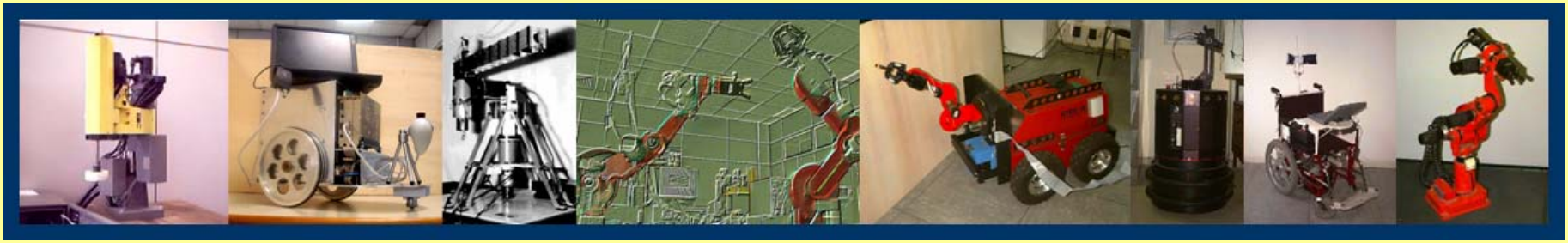
ROMA TRE
UNIVERSITÀ DEGLI STUDI

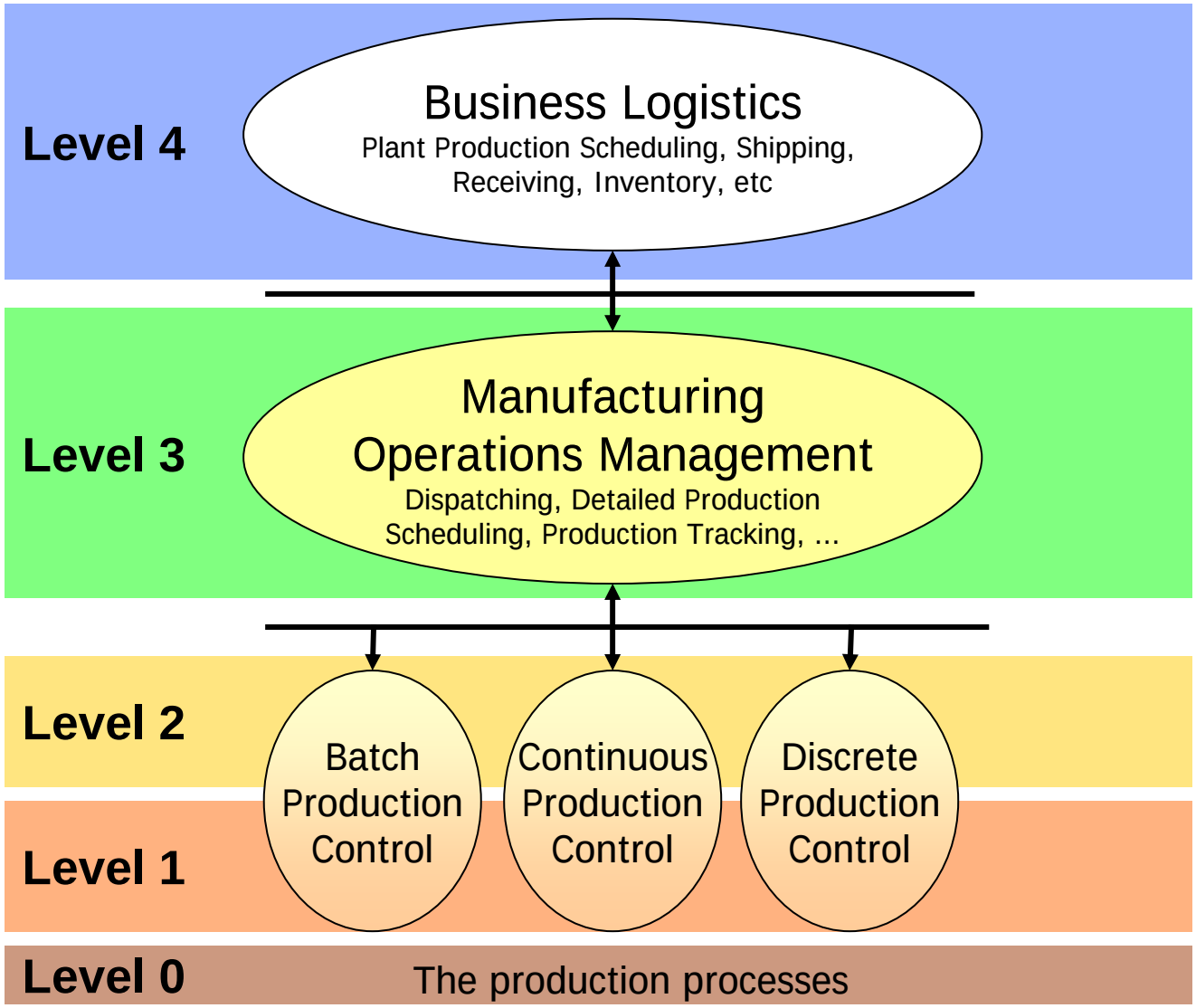
ROBOTICS AND SENSOR FUSION LABORATORY

Problematiche di sicurezza dei sistemi di monitoraggio e controllo

Prof. Stefano Panzieri



Modello Funzionale ISA-95 (2000)



Livello 4: business planning and logistics. Qui si trovano attività come la schedulazione della produzione

Level 3 è il livello del "manufacturing operations and control" del "production dispatching", del "detailed production scheduling", e del "reliability assurance"

I **Livelli 4** e **3** sono gli stessi indipendentemente dal tipo di industria

I **Livelli 2, 1,** e **0** differiscono a secondo del tipo di industria (batch, continuo, e discreto)

Cyber Incidenti: Vulnerabilità

I tre aspetti della Sicurezza

- **Sicurezza "Fisica"** (perimetrale):
  - Guardie, porte e cancelli, filo spinato…
- **Sicurezza del personale** (org)**:**
  - Selezione accurata, referenze
  - Politiche di formazione
  - Procedure di sicurezza
  - Consapevolezza e Training
- **Cyber-Security** (Tecnologia)**:**
  - Perimetro "logico"
  - Autenticazione Password (o biometria)
  - Segmentazione e segregazione reti
  - Firewalls, AntiVirus, ecc.
  - IDS - IPS (Intrusion Det/Prev Systems)

Uno strano caso a Maroochy Shire (AUS)

Una storia vera

Lo strano caso di Maroochy Shire

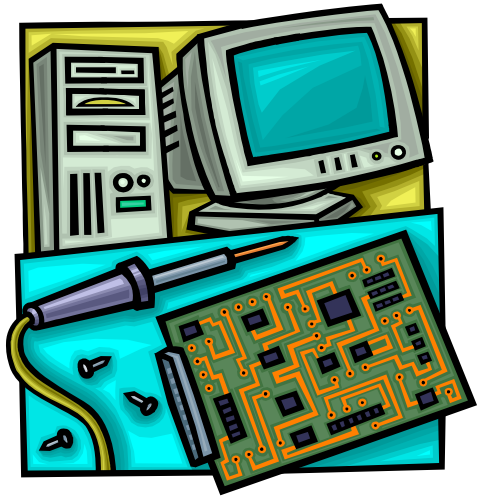
Personaggi

- Vitek Boden - Consulente di automazione
- Ente distribuzione acque di Maroochy Shire (AUS)
- I cittadini della contea di Maroochy Shire
- L' ecosistema della contea di Maroochy Shire
- Una pattuglia di polizia stradale

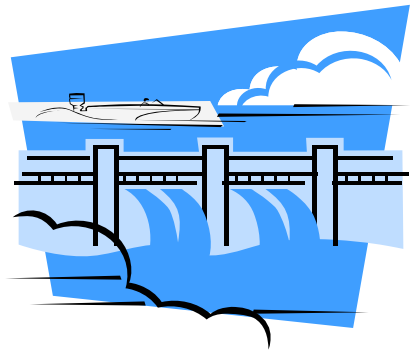
Lo strano caso di Maroochy Shire

L'antefatto

Vitek Boden è un tecnico di automazione, esperto nella programmazione di PLC e PC.



