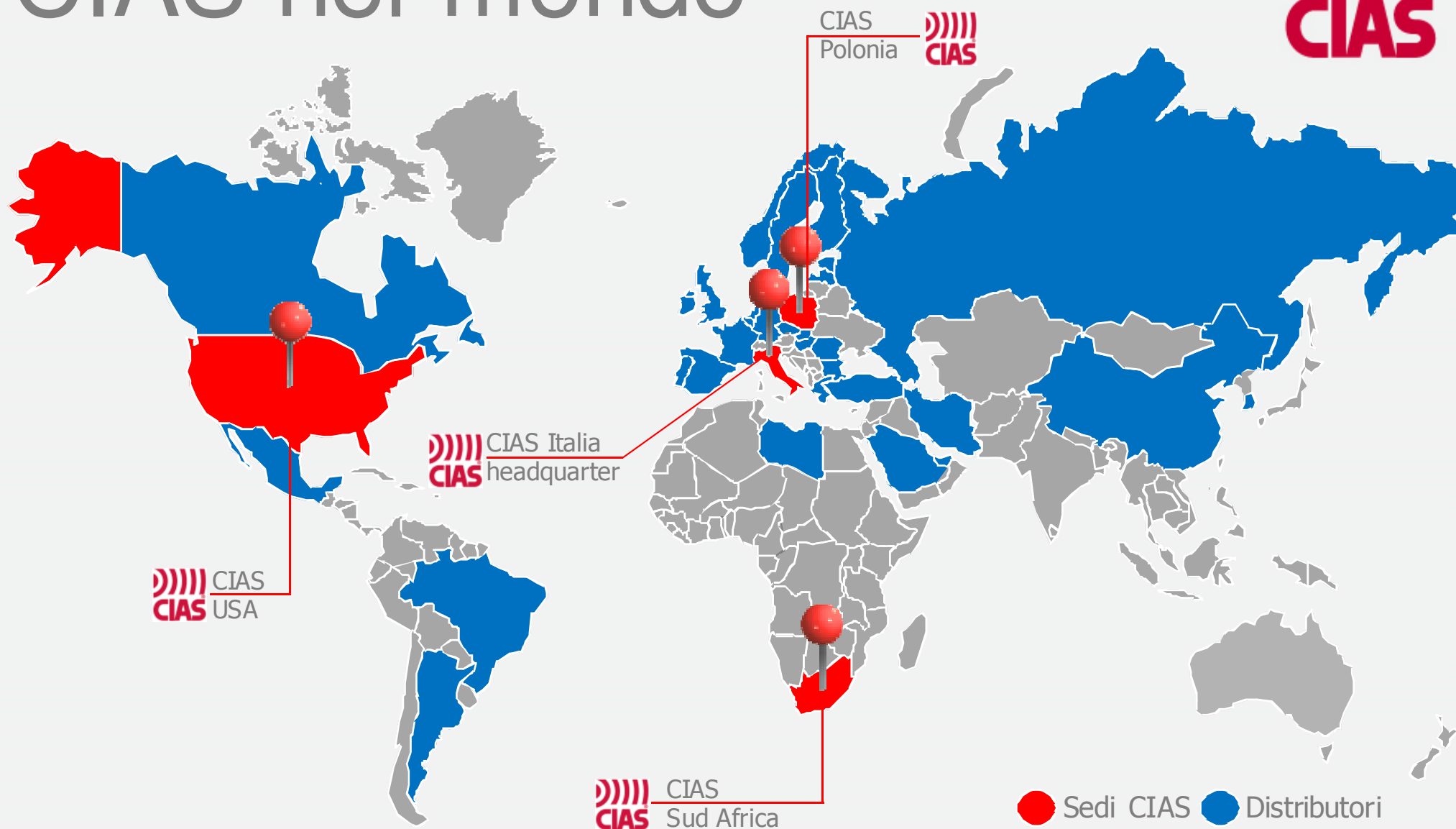
CIAS, azienda interamente italiana, nata a Milano, opera nel mercato della sicurezza dal 1974 nel campo della ricerca, dello sviluppo e della produzione di apparati e sistemi. Occupa 40 persone con un fatturato di 5,5 M€

CIAS è conosciuta a livello nazionale ed internazionale per le sue barriere per esterno a microonde, infrarosso, doppia e tripla tecnologia e sistemi antintrusione.



