SCADA Security

1 Giugno 2007, Dipartimento di Informatica

La sicurezza delle infrastrutture critiche

Alessio L.R. Pennasilico
mayhem@alba.st

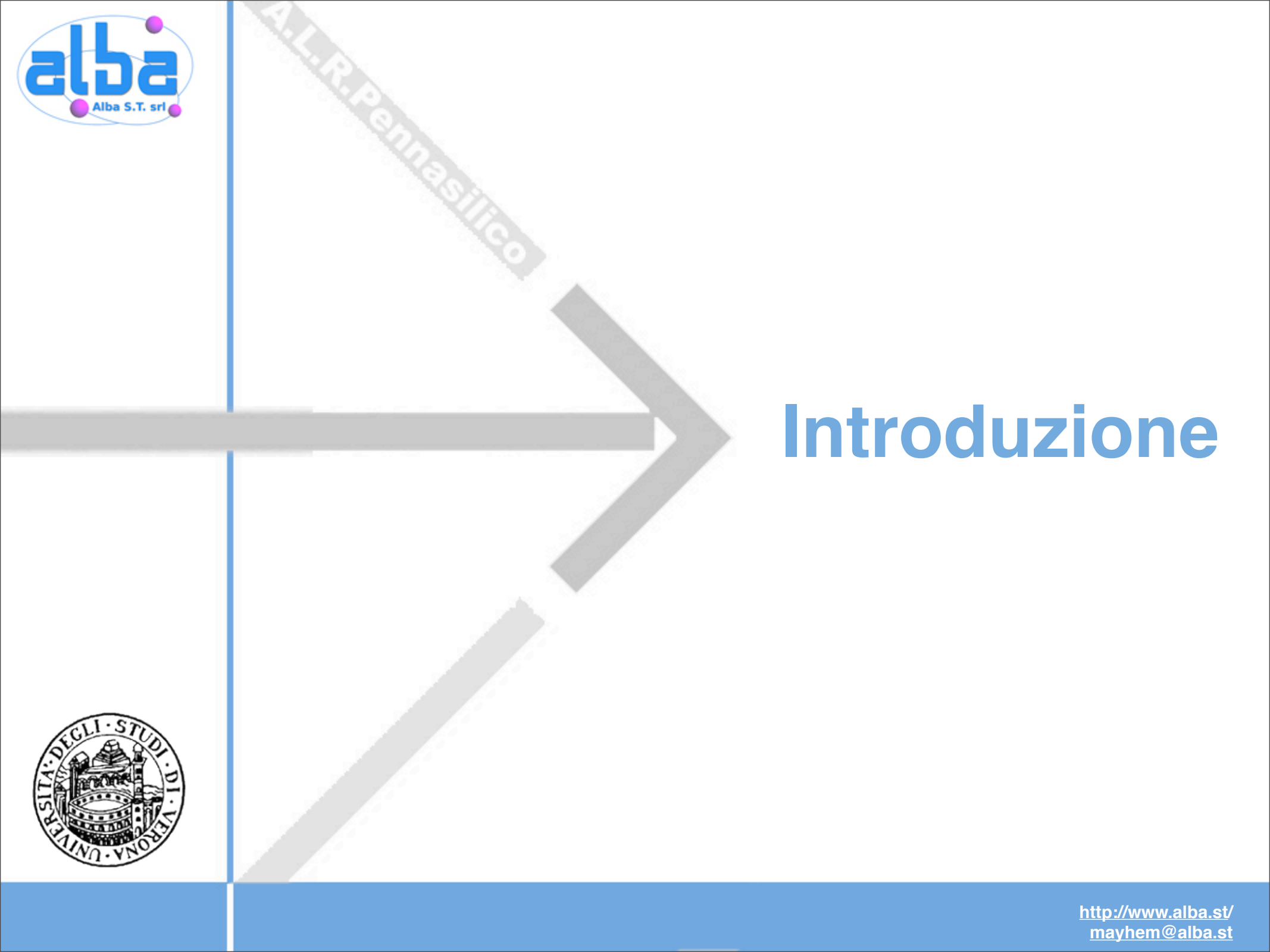
$ whois mayhem

Security Evangelist @

Member / Board of Directors:

AIP, AIPSI, CLUSIT, HPP, ILS, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer/OpenGeeks, Recursiva.org, Sikurezza.org, Spippolatori, VoIPSA.

http://www.alba.st/
mayhem@alba.st



Introduzione

SCADA

è l'acronimo di

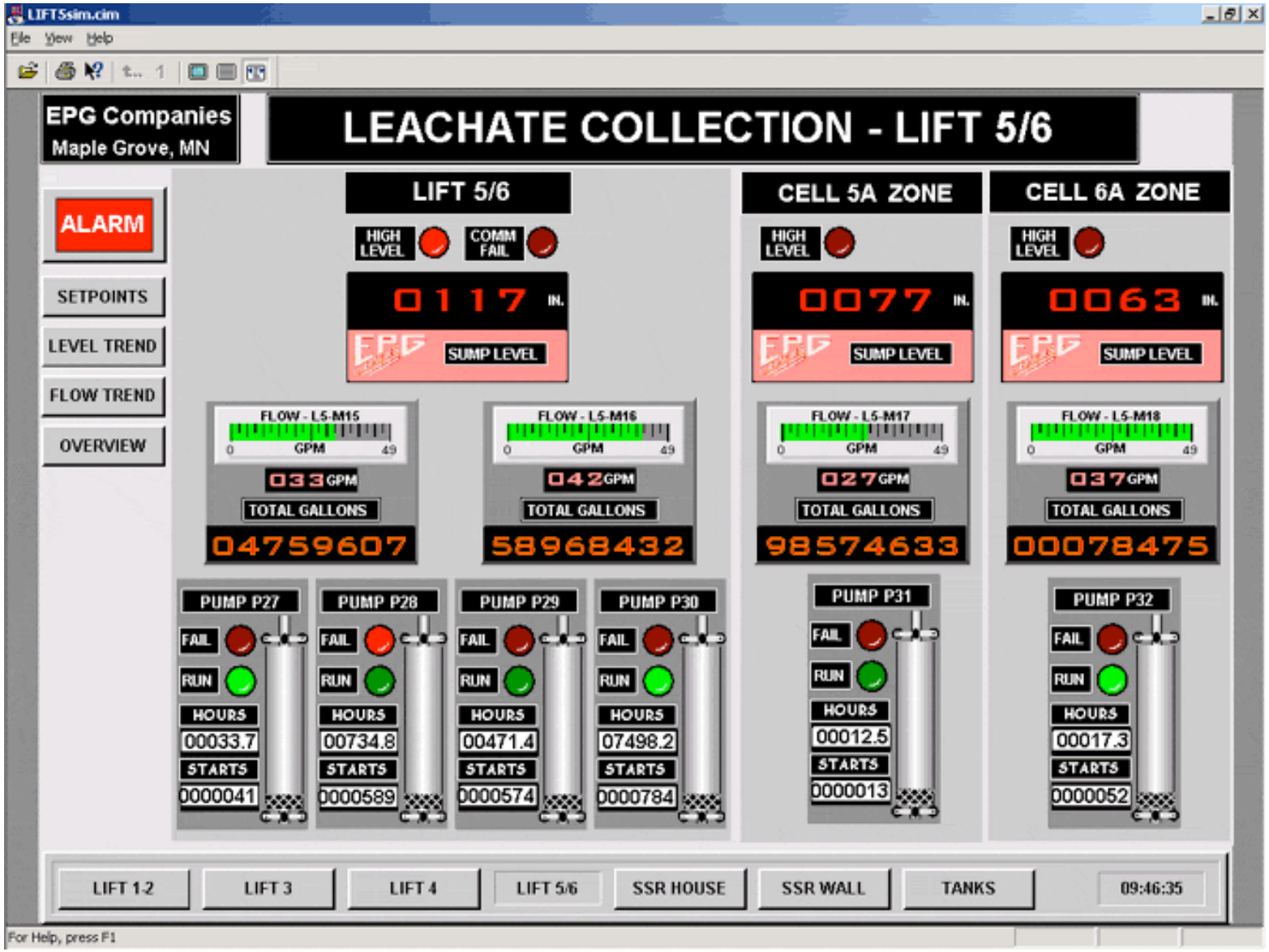
"Supervisory Control

And Data Acquisition".