Lavora come consulente di un'azienda che ha vinto l' appalto per l'installazione di un impianto di depurazione acque per l' ente che gestisce la distribuzione dell' acqua nella contea di Maroochy Shire (AUS)



Ha accesso, conosce e sa operare sul sistema di controllo di 300 nodi che governano la depurazione e distribuzione dell' acqua.

Lo strano caso di Maroochy Shire

Il movente

Vitek lascia l'azienda di integrazione e cerca di farsi assumere dall'ente che gestisce il depuratore.

Ma non viene accettato

Lo strano caso di Maroochy Shire

Il delitto

Tra **Gennaio 2000** e **aprile 2000:**

- il depuratore subisce **47** "**incidenti**" **inspiegabili**
- Milioni di litri di liquami invadono la rete di distribuzione acque
- In molte case di Maroochy Shire dai rubinetti esce acqua nera e maleodorante
- L' ecosistema (laghi, parchi e torrenti di una zona residenziale australiana - Sunshine Coast) vengono inquinati, con perdite incalcolabili di flora e fauna acquatica (e business turistico)

Lo strano caso di Maroochy Shire

La cattura

Il **23 Aprile 2000** l' auto di Vitek Boden viene fermata per un normale controllo di polizia stradale.

Sull' auto, la polizia trova apparati radio, un PC per programmare PLC, un PLC funzionante: **tutti risultano rubati dall' impianto di depurazione.**

Vitek viene **arrestato**: tra il materiale recuperato la polizia trova anche il badge per accesso all'impianto (**ancora funzionante**).

Lo strano caso di Maroochy Shire

La condanna

Il **31 ottobre 2001** in Australia Vitek Boden viene condannato per:

26 comprovate intrusioni tramite computer non autorizzate ed allo scopo di causare danni

1 caso di **inquinamento grave**

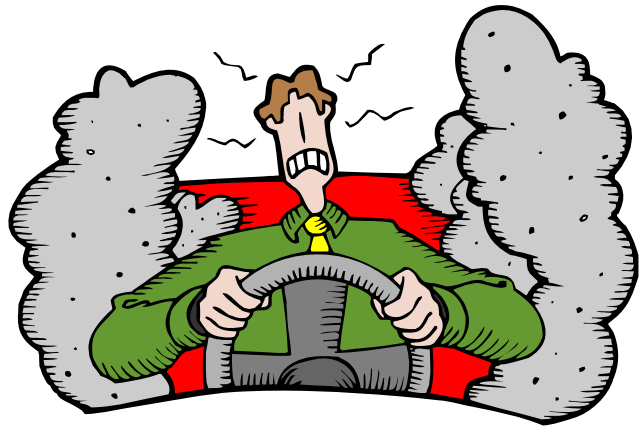
Oggi Vitek è in prigione

Altri casi di cyber-incidenti in ambiente industriale

- 1997: Shutdown alla torre di controllo Worchester Regional Airport (MA) USA
- Slammer blocca un sistema di sicurezza in una centrale nucleare in Ohio
- Italia: Sasser blocca **40 PC** in produzione in primaria azienda farmaceutica multinazionale (lotti da buttare o da rilavorare, week-end di lavoro per ripristinare i computer, riconvalida, ecc.)
- Molti non li ammettono, molti non ne sono consci, molti li attribuiscono ad “altro”…
- Unica statistica “ **ufficiale** ”: in California una venti tracciati tra il 2000 e il 2003
- Ora c’è anche il Database del BCIT

Esempi di “insiders”?

- Manutentore che aggiorna/corrompe un **PLC** in un’altra area dell’impianto via rete
- Password condivisa e poi cambiata blocca la manutenzione provocando la **fermata** dell’impianto
- **DCS** collegato a **ERP** via rete: per raccogliere i dati, un piccolo programma **in VB** causa una DOS (**Denial of Service**) con un buffer overload, causando una perdita di controllo

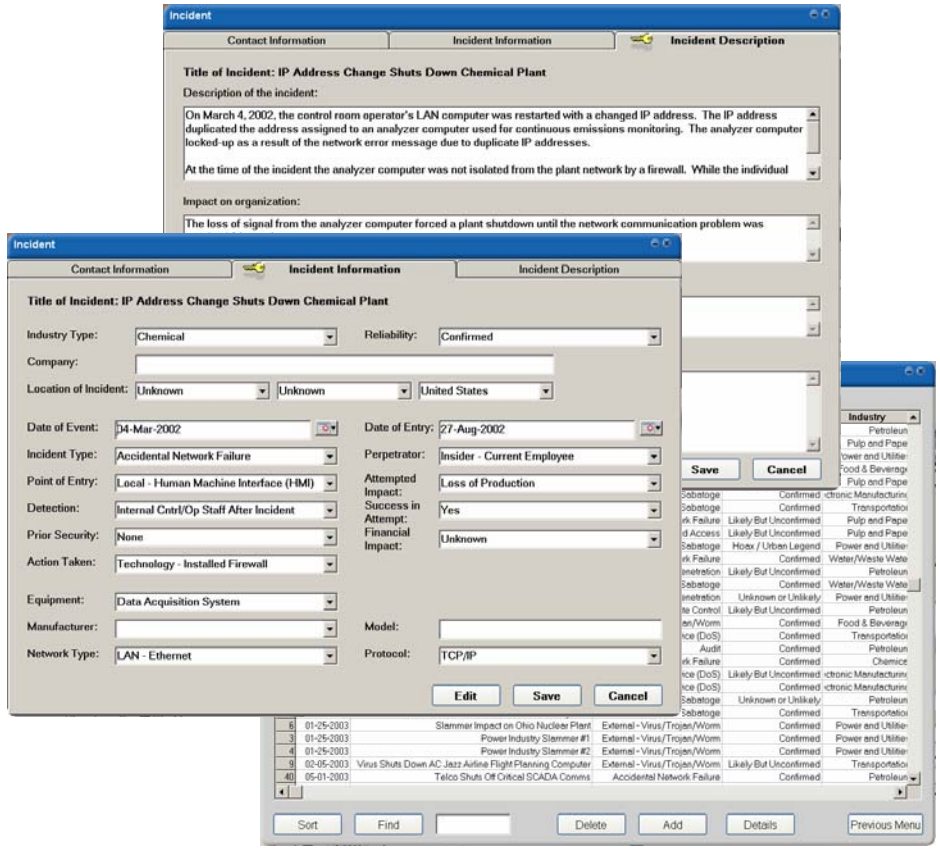


fonte: BCIT Industrial Security Incident Database (ISID)