# CIAS nel mondo

SINCE 1974  
**CIAS**







**MILITARE**

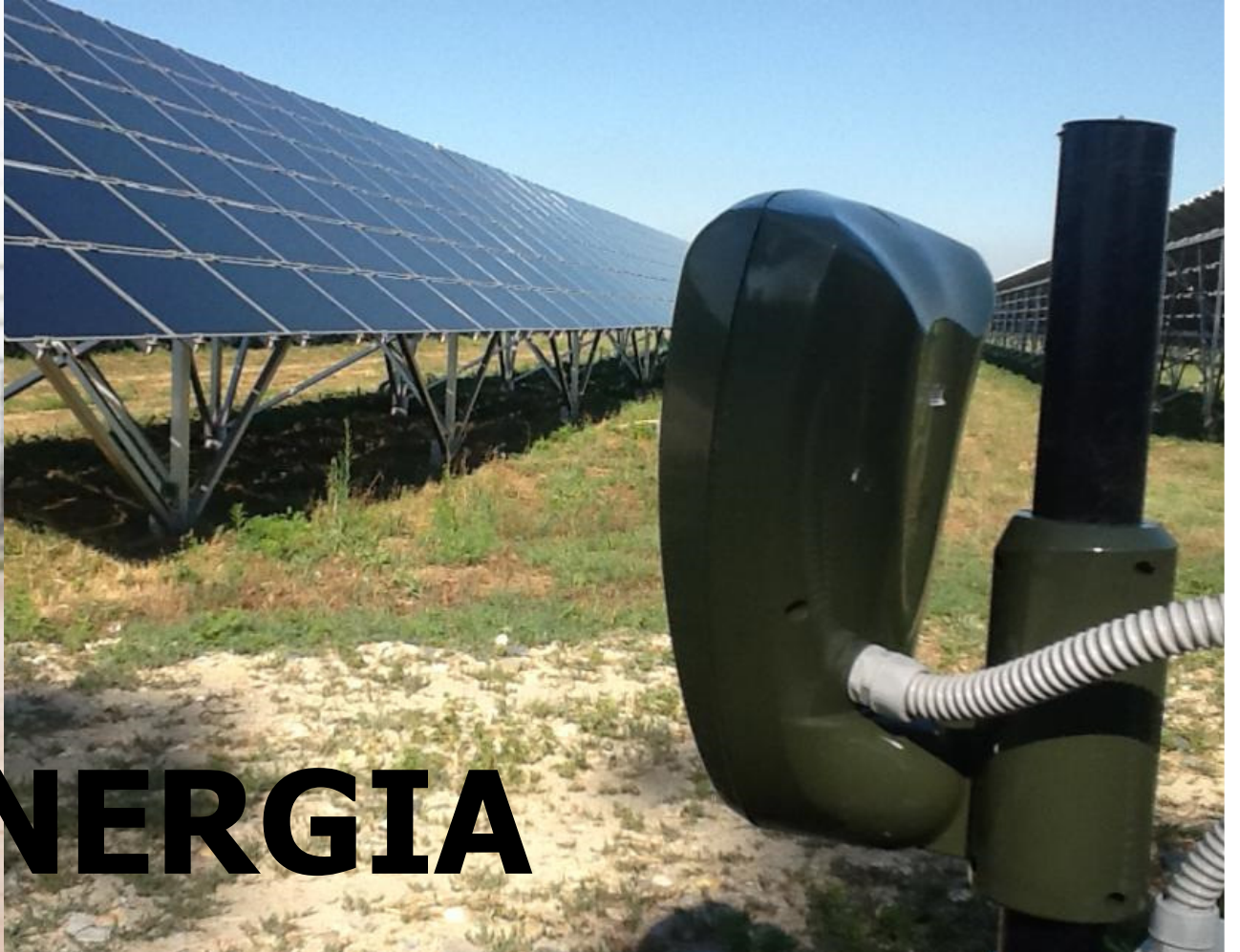






# AEROPORTI





**ENERGIA**







# OIL & GAS

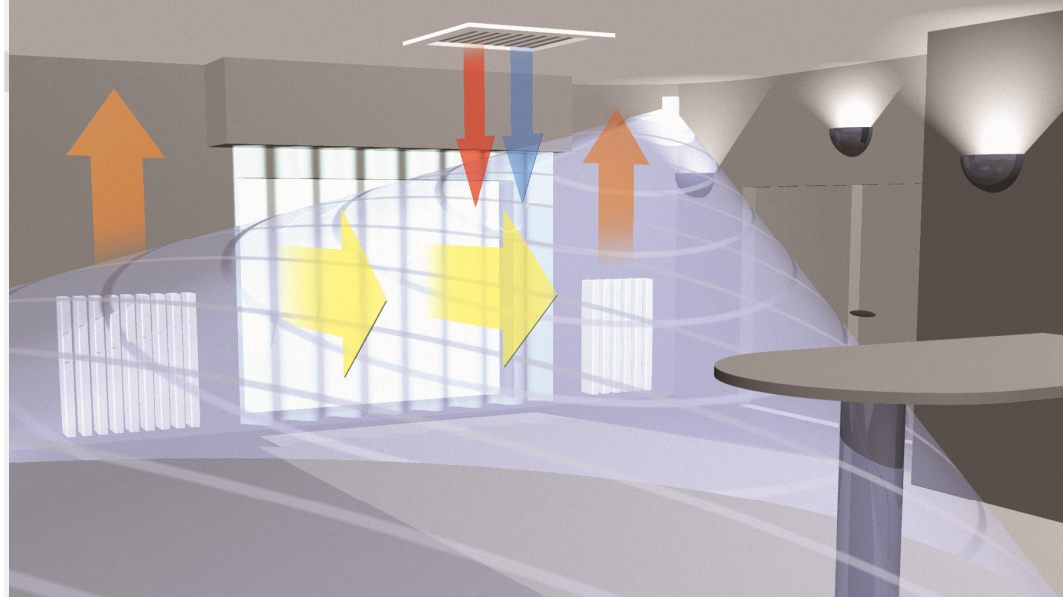






# TRASPORTI & LOGISTICA





# RESIDENZIALE





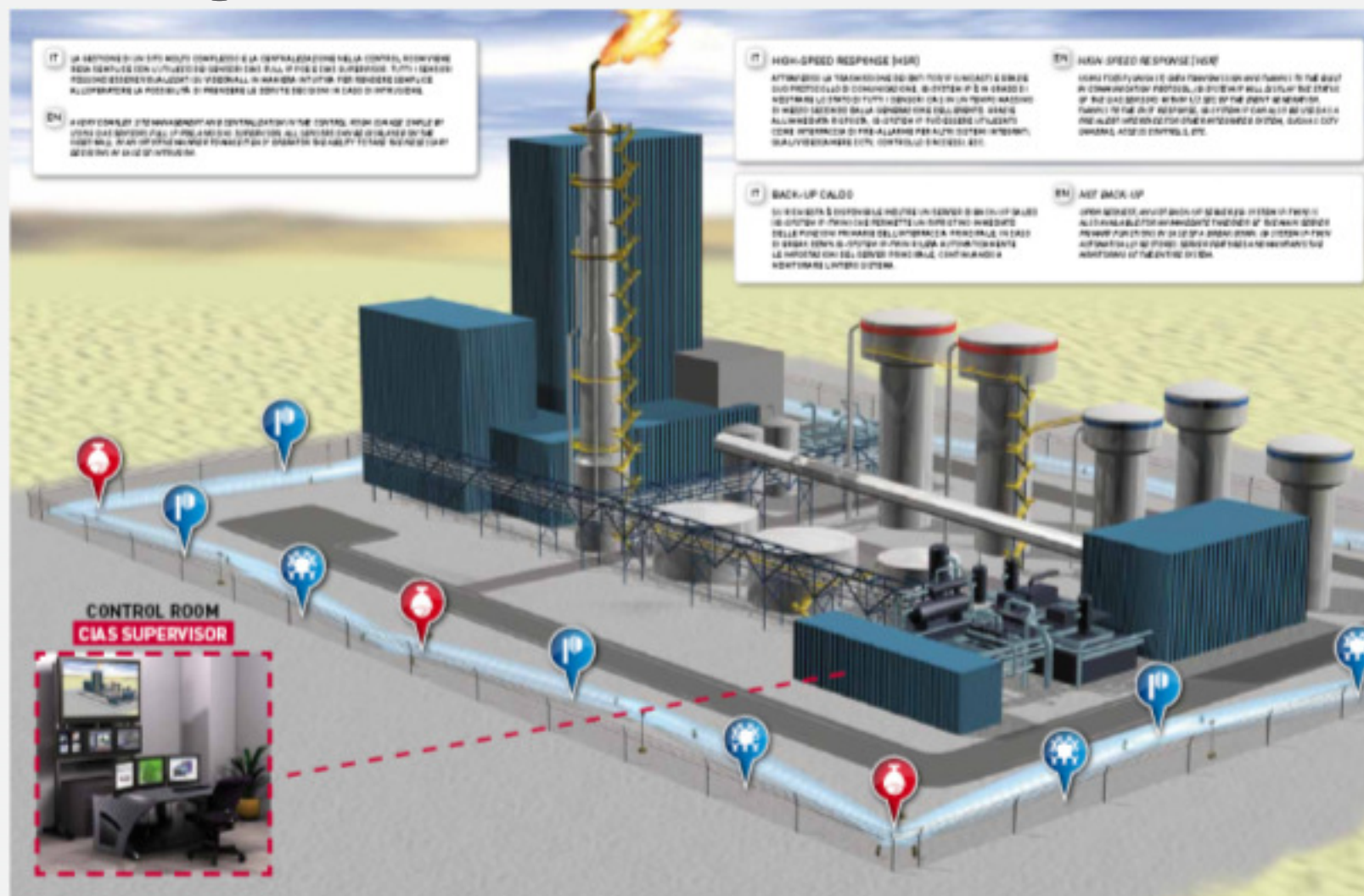


**COMMERCIALE**



**EXTREME SECURITY**

# L'integrazione TVCC e IDS



# IP DOORWAY

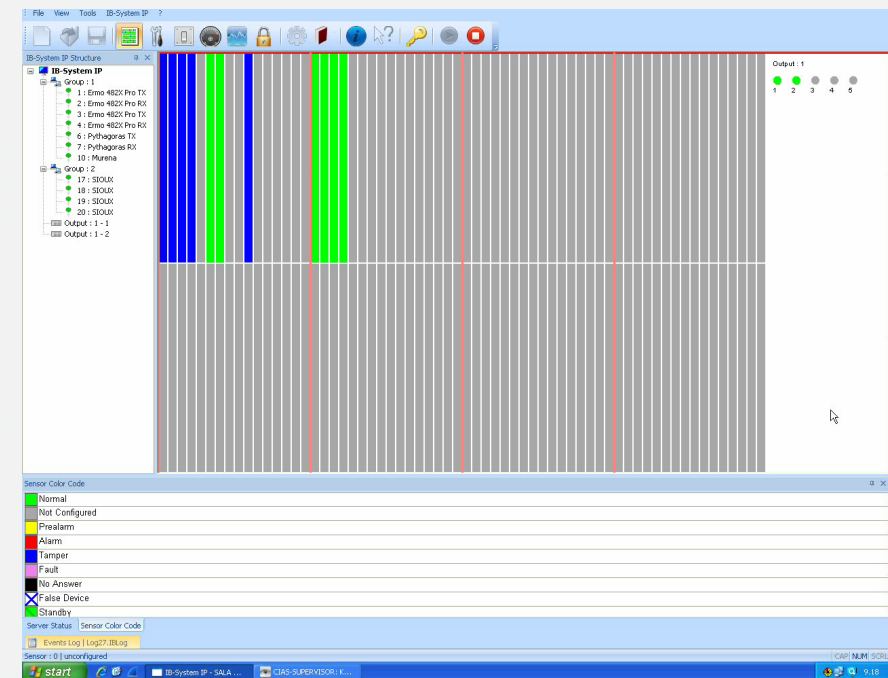
- Convertitore RS485 a IP
- Adatta a tutti i prodotti digitali CIAS