Si riferisce ad una struttura distribuita di controllo e gestione.

http://www.alba.st/
mayhem@alba.st

Esempio #1



http://www.nbtinc.com/Software/telemetry-software.html

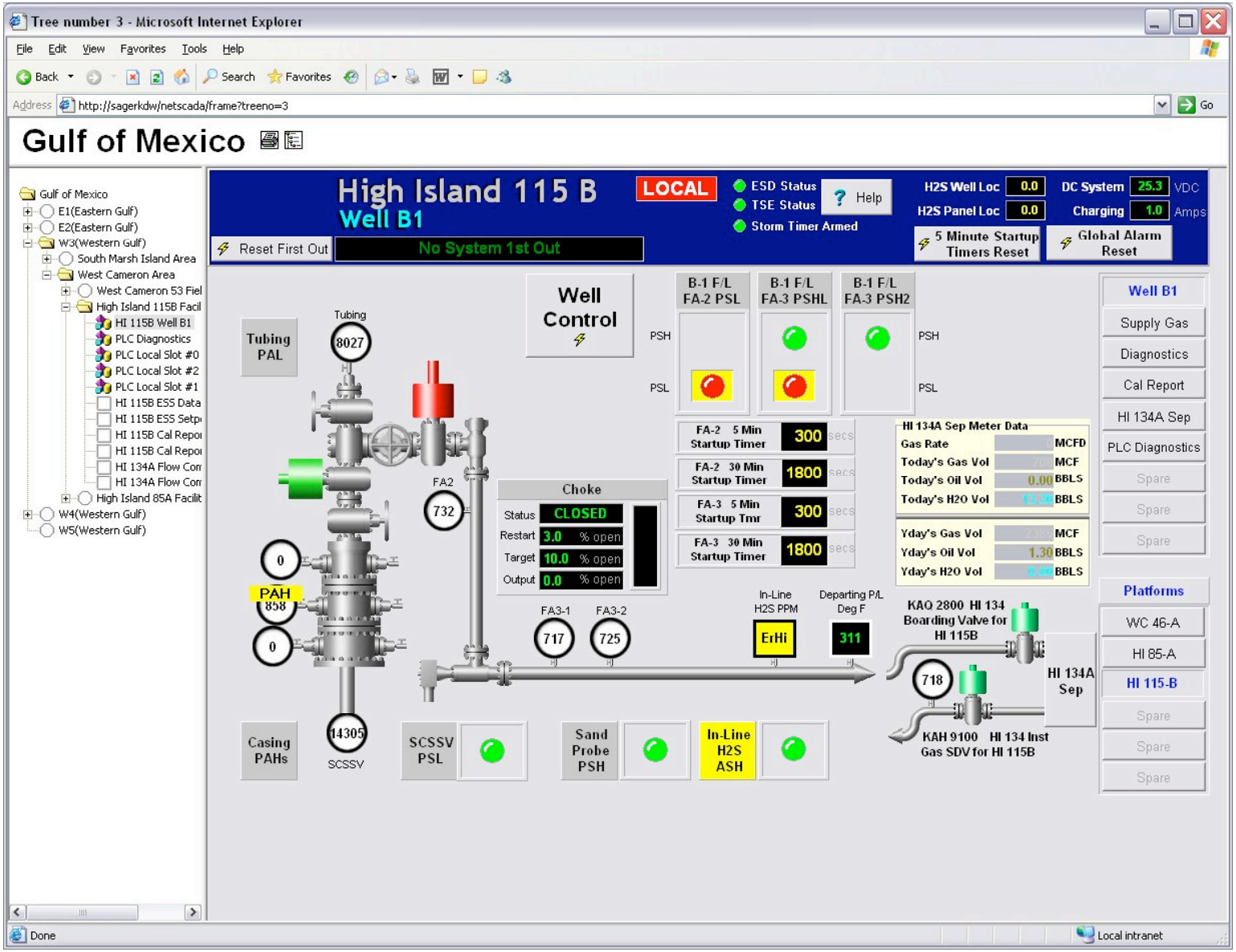
http://www.alba.st/
mayhem@alba.st

Le macchine a controllo numerico sono una realtà da anni.

Alcune di esse sono responsabili di risorse critiche per la popolazione.

http://www.alba.st/
mayhem@alba.st

Esempio #2



http://www.scadalink.com/netscada%20EI-155%20Web%20image.jpg

http://www.alba.st/
mayhem@alba.st

Infrastrutture critiche

I sistemi SCADA gestiscono infatti

centrali elettriche

fornitura di gas o acqua

comunicazioni

trasporti

http://www.alba.st/
mayhem@alba.st

Infrastruttura SCADA

Human Machine Interface (HMI)

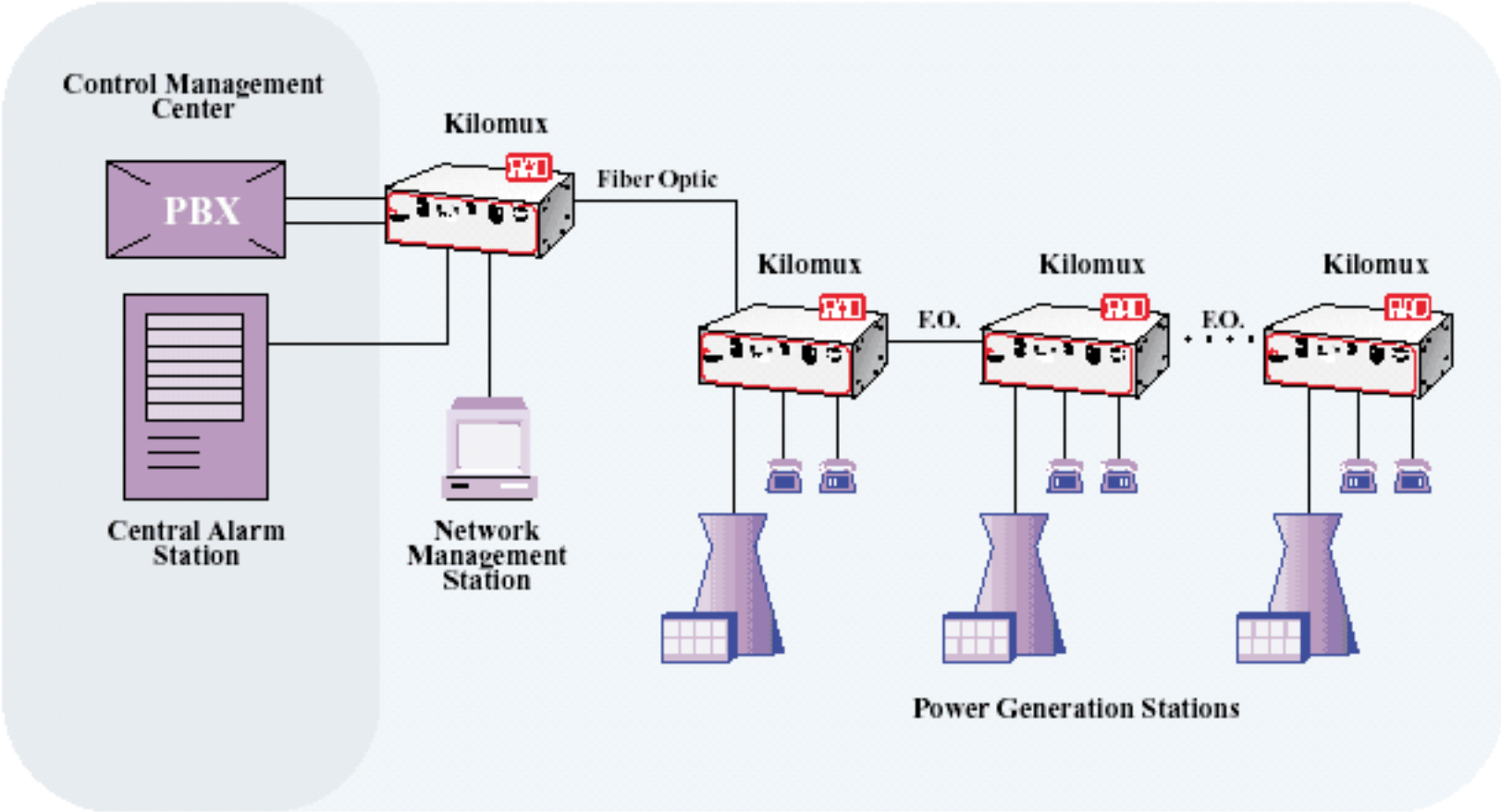
Remote Terminal Unit (RTU)

Programmable Logic Controller (PLC)