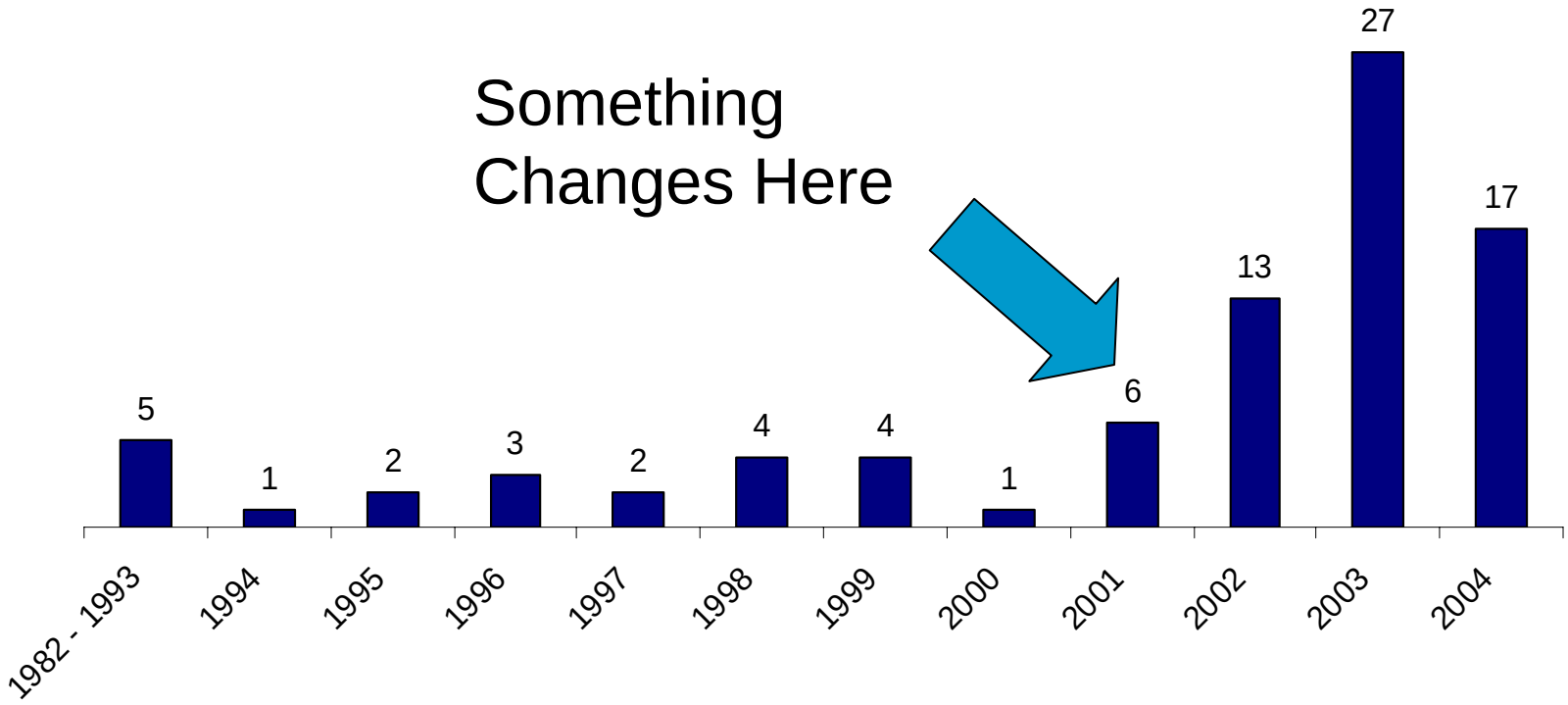
Incident Database

BCIT Industrial Security Incident Database (ISID)

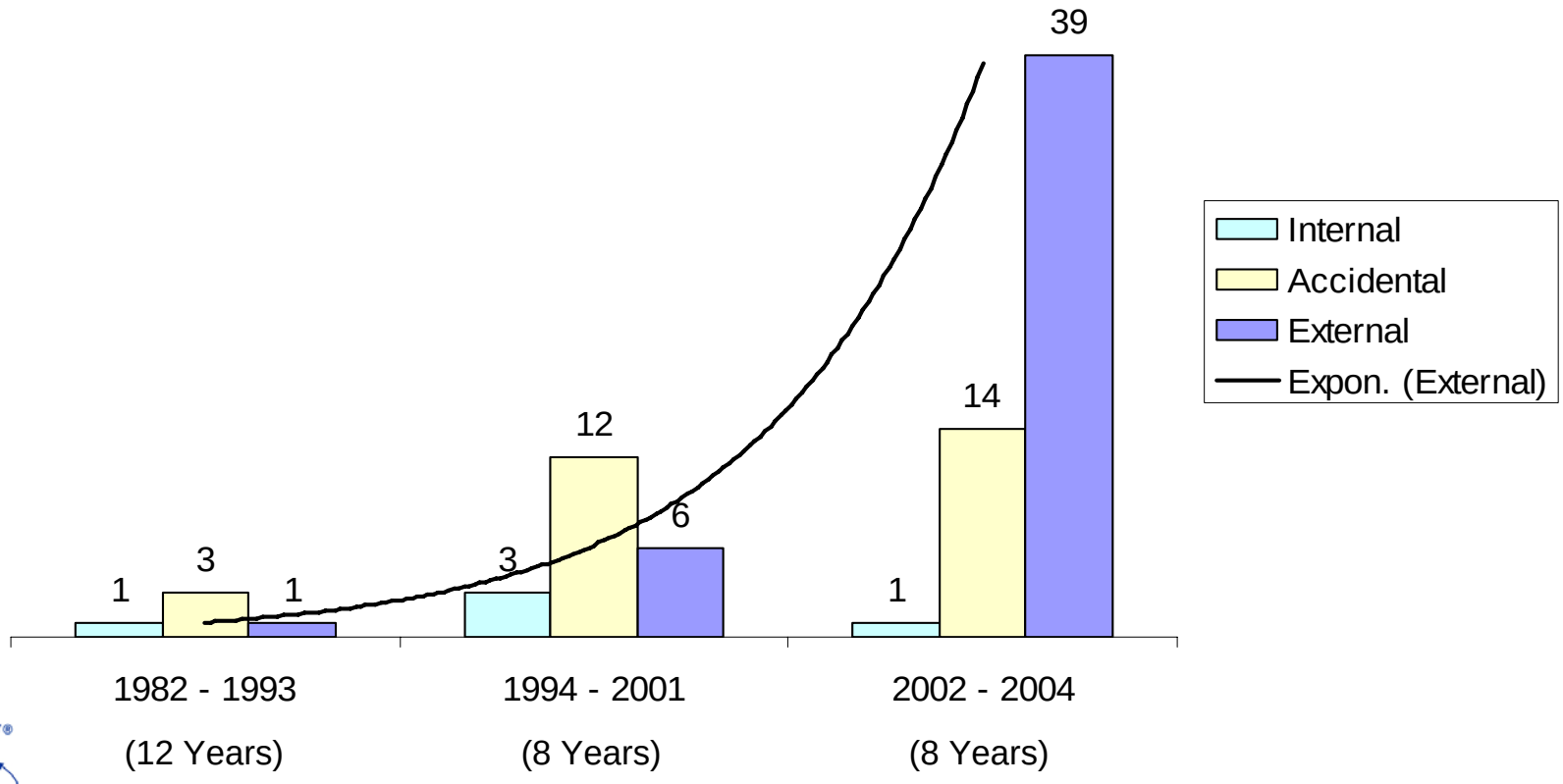
- ISID tracks network cyber incidents that directly impact industrial and SCADA operations.
- Both malicious and accidental incidents are tracked.