- PoE Standard 802.3af
- PoE con alimentazione esterna
- Collegabile fino a 1,2Km di distanza su BUS485
- Web server integrato
- Comunicazione crittografata AES128
- Permette di trasferire la Firma dei dispositivi



# IB-SYSTEM IP



- Software di supervisione di perimetri fino a 160Km
- Unico sistema di supervisione fino a 1280 dispositivi
- Bassa occupazione di banda 20Kbit per dispositivo
- Alta velocità di polling 500ms e auto configurante
- Indicazione per: allarme tamper guasto e non risposta
- Protocollo crittografato proprietario e firmato
- 100% made in Italy by CIAS





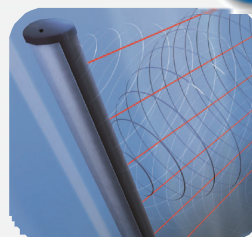
# CIAS - SUPERVISOR



**ERM0482XPRO**



**SIoux 3.0**



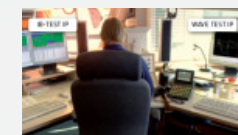
**PYTHAGORAS3TECH**



**MURENAPLUS**



SINCE 1974  
**CIAS**



**CONTROL ROOM**



**NETWORK**



**SITE**

# CIAS - SUPERVISOR

CIAS-SUPERVISOR: Keeping an eye on everything - WINDOW 1 - [Layout]