Communication infrastructure

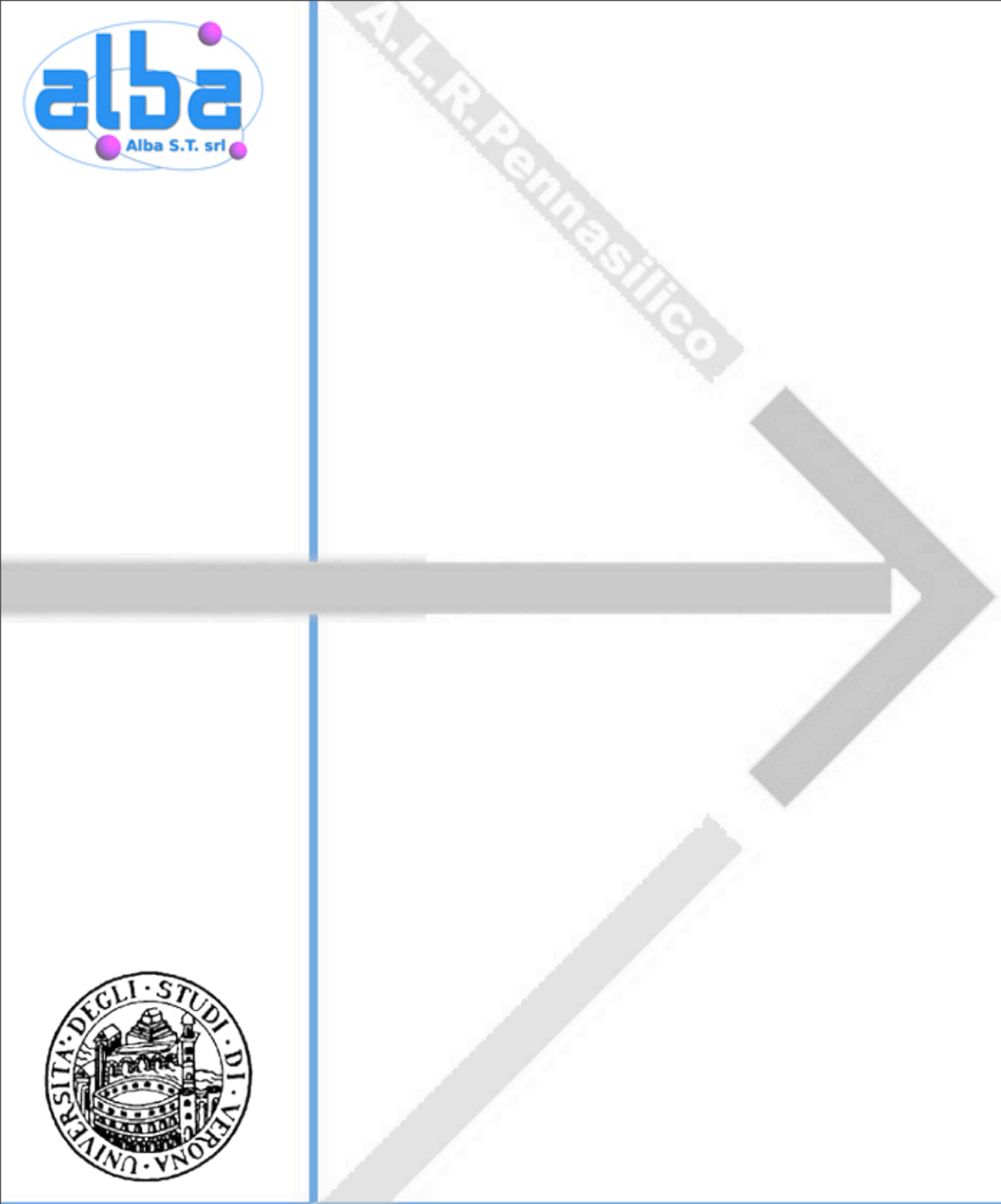
http://www.alba.st/
mayhem@alba.st

Enel



http://www.radfiber.com/Article/0,6583,27608,00.html

http://www.alba.st/
mayhem@alba.st



Requisiti

Requisiti

Performance

(sistemi real-time)

http://www.alba.st/
mayhem@alba.st

Requisiti

Disponibilità

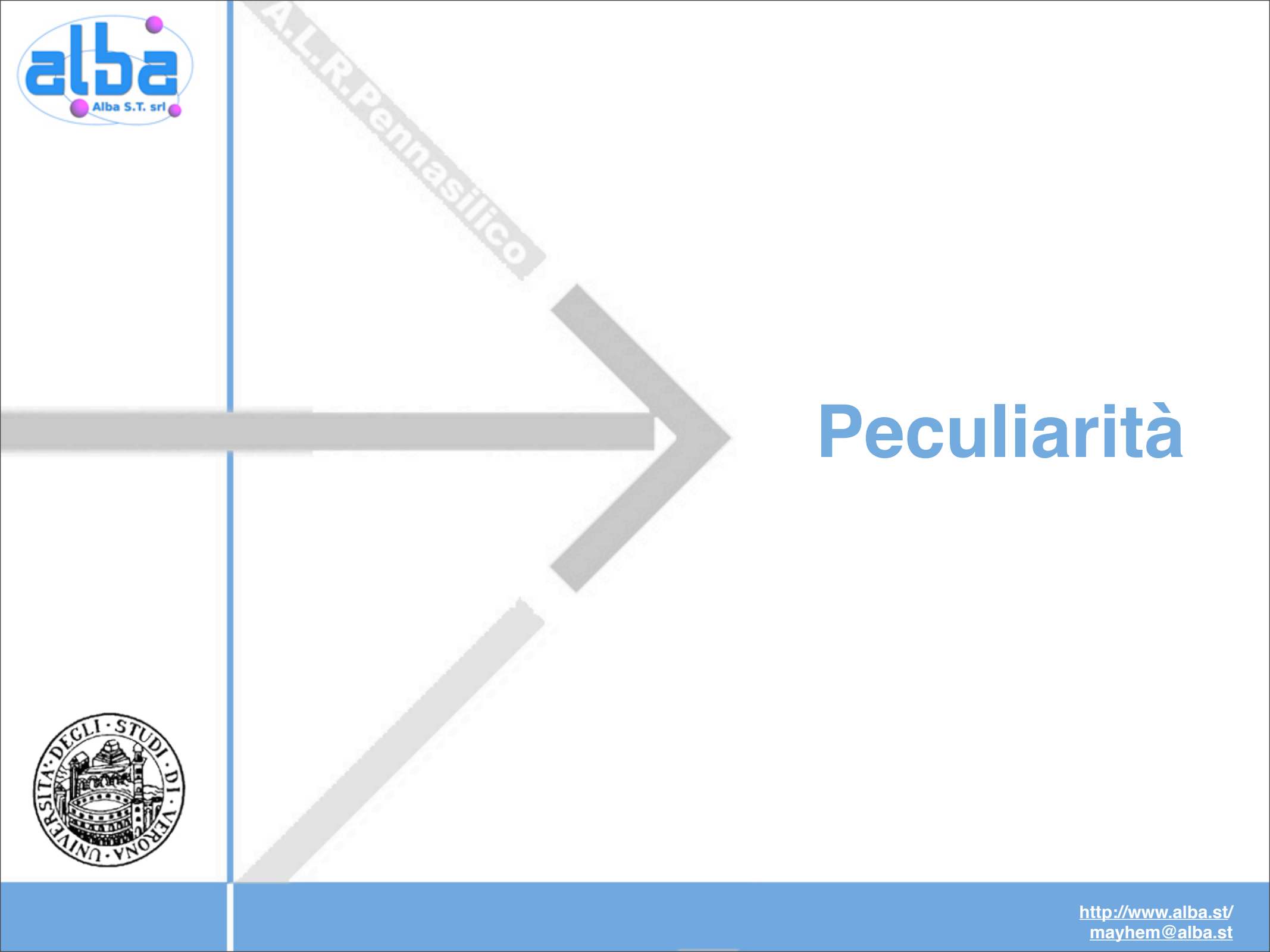
Requisiti

Nessun Imprevisto

Requisiti

Lungo ciclo di vita

http://www.alba.st/
mayhem@alba.st



Peculiarità

Protocolli

MODBUS/TCP

EtherNet/IP

DNP3

OPC

http://www.alba.st/
mayhem@alba.st

Caratteristiche

Nessuna autenticazione

Nessuna firma

Nessuna cifratura

http://www.alba.st/
mayhem@alba.st

Altri dettagli

Dati in chiaro sui device

Nessun log/accounting

Nessuna autenticazione

http://www.alba.st/
mayhem@alba.st

Gestione

Gestione

Interfaccia WEB di gestione

Gestione

Interfaccia WEB di gestione

Amministrazione remota (VNC)

http://www.alba.st/
mayhem@alba.st

Gestione

Interfaccia WEB di gestione

Amministrazione remota (VNC)

Accesso da remoto (Dial-up, VPN)

http://www.alba.st/
mayhem@alba.st

Gestione

Interfaccia WEB di gestione

Amministrazione remota (VNC)

Accesso da remoto (Dial-up, VPN)

Funzionalità non documentate (backdoor?)