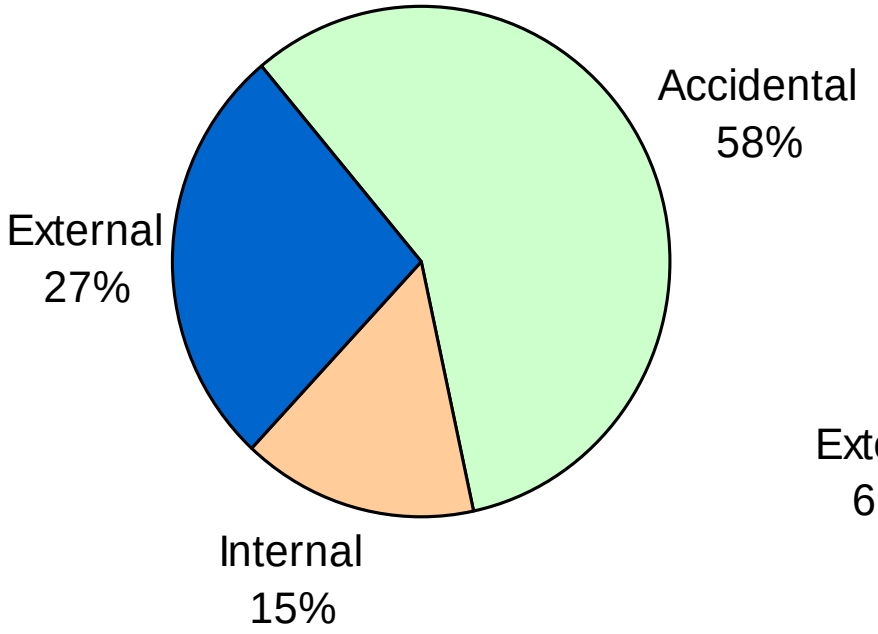
Overall Incident Trends



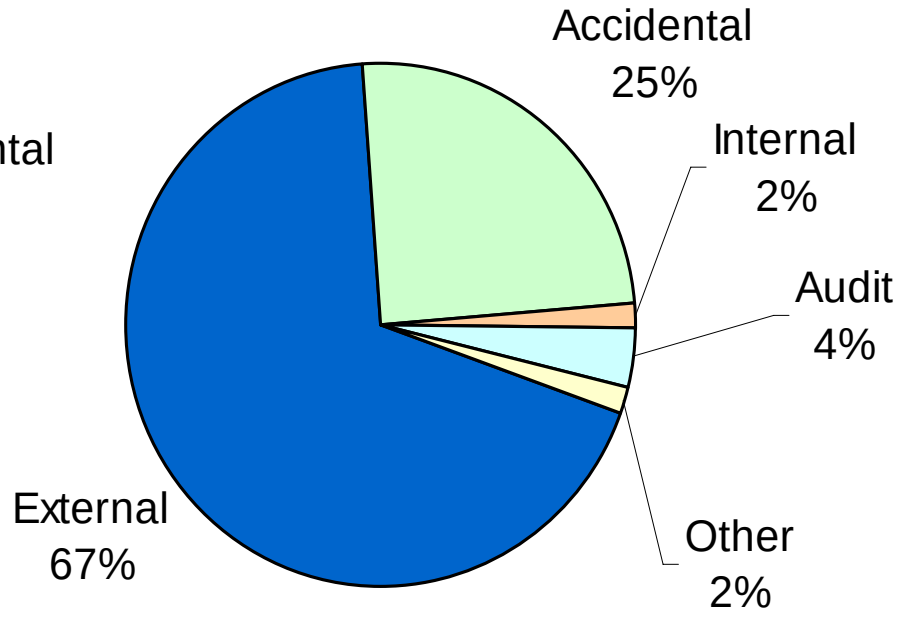
Something Happens in 2001…



The Types of Incidents Shift



1982 -2001

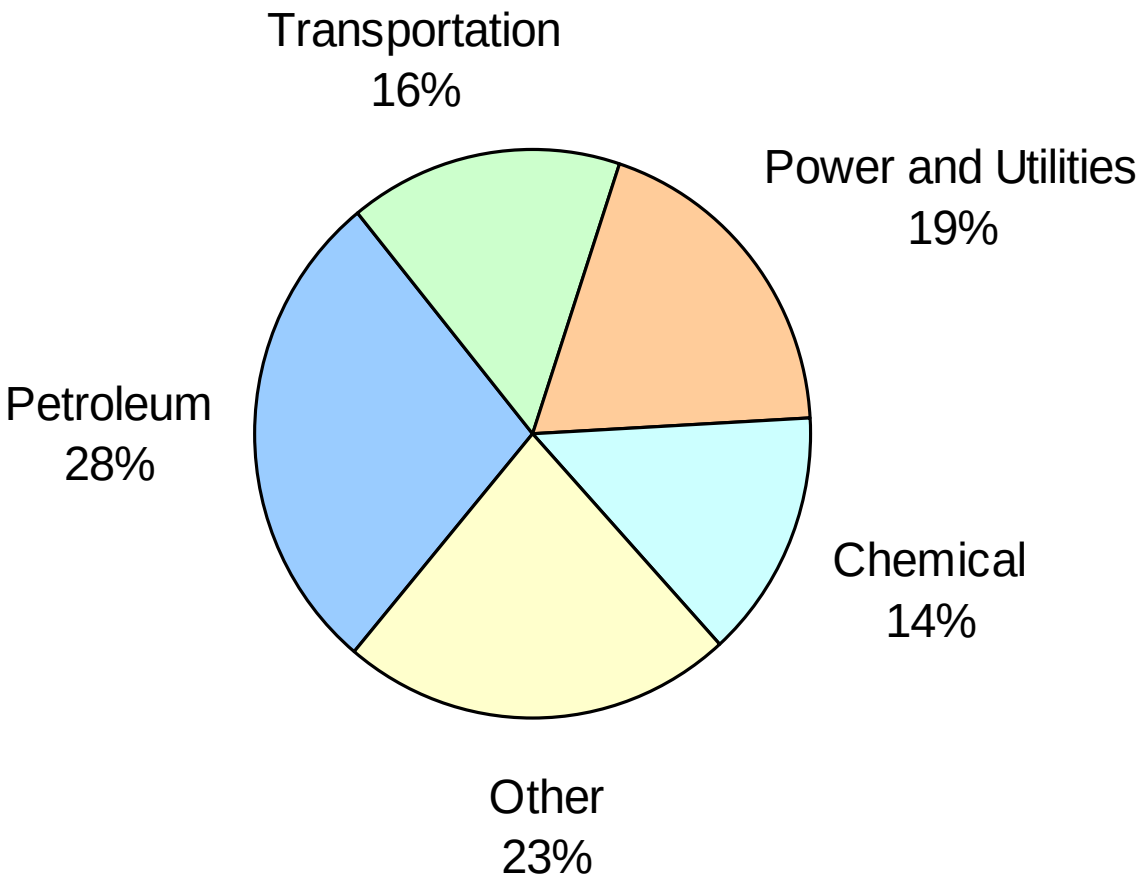


2002 -2004

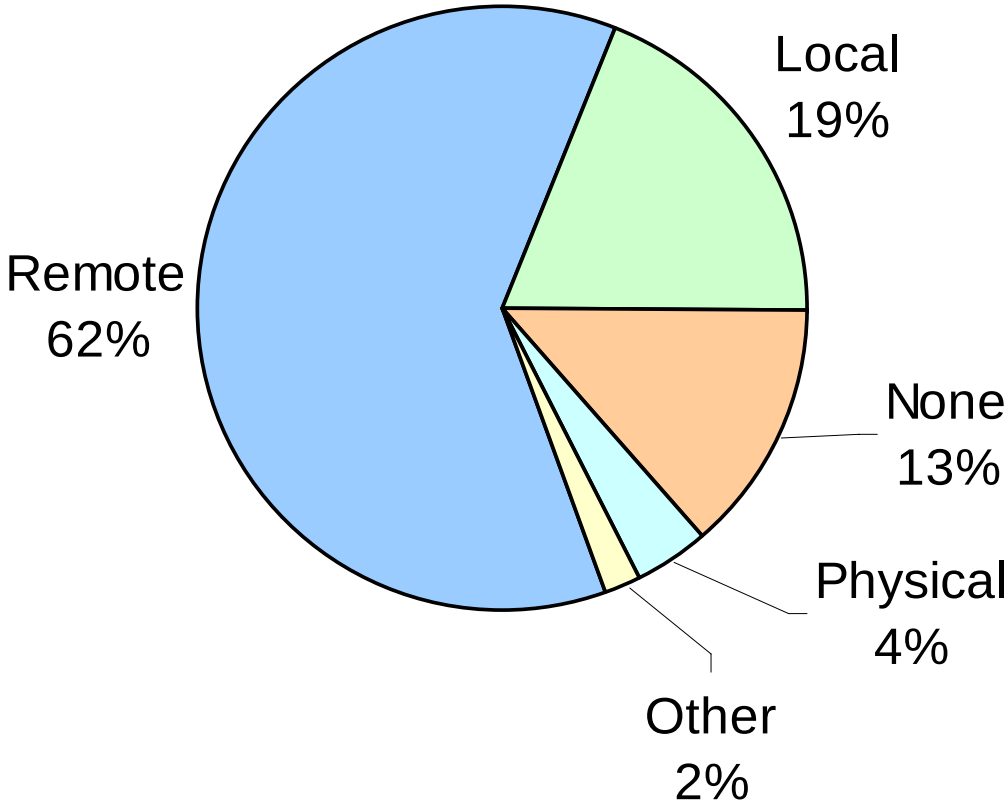
Why?

- Unlikely to be just a reporting artifact.
- Three possibilities:
  - Worms/Viruses change in 2001/2002.
  - Widespread industrial adoption of Ethernet and TCP/IP.