File Edit View Settings Layout Help

Device List

- All Devices
  - Server Dubai
    - Video Channels
      - Samsung 7080R
      - Bullet Full HD
      - Ptz FullHD
    - I/O Devices
      - CIAS - 192.168.15.3
    - Security
      - CIAS IB-System IP
    - Maps
      - Italy
      - USA
      - Various
    - Intersec Dubai
      - Booth ARTECC

Layout

Live Event

Server Name	Device	Event Description	Event Time	St...	Username	Acknowledgement Time	File Type
Server Dubai	Murena	Alarm	04:31:06 PM 19...	Open	System	04:31:06 PM 19 Jan 2014	
Server Dubai	Ermo482...	Alarm	04:30:28 PM 19...	Open	System	04:30:28 PM 19 Jan 2014	
Server Dubai	Bullet Fu...	Input Triggered Even...	04:30:16 PM 19...	Open	System	04:30:16 PM 19 Jan 2014	Video
Server Dubai	Ermo482...	Pre-Alarm	04:30:16 PM 19...	Open	System	04:30:17 PM 19 Jan 2014	

PTZ Control Device Properties

Ready



# “L’integrazione di CIAS”

Grazie alla concessione del proprio SDK, CIAS offre ai propri partner la possibilità di decodificare il suo protocollo di comunicazione così da permettere una integrazione completa, sia a livello hardware che software. In questo modo si ha la possibilità di sviluppare un’unica piattaforma in grado di gestire molteplici sistemi integrati.

Oggi CIAS è integrata con:

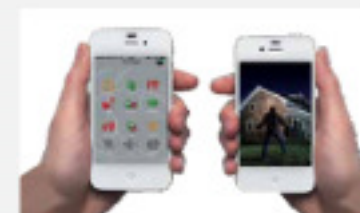


# QUASAR

SINCE 1974  
**CIAS**



- Centrale 8/40 oppure 8/80 zone e 3 uscite relè
- Tastiere touch 3.5"
- 3 bus RS485 da 1,2Km con potenza di 500mA
- Gestione mobile Android e Apple anche offline
- 16 aree, 16 gruppi, 40 operatori, 32 uscite, 4 tastiere
- Espansione wireless su bus
- Espansione GSM e PSTN Contact ID su bus
- Integrata con Cias Supervisor Milestone e Genetec
- Dialogo digitale con tutte le periferiche digitali IP e RS485
- Videoverifica fino a 12 telecamere IP (con 3 fotogrammi in email)
- Telegestione e mappe 3D live



## SENSORI DIGITALI

### BLACK-FEET CABLE



SISTEMA A CAVO  
MAGNETOFONICO PER  
LA PROTEZIONE DI MURI  
E PREDIZIONE RISCHI O  
FLESSIBILI

### MURENA 12M - 24M



SENSORE  
MONOSTATO  
DUAL DOPPLER  
DIGITALE CON  
ANALISI FUZZY  
LOGIC

### MANTA 60M - 80M



BARRIERA A  
MICROONDE  
DIGITALE CON  
ANALISI FUZZY  
LOGIC

## GRUPPO INGRESSI

### ALFA



SENSORE  
DOPPLER DA  
INTERNO

### PERSEUS 16M - 18M



FAMIGLIA DI  
SENSORI A DOPPLER  
TECNOLOGIA DA  
INTERNO

### AQUARBUS XL 8M - 12M



FAMIGLIA  
SENSORI  
& DOPPLER  
TECNOLOGIA DA  
ESTERNO

### SATELLITE 8IN



MODULO DI  
ESPAZIONE  
& 8 INGRESSI

### SATELLITE 1/0



MODULO DI  
ESPAZIONE  
CON 1 INPUT E 1  
OUTPUT

### DARWIN



BARRIERA IR E  
OT PER PORTE E  
FINESTRE

## FAMIGLIA COSMOS



COSMOS PSTN BUS  
MODULO TELEFONICO  
ABILITATO PER COLLEGAMENTO  
SUL LINGUA PSTN CON  
PROTOCOLLO CONTACT ID  
E INTERFACCIA VOCE



COSMOS-GSM BUS  
CONNESSIONE  
TELEFONICA GSM  
COMPENSAZIONE DI MENU  
VOCALE PER LA  
PROGRAMMAZIONE

## ALTRO

## FAMIGLIA ECHO

## GRUPPO USCITE

### DISPOSITIVI



ECHO XL  
SIRENA PER  
ESTERNO



ECHO X5  
SIRENA PER INTERNO  
A BASSO CONSUMO



SATELLITE 40UT  
MODULO DI  
ESPAZIONE &  
RELE

## INTEGRAZIONE TVCC



**HIKVISION**

**D-Link**  
**AXIS**  
COMMUNICATIONS



## QUASAR

BUS 485

IP

BUS 485

IP

BUS 485

IP

BUS 485

IP

BUS 485  
IP  
RELE

IP



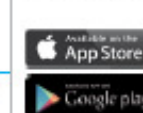
INTERNET  
comunicazione  
crittografata