http://www.alba.st/
mayhem@alba.st

Leggerezze

http://www.alba.st/
mayhem@alba.st

Leggerezze

Configurazioni di default

http://www.alba.st/
mayhem@alba.st

Leggerezze

Configurazioni di default

Nessun backup delle configurazioni

Leggerezze

Configurazioni di default

Nessun backup delle configurazioni

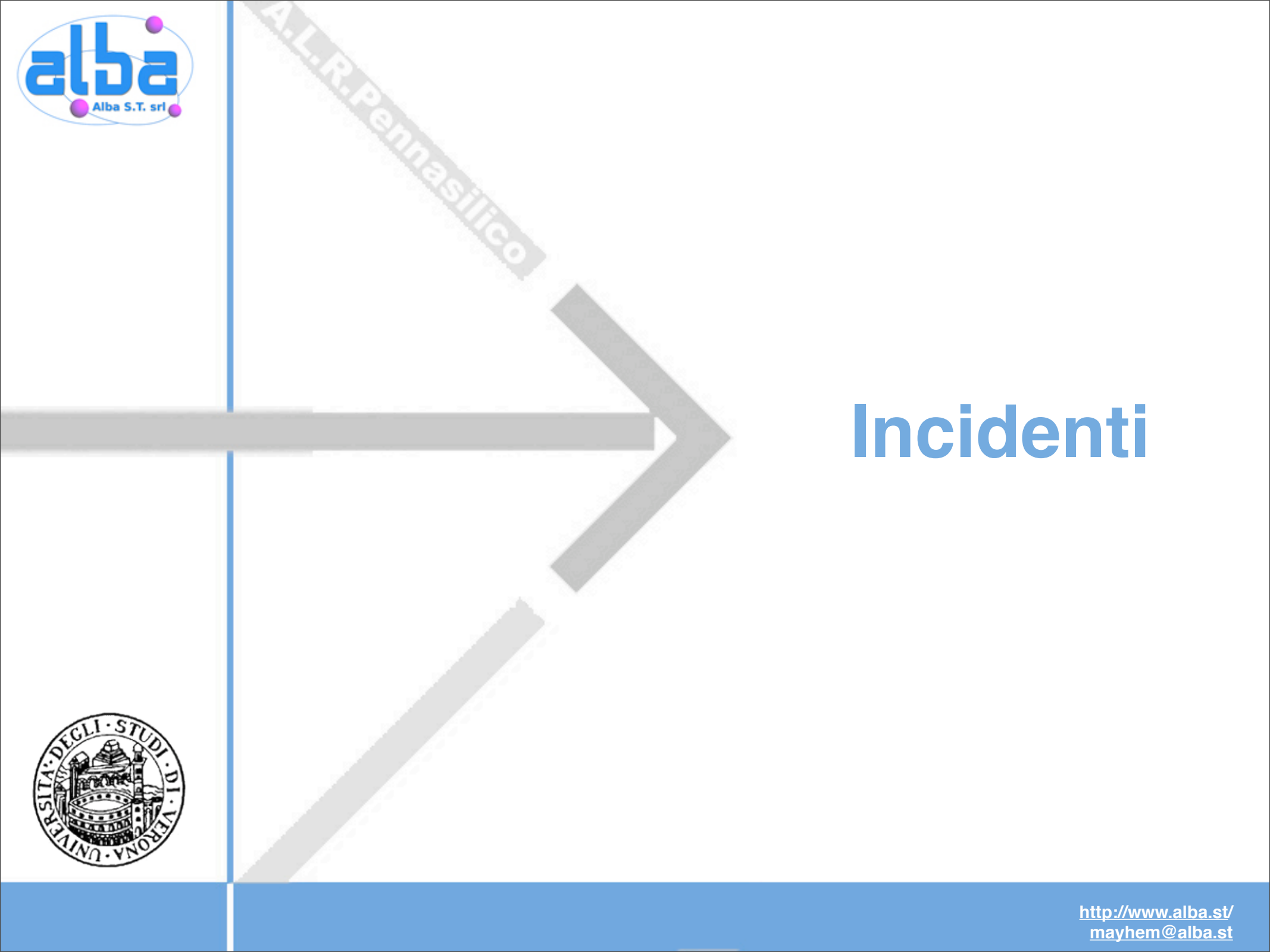
Nessun piano di DR **testato**

http://www.alba.st/
mayhem@alba.st

Vulnerabilità

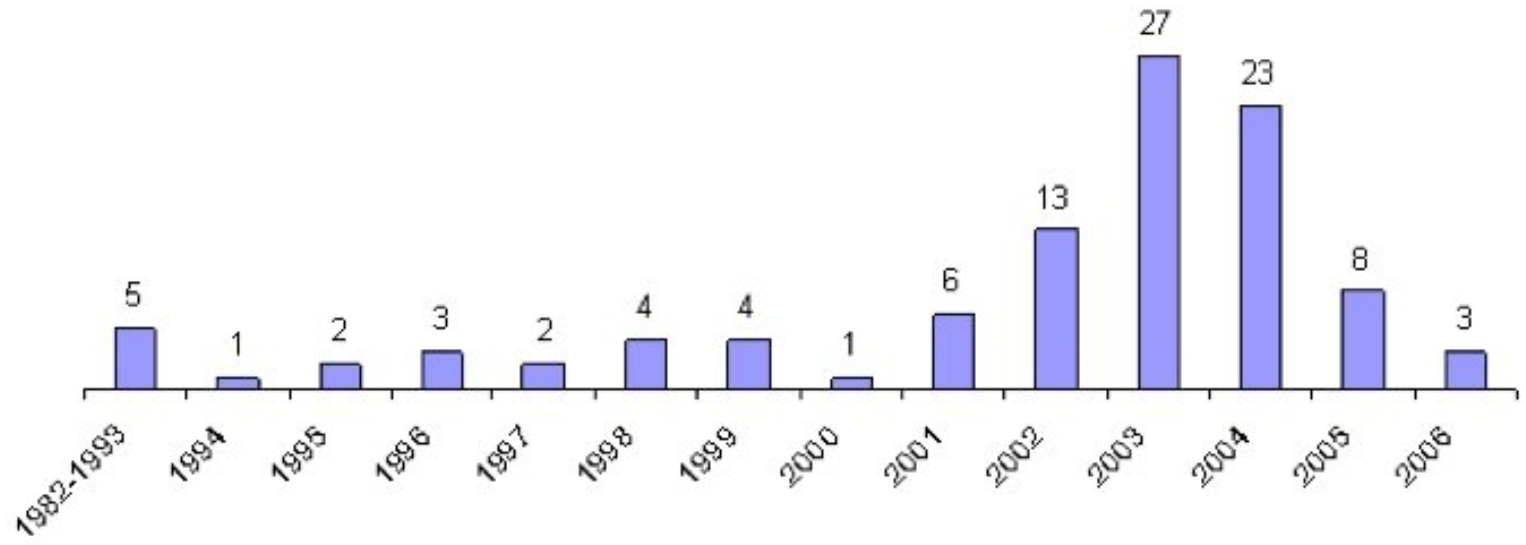
Vulnerabili a virus, worm, anomalie

Un errore può causare un effetto a catena (dirompente)



Incidenti

Known incidents



Incidenti per anno

(NIST, Guide to SCADA Security)

http://www.alba.st/
mayhem@alba.st

2001

Aumenta il numero degli attacchi

Aumentano gli incidenti provocati/ provenienti dall'esterno

http://www.alba.st/
mayhem@alba.st

Anni 80/90

Security through obscurity

Hardware proprietario

Firmware proprietario

Cablaggio proprietario

Protocolli proprietari (o specifici)

Isolato dall'infrastruttura

http://www.alba.st/
mayhem@alba.st

Eravamo abituati a ...

http://www.metroland.org.uk/signal/amer01.jpg

http://www.alba.st/
mayhem@alba.st

Il mercato

Nel tempo anche i produttori di questi sistemi si sono adeguati agli standard, per abbattere i costi.