  - “SCADA” enters the public’s (and the hacker’s) awareness after 9/11.

Who is Getting Attacked?

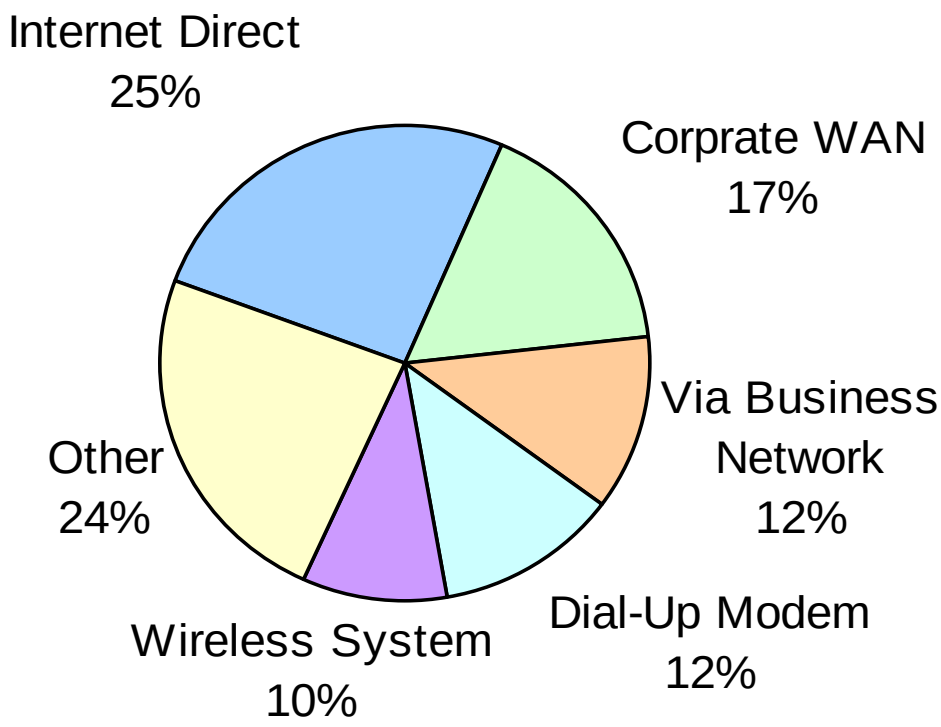


Where Do Attacks Come From?



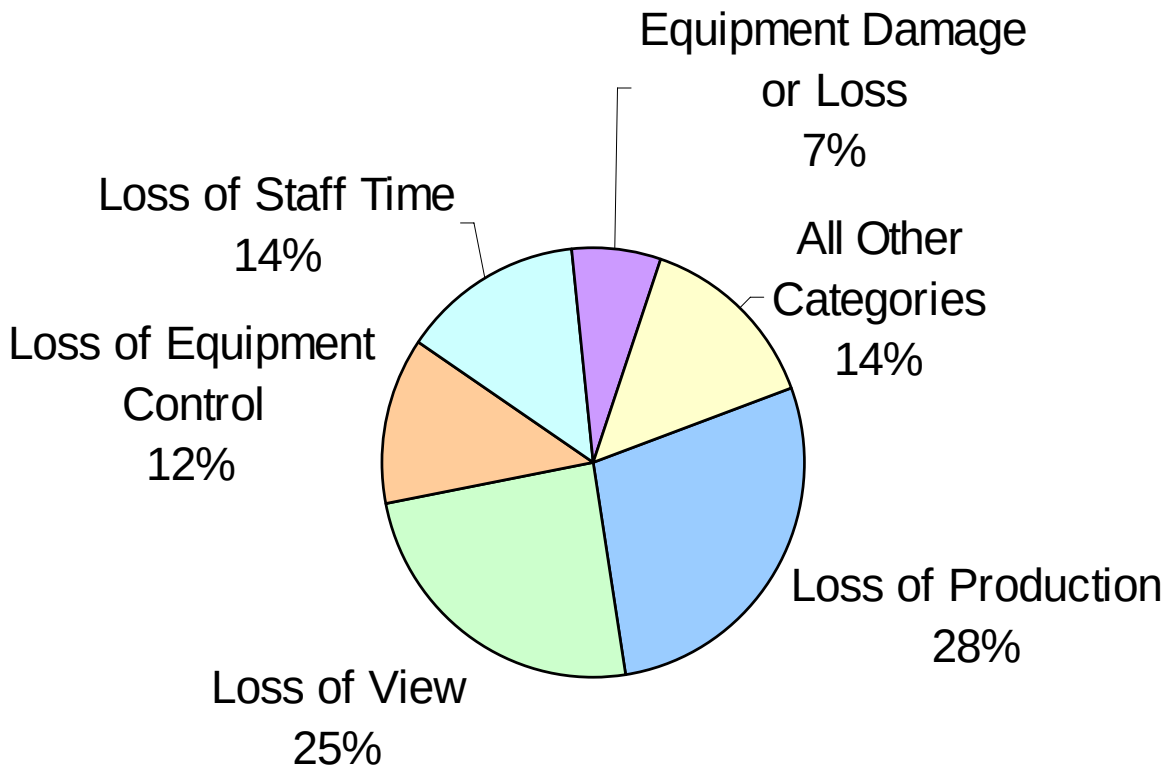
Getting in From the Outside

- Lots of ways in:
  - Internet Directly,
  - Corporate WAN,
  - Business Network,
  - Wireless,
  - Dial-up,
  - 3rd Party VPN,
  - Telco System.