INTERNET  
comunicazione  
crittografata

## APPLICAZIONI MOBILE

### QUASAR MOBILE (APP)



## INTERFACCIA UTENTE



LA TASTIERA  
TOUCH-SCREEN 3.5"  
& COLORI DI TIPO REGISTRATO

BUS 485



LETTORE DI PROSSIMITA'  
CON SOSTO DI 3 AREE DI RILEVAMENTO  
AZIONABILE CON CARO  
O PORTA CHIAVI TAG



IP

## FAMIGLIA VIA RADIO TAURUS

### TAURUS-IR



SENSORE  
IR RADIO  
SUPERVISIONATO  
2 CANALI

### TAURUS-CURTAIN



SENSORE IR VIA  
RADIO A TENDA  
PER FINESTRE  
& PORTE  
FINESTRE

### TAURUS-TAP



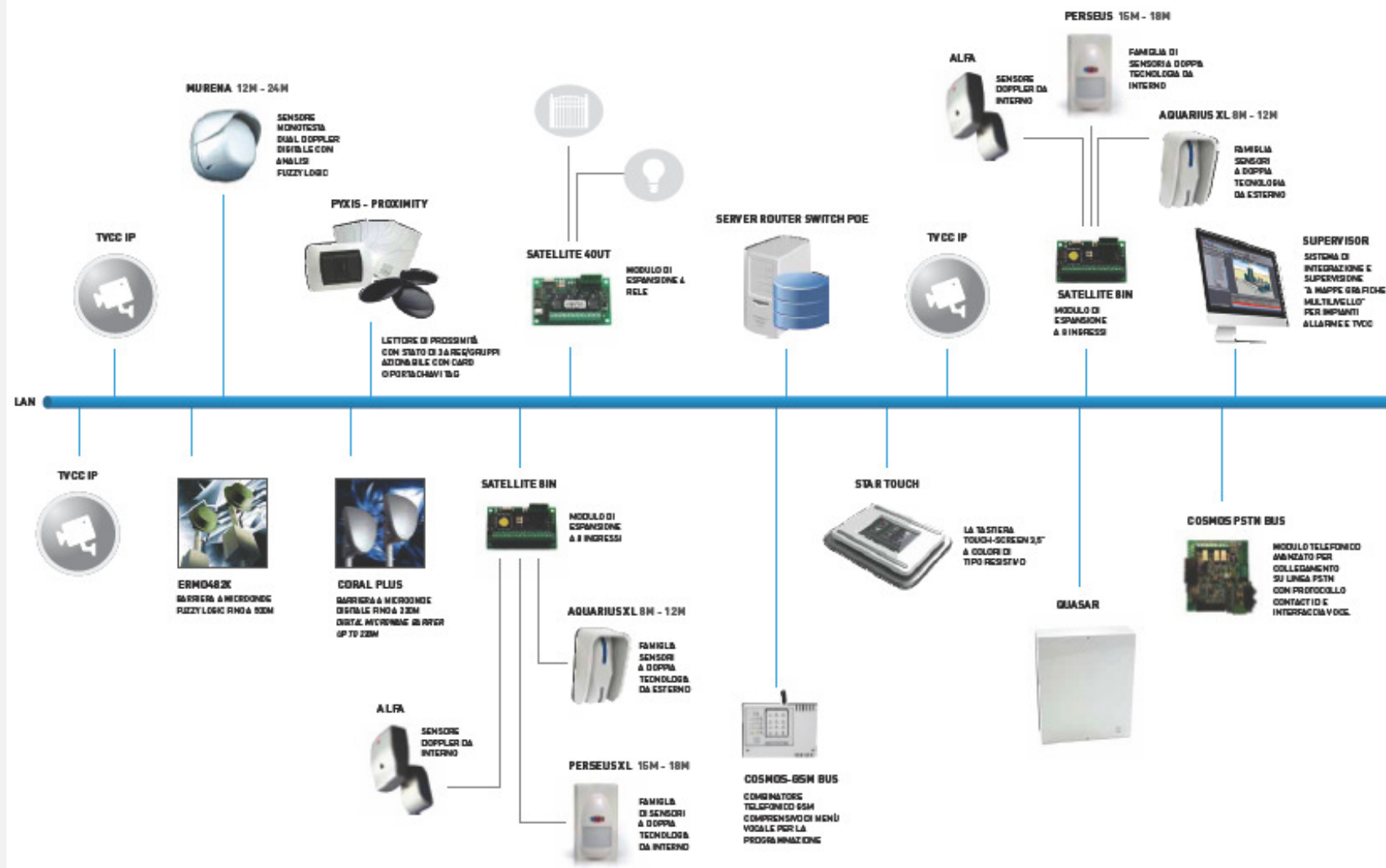
SENSORE VIA  
RADIO ANTI-  
SOLLEVAMENTO  
TAPPARELLA

### TAURUS-CONTACT +



CONTATTO  
MAGNETICO  
VIA RADIO  