http://www.alba.st/
mayhem@alba.st

Cheapness through standards

Standard PC

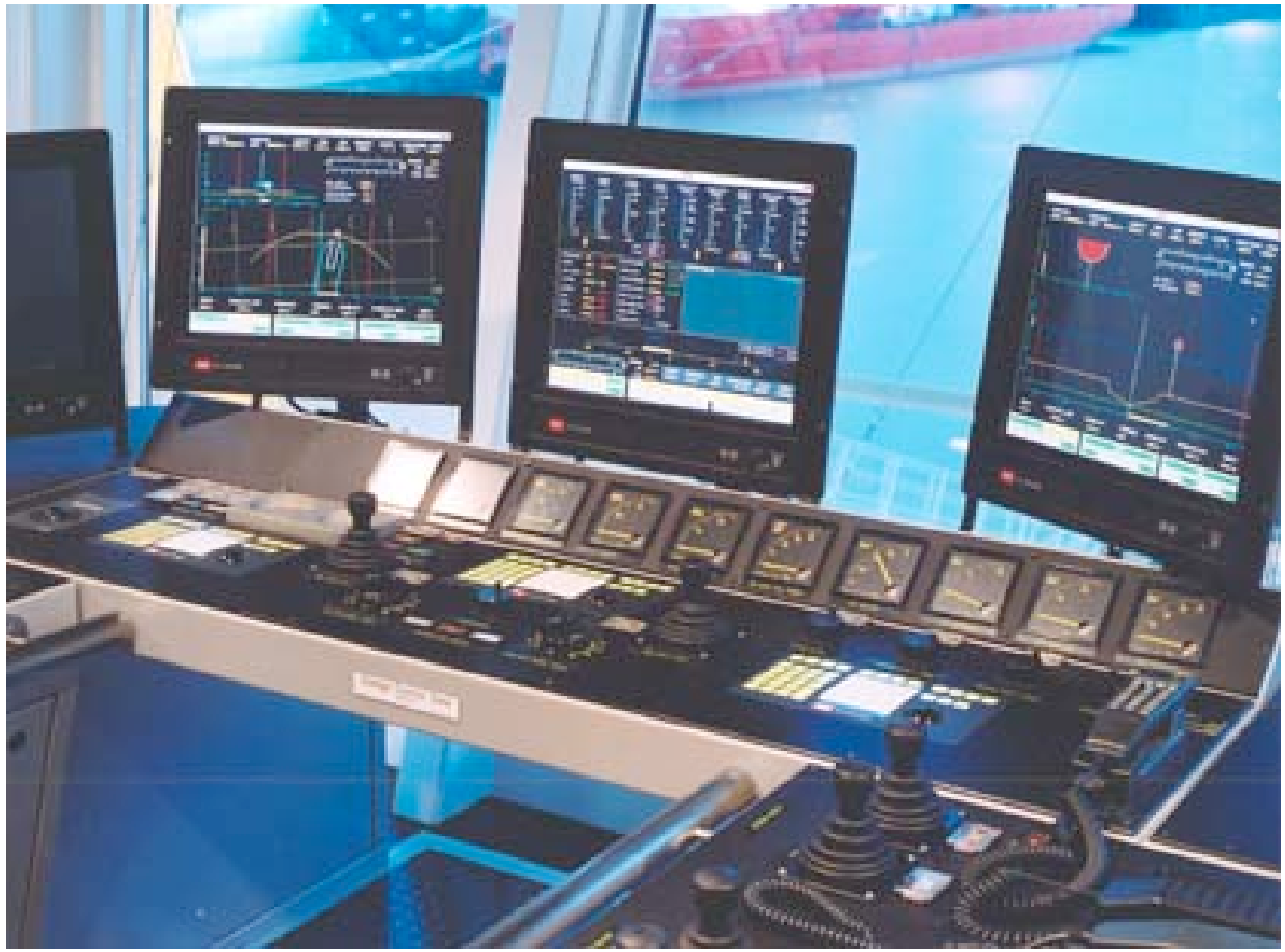
Sistemi Operativi Legacy

Ethernet, TCP/IP, wifi!

Cablaggio strutturato / FX

http://www.alba.st/
mayhem@alba.st

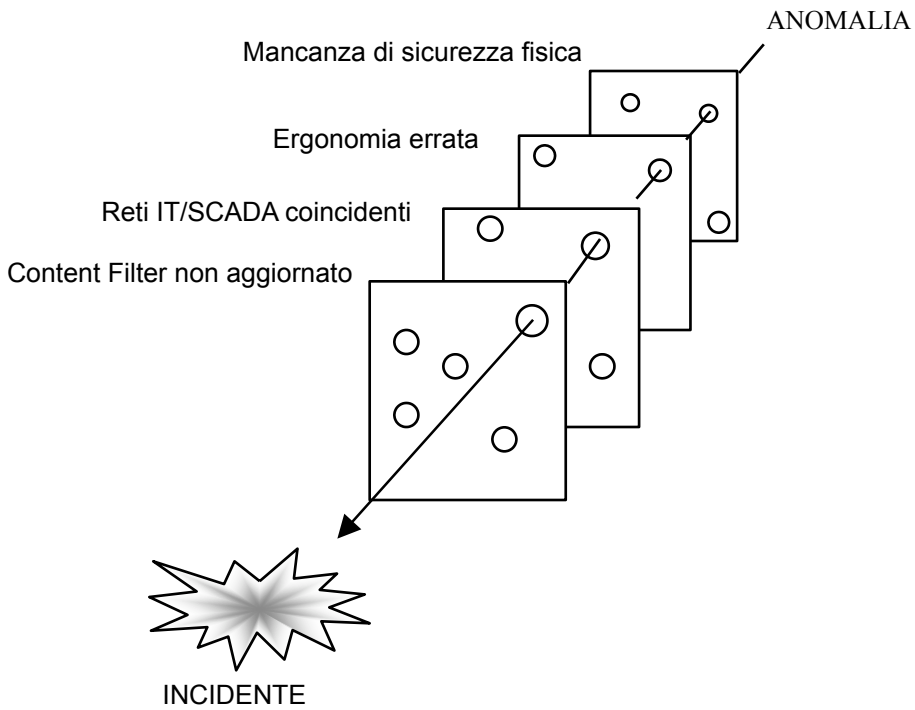
... oggi abbiamo...



http://www.ihcsystems.com/section_n/images/efficientdredgingnewsapril2005_Page_09_Image_0002.jpg

http://www.alba.st/
mayhem@alba.st

Dimensione collettiva della sicurezza

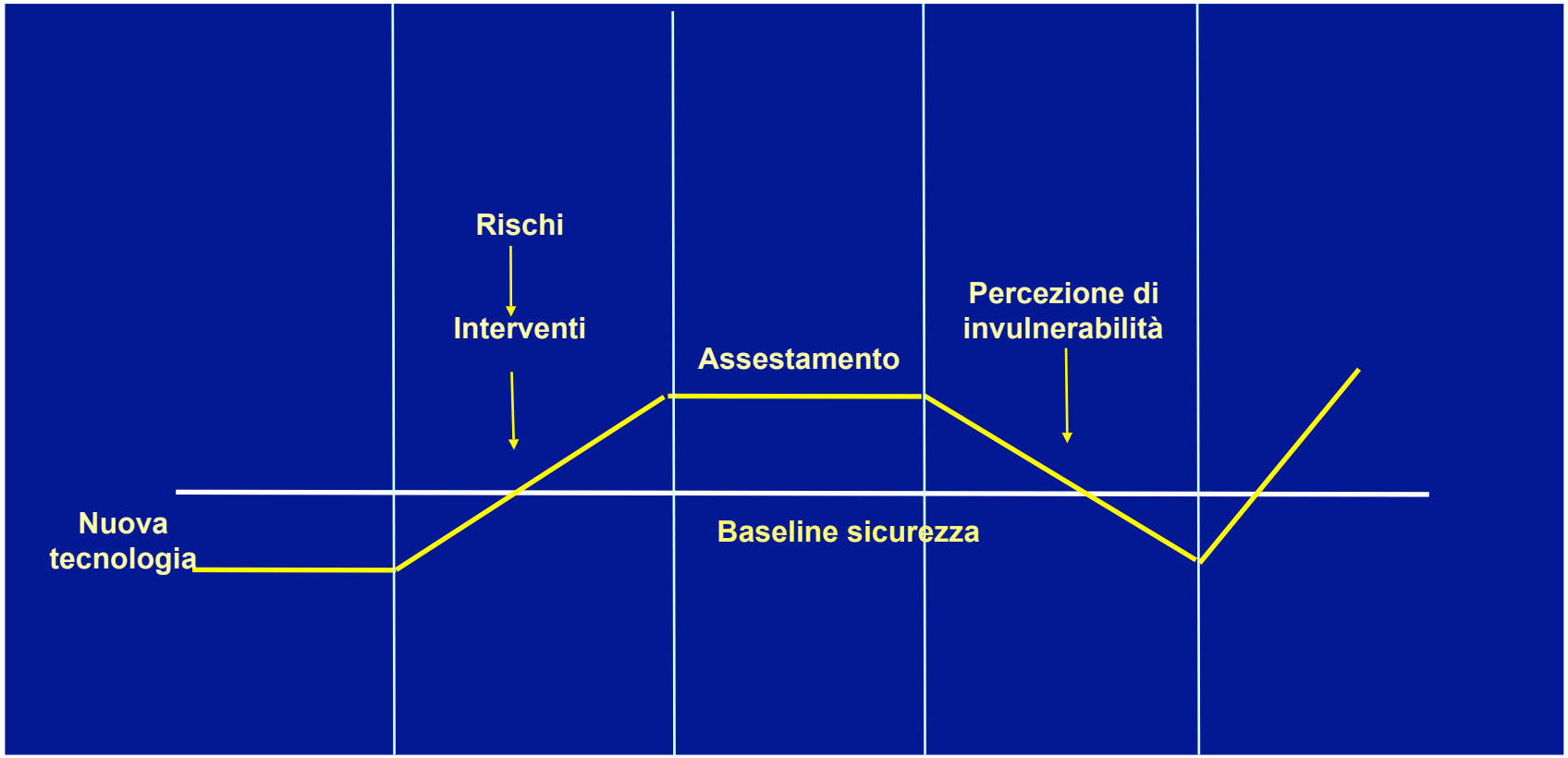


- processo multi-stratificato
- fallimenti locali a qualsiasi livello e per ogni ruolo, interagendo tra loro, abbassano il livello globale di sicurezza.