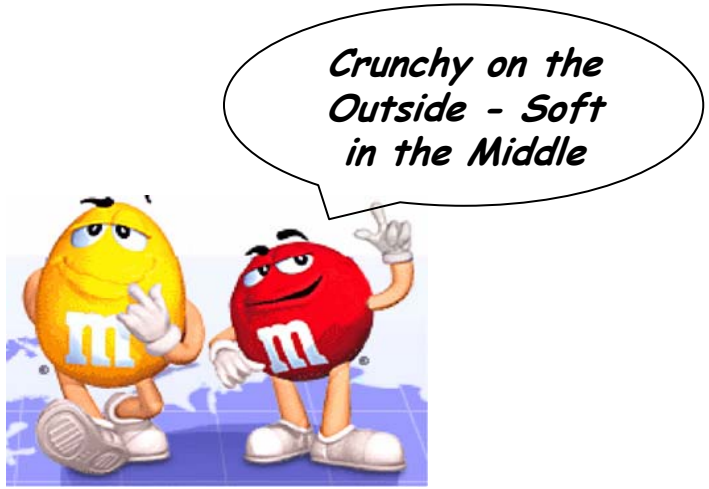
Consequences are Not Simply Financial

- Difficult to define financially:
  - HSE, Reputation, Brand, License to Operate
  - 28% suffered loss of production
  - 37% experienced loss of control or view



A Perimeter Defence is Not Enough

- The bad guys will eventually get in.
- We can't just install a firewall and forget about security.
- Must harden the plant floor.



Don't Bring a Knife to a Gun Fight…

- The world has changed.
- Know your "enemy" and pick your strategy accordingly.
- The wrong strategy won't protect your plant!

Perché le minacce

Cosa succede nell'industria	Cosa succede nel settore della sicurezza informatica
Maggiore quantità ed estensione di sistemi SCADA	Le organizzazioni più attaccate sono quelle che gestiscono Infrastrutture Critiche
Forte tendenza all'utilizzo di piattaforme standardizzate, e.g. Windows 2000	I sistemi maggiormente vulnerabili sono Microsoft ed i software basati sul Web
Progressivo spostamento verso sia il protocollo IP, sia il protocollo di gestione della rete SNMP	I protocolli più semplici da rompere sono IP e SNMP
Tendenza ad avere grande connettività tra la rete business e quella di gestione dell'impianto	Incrementano le opportunità di accesso
Diffusione della connettività Wireless	Il miglior modo per realizzare un accesso semplice ed illegale è la connessione Wireless
Le strutture informatiche sono comunque vincolate e ben controllate	Le risorse IT per la sicurezza sono complesse e difficili da gestire correttamente anche se stanno emergendo delle tecnologie significative
Il personale IT ben addestrato è difficilmente reperibile	Di tutti I professionisti IT quelli addetti alla sicurezza sono i più rari e costosi

11 motivi

11 motivi per i quali la **Sicurezza** di sistemi d controllo in produzione
(DCS, PLC, SCADA/HMI, reti di fabbrica, ecc.)
è differente da quella dell'I.T.

Perché la Sicurezza è diversa? /1

I rischi sono diversi!

- **Sistemi IT:**
  perdita di dati e informazioni, file e documenti, provocano ritardi di transazioni e incidono sul business (**risorse, tempo, soldi**), …
- **Sistemi di controllo:**
  oltre a quanto previsto per i Sistemi IT, la non sicurezza dei sistemi può incidere sull' integrità fisica di persone (**salute, incidenti sul lavoro, rischio ambientale e territoriale**) e sulla conservazione di impianti di produzione e cose (**risorse, tempo, soldi, macchinari,** …)

Perché la Sicurezza è diversa? /2

L'architettura di rete è diversa!

- **Sistemi IT:**
  Architettura Client-server, con gestione di rete con particolari punti critici (solo i server?)
- **Sistemi di controllo:**
  Gli stessi "client" sono dei "server" di dati critici e real-time distribuiti sulla rete (Controllori/DCS, PLC, SCADA/HMI, CNC, DNC, ecc.) ?

Perché la Sicurezza è diversa? /3

I requisiti di disponibilità sono diversi!

- **Sistemi IT:**
  attività nel normale orario di ufficio e possibilità di gestire fermate e/o “re-boot” per eventuali manutenzioni
- **Sistemi di controllo:**
  In molti casi sempre attivi 24/24h, 7/7gg in impianti a produzione continua o secondo turni e lotti di produzione. Fermare i sistemi non è possibile senza fermare la produzione!

Perché la Sicurezza è diversa? /4

Conseguenze a volte difficilmente prevedibili.

- **Sistemi IT:**
  In I.T. la conseguenza è la perdita di dati.
- **Sistemi di controllo:**
  Le conseguenze dipendono dal processo controllato. Tutte le funzioni devono essere verificate affinché non aggiungano vulnerabilità al sistema ed al processo (effetto Domino?).

Perché la Sicurezza è diversa? /5

Tempi critici per le interazioni.

- **Sistemi IT:**
  in situazioni di emergenza ci sono procedure per la salvaguardia dei dati, la chiusura delle applicazioni, lo shut down dei sistemi, …
- **Sistemi di controllo:**
  le reazioni in situazioni di emergenza devono essere rapide ed efficaci. Le informazioni critiche devono essere aggiornate sotto gli occhi degli operatori; a volte non c'è tempo per richiedere password per autenticazioni o autorizzazioni

Perché la Sicurezza è diversa? /6

I tempi di risposta richiesti ed il traffico di rete sono diversi.

- **Sistemi IT:**
  Il throughput e le prestazioni del sistema e della rete sono prevedibili e spesso non sono critiche.
- **Sistemi di controllo:**
  Non sono accettabili ritardi negli azionamenti, nella rilevazione dei dati da sensori e controllori. I "telegrammi" di dati e le elaborazioni sono brevi e frequenti. Spesso non è necessario un alto "throughput" della rete, ma è necessario garantire le prestazioni.

Perché la Sicurezza è diversa? /7

I software di sistema sono diversi.

- **Sistemi IT:**
  Software di sistema e sistemi operativi noti e collaudati per attività di gestione informatica
- **Sistemi di controllo:**
  I S.O. possono essere diversi, oppure sono gli stessi dei sistemi IT, ma usati in modo diverso: le regole abituali nel mondo IT spesso non sono praticabili.
  Che sistema operativo o che scheda di rete hanno un PLC o un DCS?
  Lo skill delle persone è diverso da personale I.T.

Perché la Sicurezza è diversa? /8

Limitazioni delle risorse Hardware e Software.

- **Sistemi IT:**
  I.T. definisce i requisiti hardware e software dei sistemi e gestisce manutenzione e aggiornamento, secondo regole e procedure di sicurezza informatica.
- **Sistemi di controllo:**
  Spesso hardware e software sono “speciali” e forniti insieme a tutto il sistema. Non si può aggiornare l’uno o l’altro secondo le richieste della sicurezza I.T.

Perché la Sicurezza è diversa? /9

Integrità di dati e informazioni.

- **Sistemi IT:**
  I dati sono sui server e difendibili con le “regole del R.I.D.” (Riservatezza, Integrità, Disponibilità)
- **Sistemi di controllo:**
  I dati e le informazioni arrivano direttamente da sensori, controllori e sottosistemi: la loro integrità è essenziale e spesso non controllabile.
  Necessitano precauzioni specifiche per eliminare eventuali fonti di corruzione dei dati e intrusioni.

Perché la Sicurezza è diversa? /10

Le comunicazioni sono diverse.

- **Sistemi IT:**
  I protocolli ed i mezzi di comunicazione sono di solito noti e legati a standard (TCP/IP, ecc)
- **Sistemi di controllo:**
  I protocolli ed i mezzi di comunicazione sono diversi, spesso proprietari o specifici per l'applicazione: reti tra PLC, DCS, CNC/DNC, comunicazioni seriali asincrone con RTU, ecc.

Perché la Sicurezza è diversa? /11

Aggiornamenti Software.