2 CANALI E  
RILEVATO DI  
IMPATTI

# QUASAR FULL IP

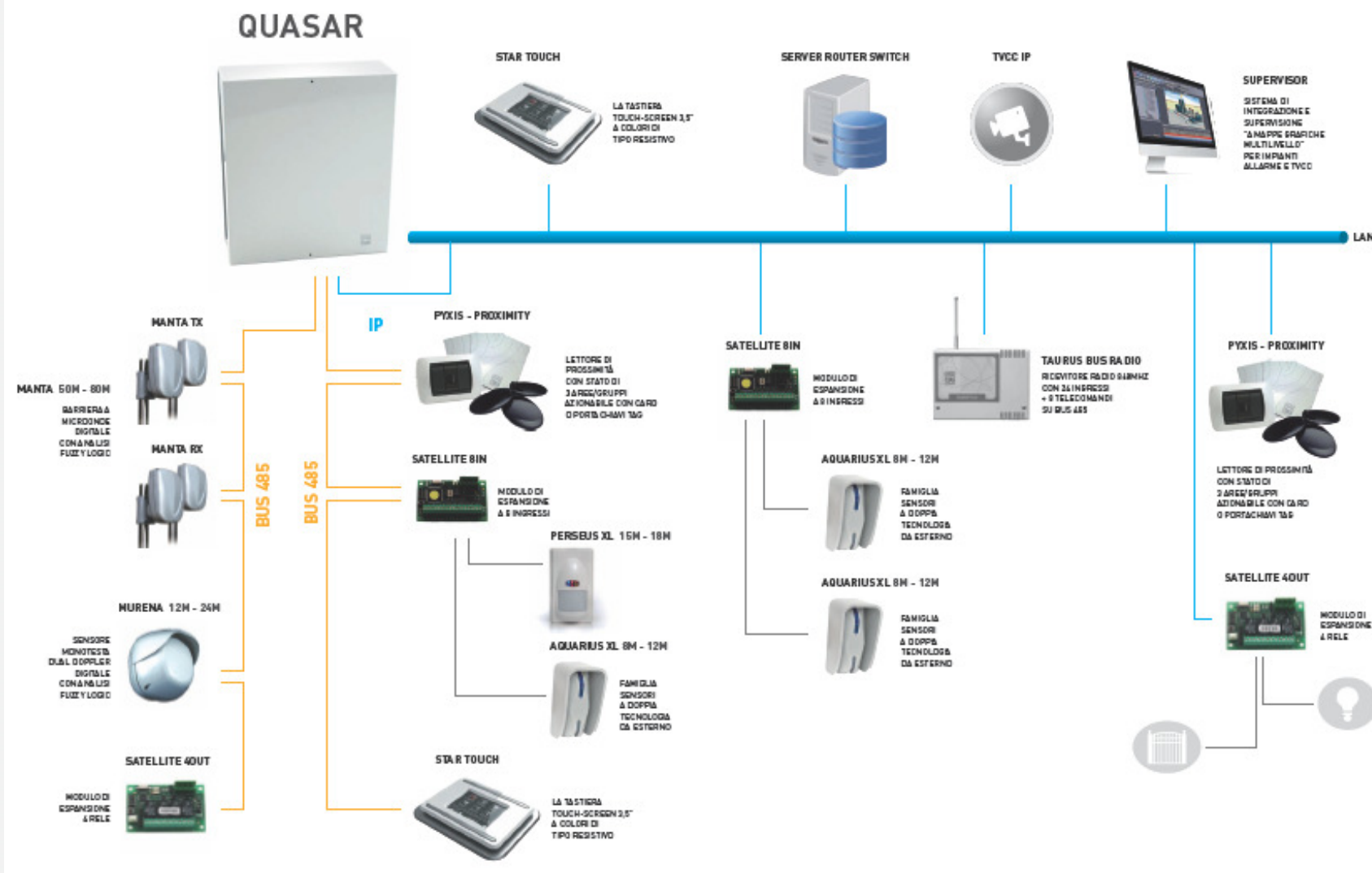




# QUASAR HYBRID



SINCE 1974  
**CIAS**



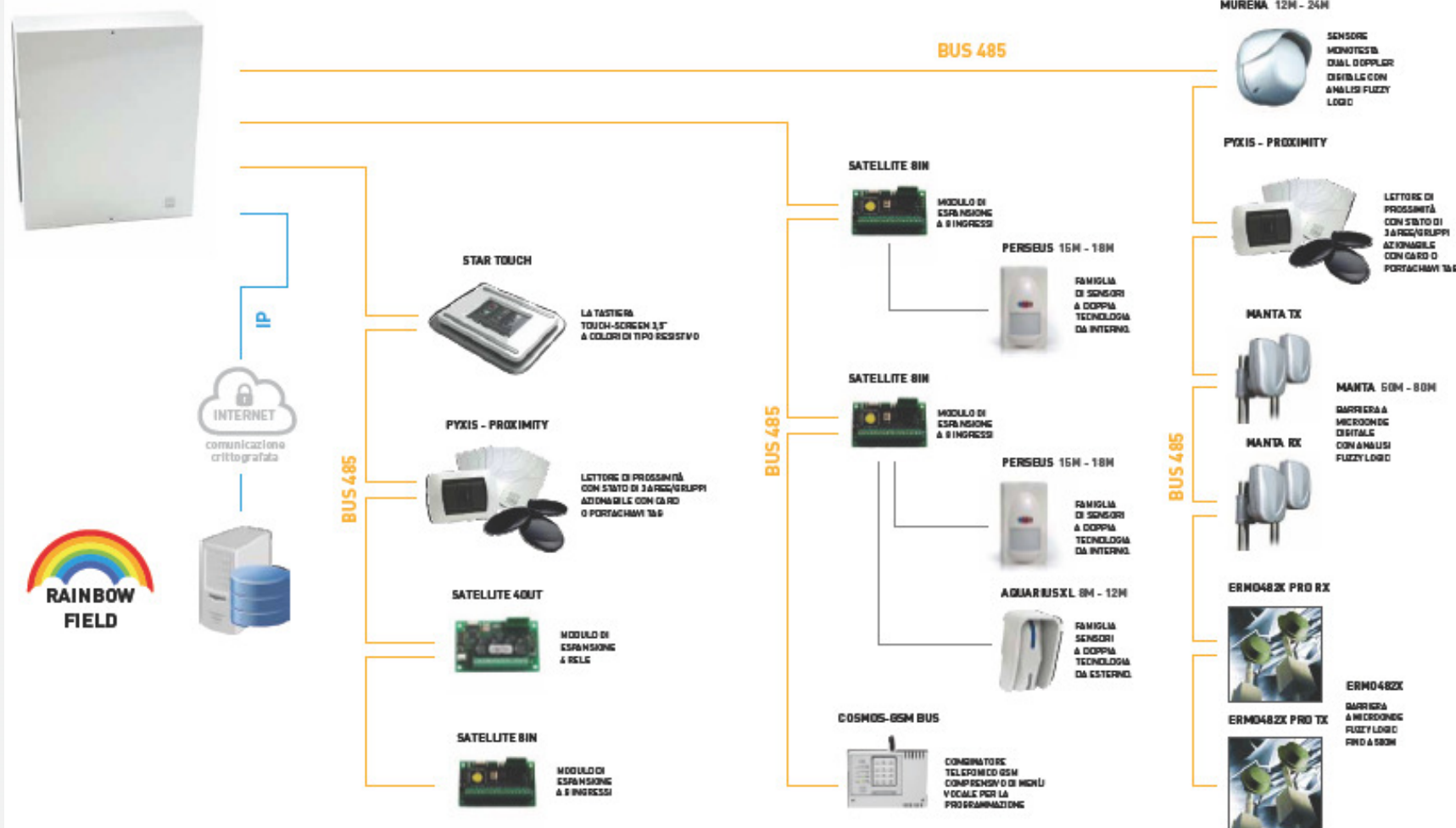
EXTREME SECURITY

WWW.CIAS.IT

# QUASAR BUS



## QUASAR



***Grazie dell'attenzione!***

***visitaci su:***

***[www.cias.it](http://www.cias.it)***