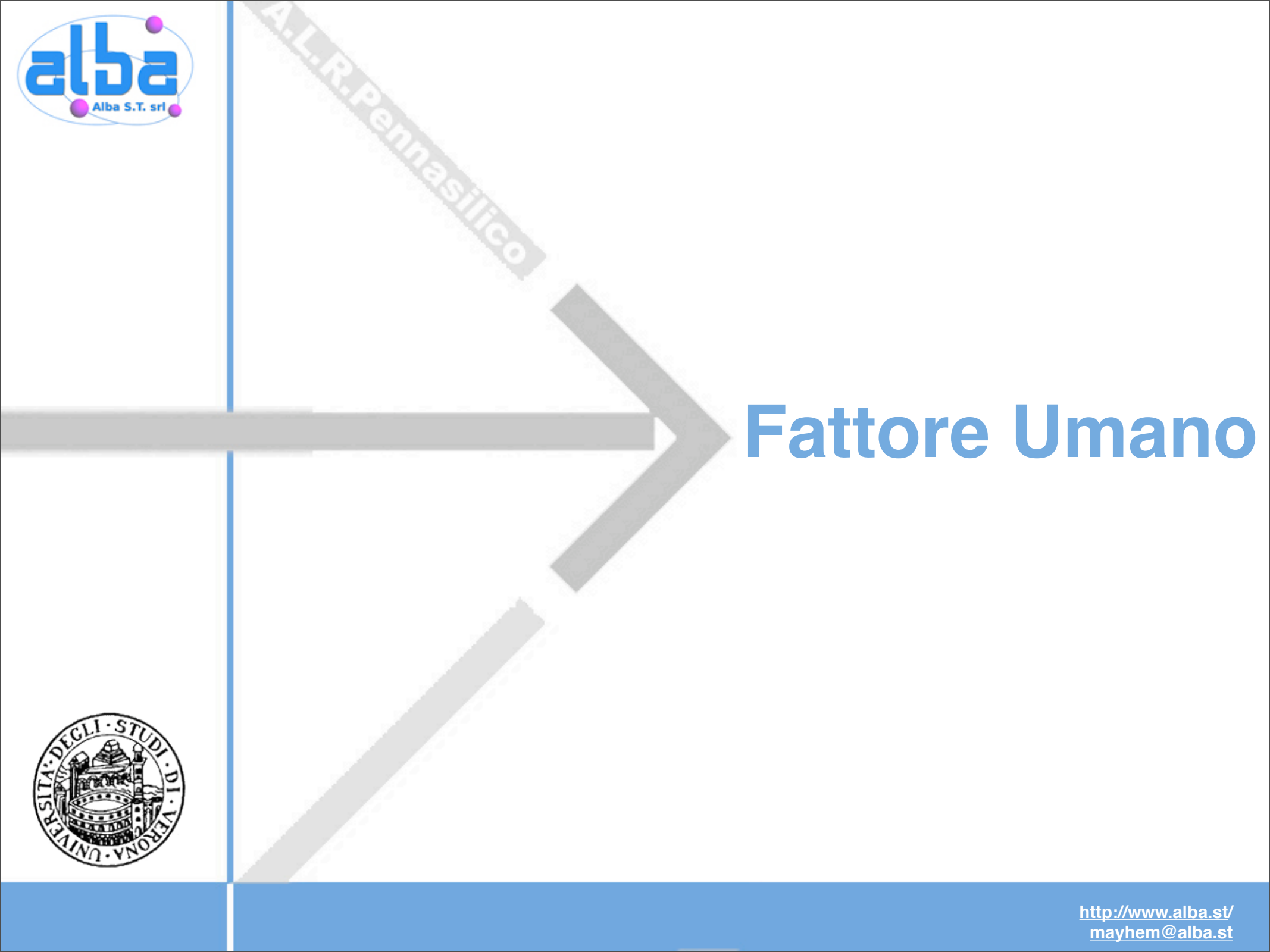
1

http://www.alba.st/
mayhem@alba.st

Andamento della sicurezza all'introduzione di una nuova tecnologia



http://www.alba.st/
mayhem@alba.st



Fattore Umano

http://www.alba.st/
mayhem@alba.st

Percezione

Gli attuali sistemi SCADA vengono spesso percepiti ancora come le “vecchie” macchine, disconnesse, non interoperabili, in nessun modo correlate ai rischi delle reti IP.

http://www.alba.st/
mayhem@alba.st

Errata percezione del rischio

http://www.alba.st/
mayhem@alba.st

Errata percezione del rischio

non corretta implementazione

http://www.alba.st/
mayhem@alba.st

Errata percezione del rischio

non corretta implementazione

non corretta gestione

http://www.alba.st/
mayhem@alba.st

Conseguenze

abbassamento della sicurezza

ripercussioni economiche

danni a persone

Conseguenze

Le persone

I CSO spesso non sono coinvolti nella sicurezza dell'infrastruttura

Gli operatori utilizzano i computer dedicati a SCADA come "normali PC"

http://www.alba.st/
mayhem@alba.st

Blockbuster

“Il sistema di gestione della centrale elettrica non rispondeva. L’operatore stava guardando un DVD sul computer di gestione”

CSO di una utility di distribuzione energia elettrica

http://www.alba.st/
mayhem@alba.st

Connessioni

La rete SCADA è troppo spesso collegata o coincidente con la rete dei “normali” computer.

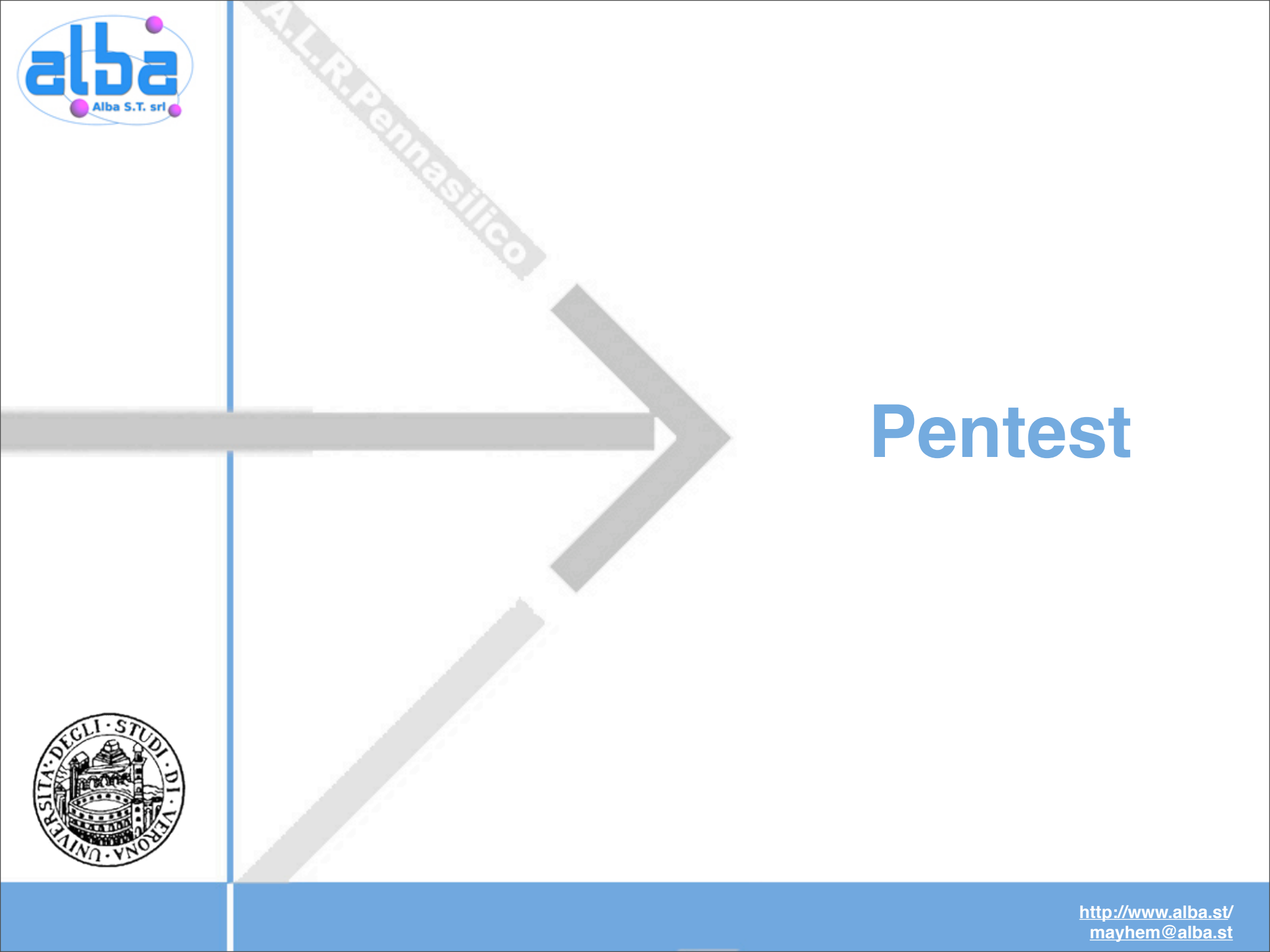
http://www.alba.st/
mayhem@alba.st

Worm

“In August 2003 Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours.”