- **Sistemi IT:**
  I.T. aggiorna costantemente all'ultima release del software di sistema o applicativo per garantire la manutenibilità, le performance e la sicurezza
- **Sistemi di controllo:**
  Difficilmente si possono installare patch di software di sistema o applicativo: prima è necessario un **test accurato** di ogni componente per verificare impatti con gli altri componenti e moduli del sistema, verificare che non si infrangano regole di validazione, ….

Perché la Sicurezza è diversa?

Perché sono diversi:

- **I rischi**
- **L'architettura di rete**
- **I requisiti di disponibilità**
- **Le conseguenze (a volte difficilmente prevedibili)**
- **I tempi critici per le interazioni**
- **I tempi di risposta richiesti ed il traffico di rete**
- **I software di sistema**
- **La limitazioni delle risorse Hardware e Software.**
- **L' integrità di dati e informazioni.**
- **Le comunicazioni**
- **Gli aggiornamenti del Software.**

CPNI

- Center for the Protection on National Infrastructures
  - “CPNI is formed from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the **UK**'s Security Service), the National Security Advice Centre (NSAC)”
  - “Our advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services safer”

Some key differences between IT and SCADA/Process Control Security

Topic	Corporate IT	Process Control
Anti Virus	*Widely used*	*Often difficult/impossible to deploy*
Lifetime	*3-5 years*	*5-20 years*
Outsourcing	*Widely used*	*Rarely used for Operations*
Patching	*Frequent (daily?)*	*Slow (requires vendor approval)*
Change	*Frequent*	*Rare*
Time Critical	*Delays OK*	*Often safety dependent*
Availability	*Outages OK (overnight)*	*24/7/365 for years*
Security Skills & Awareness	*Pretty good*	*Poor*
Security Testing	*Widely used*	*Use with care!*
Physical Security	*Usually secure and manned*	*Often remote and unmanned*

However many of the protection measures used in standard IT security frameworks can be adapted and adopted for use in the process control & SCADA environments

Principali Errori

Perché gli errori?

- Le differenze tra la security dei sistemi IT e quella dei sistemi di supervisione e controllo sono molte, troppe, per essere trattate con le metodologie standard
- Gli errori che si commettono nell'implementazione di una policy di sicurezza sono molteplici e portano a delle vediamone almeno alcuni, quelli che vulnerabilità molto comuni

Policy di sicurezza assenti

- In qualche caso non esistono delle politiche di sicurezza chiare o, alle volte, pur esistendo, non sono seguite
- La security è comunque un ciclo che comprende la valutazione del rischio, la progettazione e l'implementazione di nuove contromisure in termini di policy e strumenti HW e SW, la loro convalida e, quindi, un nuova valutazione del rischio
- Questo ciclo deve essere sempre attivo, pena la perdita di efficacia delle contromisure

Poca consapevolezza sui problemi dell'impianto

- La cui prima ricaduta consiste nell'utilizzo di contromisure standard quando ne servirebbero di più appropriate

Documentazione della rete non sempre disponibile e aggiornata

- Naturalmente una documentazione accurata e una politica di gestione della configurazione sono di fondamentale importanza, insieme a dei piani di Business Continuity (possibilmente testati) e una politica chiara per la gestione della contingenza e delle ripartenze (Disaster Recovery)
- A tal proposito, vale l'esperienza americana maturata durante gli uragani del 2005 (Katrina e le sue sorelle), durante la quale si sono posti molti problemi per far ripartire correttamente i sistemi di controllo dei vari impianti danneggiati
- Un documento del Control Systems Security Center (CSSC, http://controlsystemssecurity.inl.gov) spiega molto bene come le configurazioni vadano annotate e controllate accuratamente, e come l'HW e SW utilizzato debba essere validato sia dal punto di vista del firmware, sia da quello delle policy di sicurezza prima di essere installato

Scarsa separazione tra la rete di controllo e quella aziendale

- Una segmentazione e segregazione non accurata è ancora uno degli errori più comuni
- Tra l'altro, il monitoraggio delle reti, cablate o wireless, dovrebbe essere un normale modo di procedere che, unito alla presenza di anti-malaware e di sistemi anti intrusione che verifichino gli accessi remoti, porterebbe un enorme vantaggio in termini di security globale

Controllo degli accessi non sempre praticati

- Spesso causata da sistemi operativi datati o comunque mal configurati
- Non essendo semplice mantenere aggiornate le Access Control List che indicano quali utenti/processi possono accedere a determinate risorse, spesso queste non vengono utilizzate correttamente
- Si tratta, in generale, di problemi legati alla scarsa manutenzione dei sistemi

Mancata registrazione di eventuali incidenti

- Questo è un errore molto comune, e lo si commette quando si pensa di utilizzare un IDS in maniera non supervisionata, cioè senza la presenza costante di un operatore
- Quest'ultimo, aiutandosi con una console opportuna, dovrebbe tener traccia di tutte le anomalie, registrarle e analizzarle, per poter prevenire future intrusioni aggiornando opportunamente l'IDS

Utilizzo di sistemi consumer come componenti di rete

- In realtà di dispositivi specificatamente progettati per l'ambiente industriale non ce ne sono moltissimi, specie quando di parla di sicurezza
- Certo è che quelli consumer, come detto anche in precedenza, hanno caratteristiche non sempre soddisfacenti
- Non solo, un HW troppo noto a livello mondiale espone a minacce derivanti dalla buona conoscenza delle sue vulnerabilità.

Normative per la Safety e la Security

Sicurezza?