Nist,Guide to SCADA

http://www.alba.st/
mayhem@alba.st



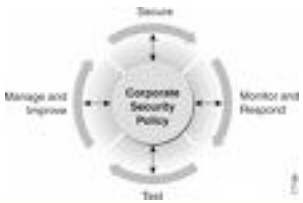
Pentest

http://www.alba.st/
mayhem@alba.st

Il motto

Security testing is a need...

PenTesting is a problem...



http://www.alba.st/
mayhem@alba.st

Il problema

un semplice port scan

potrebbe generare

comportamenti non previsti

con conseguenze sulle persone

http://www.alba.st/
mayhem@alba.st

Il braccio robotico

“While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated.”

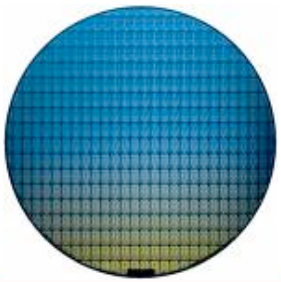
Nist,Guide to SCADA

http://www.alba.st/
mayhem@alba.st

Non solo biscotti

“Ping sweep was being performed on an ICS network to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers.”

Nist,Guide to SCADA



http://www.alba.st/
mayhem@alba.st

Approcci

identificare le vulnerabilità richiede un diverso approccio

le altre macchine possono essere riavviate ripristinate o sostituite con “pochi” disagi per gli utenti

http://www.alba.st/
mayhem@alba.st

Le macchine SCADA

controllano un processo che si svolge nel mondo “reale”

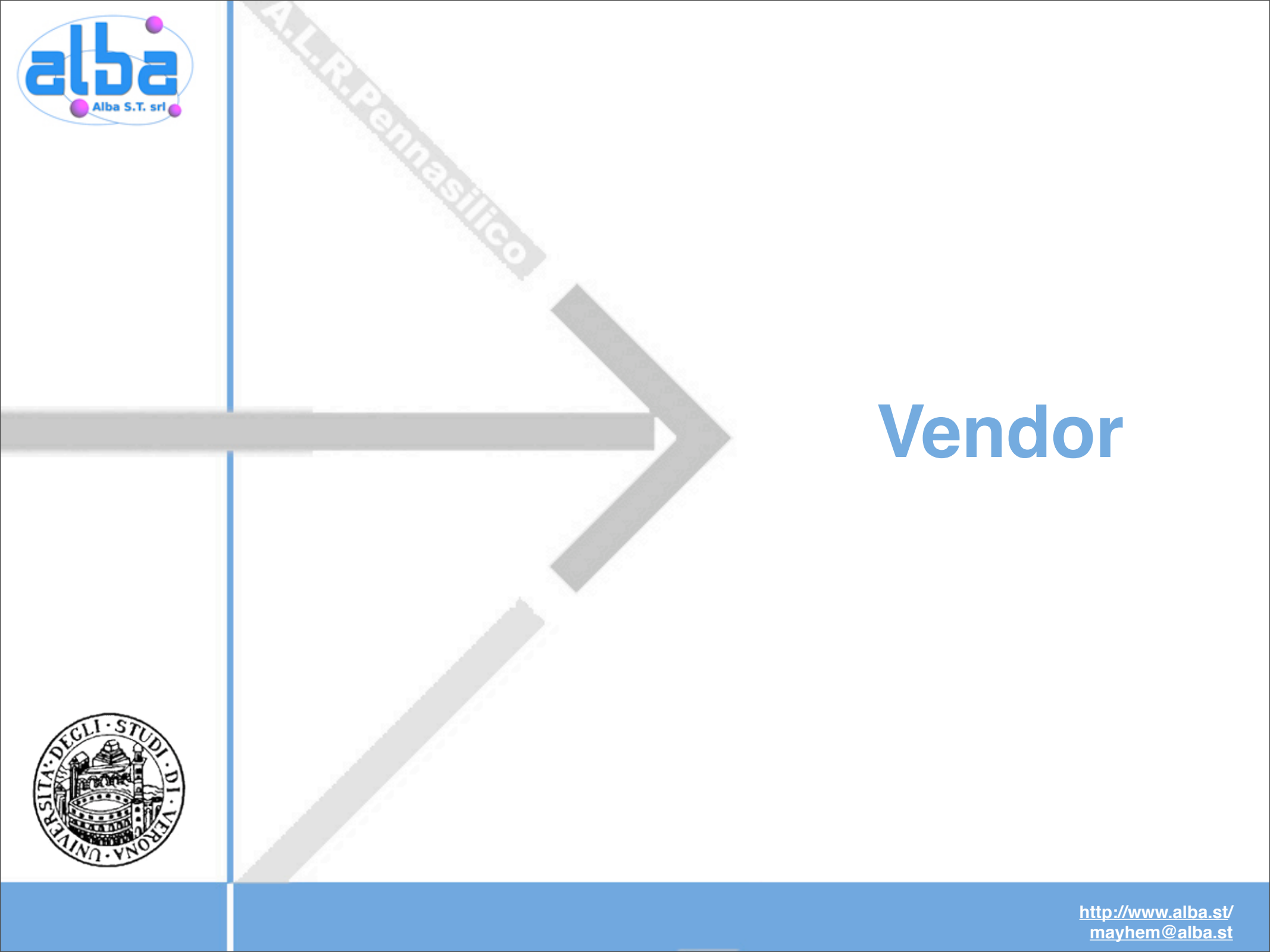
reali sono le conseguenze

http://www.alba.st/
mayhem@alba.st

Tablella #A

To Be Identified	Usual IT Action	Suggested ICS Actions
Hosts, nodes, and networks	Ping sweep (e.g., nmap)	• Examine router configuration files or route tables • Perform physical verification (chasing wires) • Conduct passive network listening or use intrusion detection (e.g., snort) on the network • Specify a subset of IP addresses to be programmatically scanned
Services	Port scan (e.g., nmap)	• Do local port verification (e.g., netstat) • Scan a duplicate, development, or test system on a non-production network
Vulnerabilities within a service	Vulnerability scan (e.g., nessus)	• Perform local banner grabbing with version lookup in Common Vulnerabilities and Exposures (CVE) • Scan a duplicate, development, or test system on a non-production network

http://www.alba.st/
mayhem@alba.st



Vendor

I produttori dovrebbero

scegliere di investire nella sicurezza

http://www.alba.st/
mayhem@alba.st

I vendor

comportamento spesso inadeguato
alle richieste degli utilizzatori

la fase di verifica dovrebbe avvenire
in fase di progettazione

prima della “messa in produzione”.

http://www.alba.st/
mayhem@alba.st

Il caso

“Il nostro fornitore ci fornisce patch da applicare una volta all’anno”

CSO di una utility di distribuzione energia elettrica

http://www.alba.st/
mayhem@alba.st

Test Bed

Usare la virtualizzazione

(molti prodotti in fase di sviluppo)

Partecipare/Utilizzare ai progetti honeynet su SCADA

http://scadahoneynet.sourceforge.net/

http://www.alba.st/
mayhem@alba.st

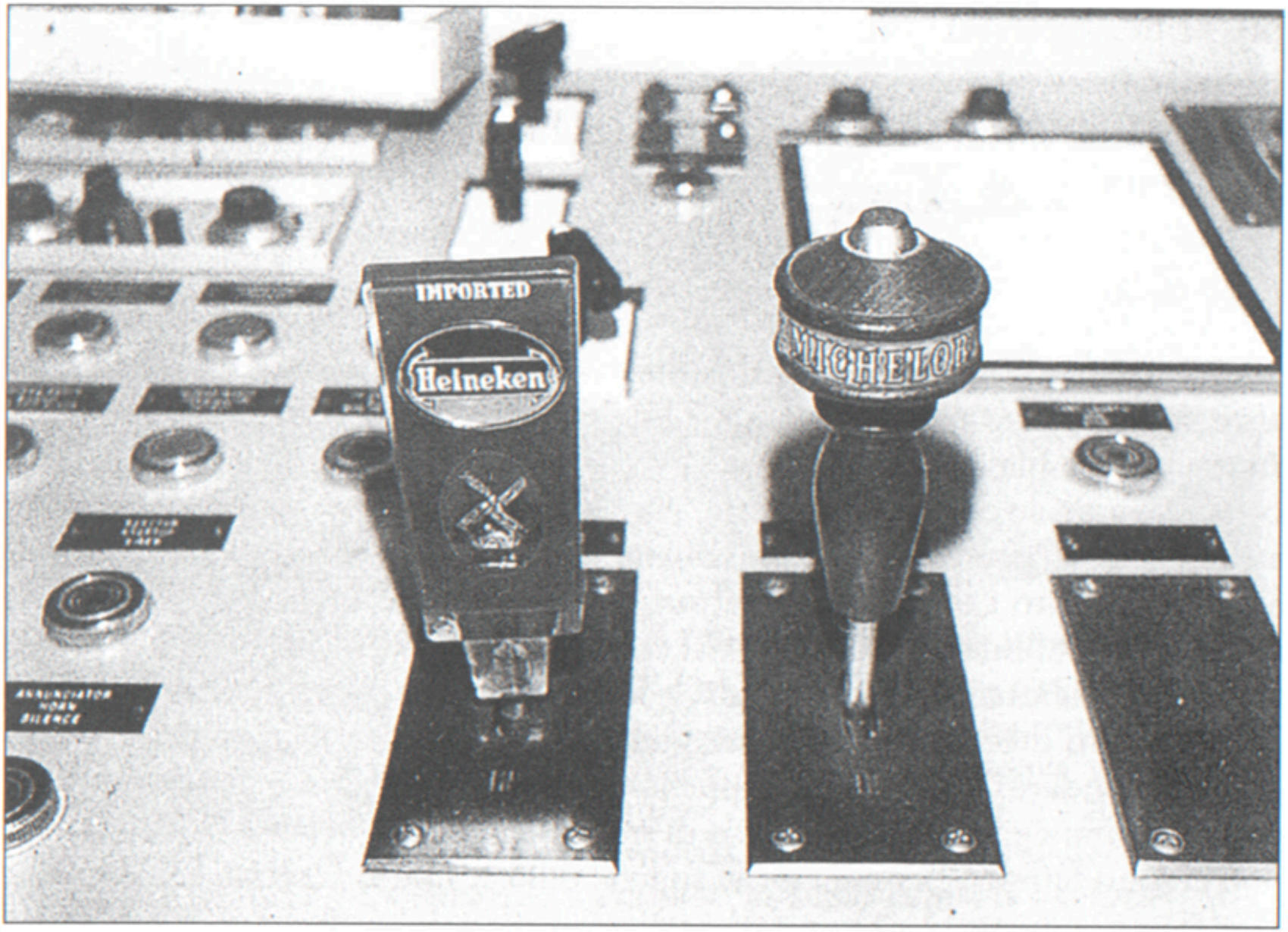
Ambienti di test

“Stiamo costruendo una centrale di test per fare tutte le prove del caso”

CSO di una utility di distribuzione energia elettrica

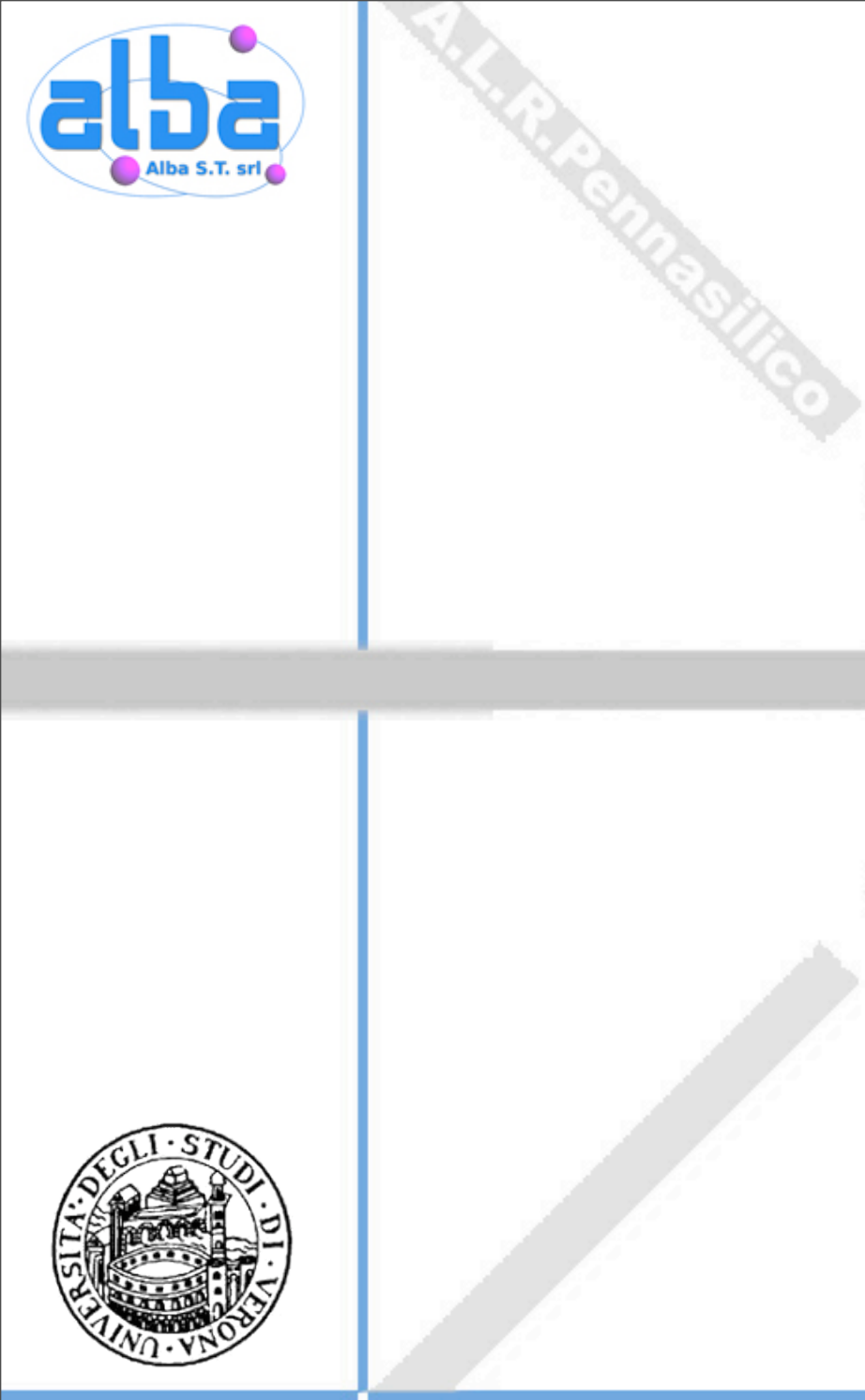
http://www.alba.st/
mayhem@alba.st

Ergonomia



Donald Norman,
"La caffettiera del masochista"

http://www.alba.st/
mayhem@alba.st



Contromisure

http://www.alba.st/
mayhem@alba.st

Sinergie

Per gestire un'infrastruttura SCADA è necessario un team:

CIO/CSO e dirigenti

IT specialist and ICS engineers

responsabili per la sicurezza fisica

http://www.alba.st/
mayhem@alba.st

Formare sui rischi..

IT/CSO/Management

operatori SCADA

sorveglianti/guardie

chi scrive e gestisce le policy

http://www.alba.st/
mayhem@alba.st

Implementare...

- ✓ Sicurezza Fisica
- ✓ VLAN/DMZ
- ✓ Firewall/Content Filter
- ✓ Quality of Service
- ✓ Ridondanza
- ✓ Documentazione corretta
- ✓ ... ed applicare le policy

http://www.alba.st/
mayhem@alba.st

Best Practice

- Adottare infrastrutture di AAA
- Utilizzare l'encryption (VPN)
- Disabilitare i servizi inutili
- Condurre regolari test di sicurezza con un metodo appropriato
- Utilizzare ambienti di test

http://www.alba.st/
mayhem@alba.st

Web-o-Graphy

http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf

https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

http://cansecwest.com/slides06/csw06-byres.pdf

http://www.physorg.com/news94025004.html

http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=206

http://www.apogeonline.com/libri/88-503-1042-0/ebook/libro

http://www.sans.org/reading_room/whitepapers/warfare/1644.php

http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm

http://www.securityfocus.com/news/11402

http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf

http://www.visionautomation.it/modules/AMS/article.php?storyid=32

http://www.iscom.istsupcti.it/index.php?option=com_content&task=view&id=16&Itemid=1

Ringraziamenti

Elisa Bortolani @ UniVR

Raoul Chiesa @ ISECOM

Enzo Maria Tieghi @ Clusit

Sabato 16 Giugno 2007

Linux e la Sicurezza Personale

Relatori da tutta italia

Una giornata incentrata sul software OpenSource e la Sicurezza

Itis G. Marconi - www.verona.linux.it

Domande?

Queste slide sono disponibili su:
http://www.alba.st

Per domande o approfondimenti:
mayhem@alba.st

Domande?

Grazie per l'attenzione!

Queste slide sono disponibili su:
http://www.alba.st

Per domande o approfondimenti:
mayhem@alba.st