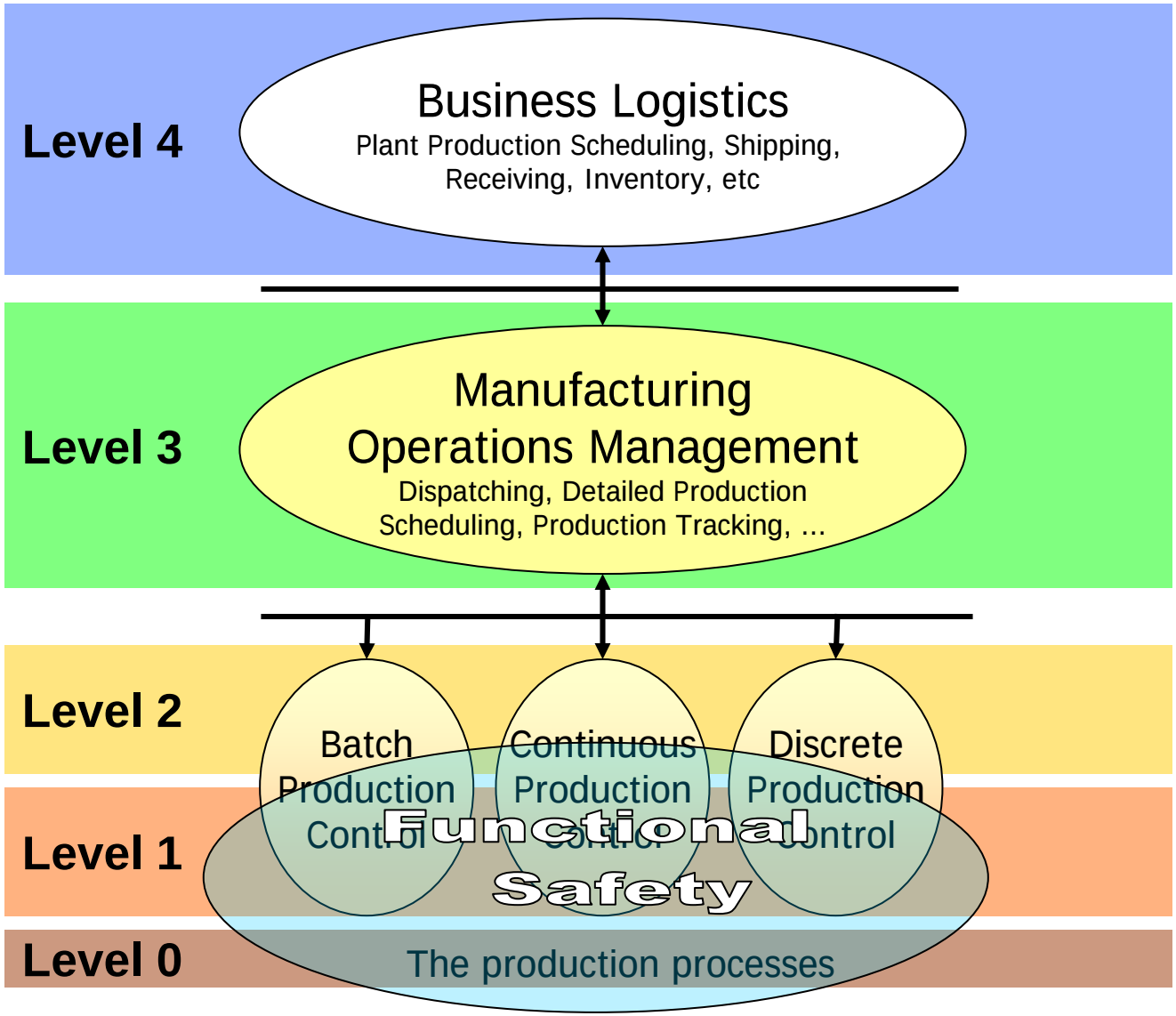
Organizzazioni

- ISO: International Organization for Standardization
- ISA: Instrumentation, Systems and Automation Society
- NIST: National Institute of Standards and Technology
- NERC: North American Electric Reliability Council
- CIDX: Chemical Industry Data Exchange
- IEEE: Institute of Electrical and Electronics Engineers
- IEC: International Electrotechnical Commission
- CIGRE': International Council on Large Electric Systems
- Department of Energy National SCADA Test Bed Program
- PCSF: Process Control System Cyber Security Forum

Passi iniziali

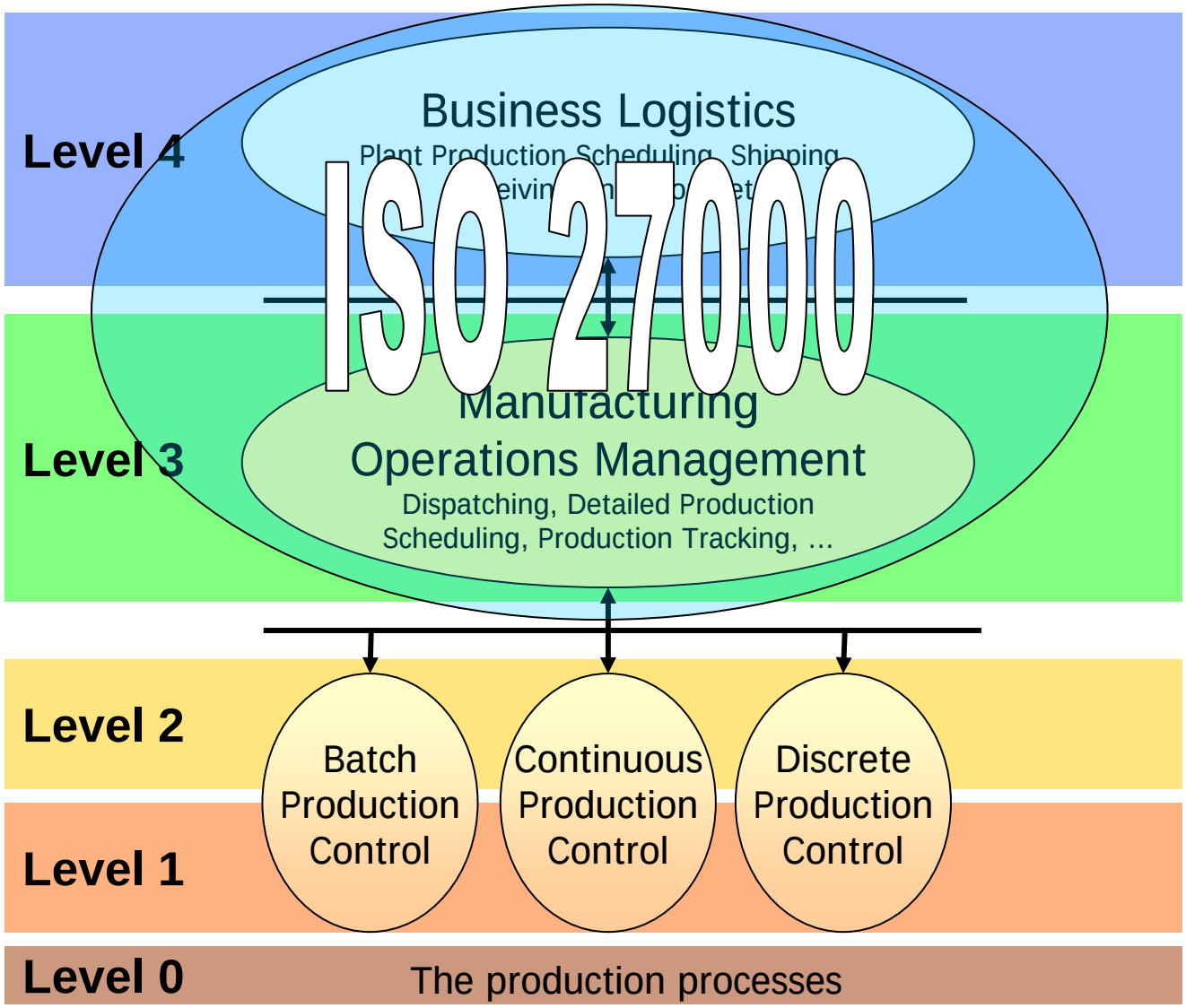
- "21 Steps to improve Cyber Security of SCADA Networks"
  (Ufficio di Presidenza degli USA)
- "Common vulnerabilities in critical infrastructure control systems"
  (U.S. Dept. Of Energy's National Nuclear Security Administration)
- Securing Process Control Systems - IT Security
  (Europarlamento)

ISA95 and Functional Safety



Area specificata nelle 61508 e 61511

ISA95 e ISO 27000



BS7799 – ISO 17799 - ISO27000

- A corporation applying it will have to perform a risk assessment, prepare its security resources, and prepare the needed elements for certification and compliance. These will include the corporate security policy, and the functional and assurance requirements that have to be implemented. The standard provides a generic list of these requirements at a high level, independently from specific technologies. A fundamental point is the provision of appropriate security policies. A policy should set the direction for action and the commitment of the company to information security. Remaining at the management level, the application of this standard to industrial installations, mainly one with potential critical consequences, seem to merit a review, or at least a complement with particular considerations on, for instance, timing issues related to control applications.

27001

- Management Responsibility
- Internal Audits
- ISMS (Information Security management System) Improvement
- Annex A - Control objectives and controls
- Annex B - OECD principles and this international standard
- Annex C - Correspondence between ISO 9001, ISO 14001 and this standard

27002

- Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Communications and Ops Management
- Access Control
- Information Systems Acquisition, Development, Maintenance
- Information Security Incident management
- Business Continuity
- Compliance

27003

- To provide help and guidance in implementing an ISMS
  1. Introduction
  2. Scope
  3. Terms & Definitions
  4. CSFs (Critical success factors)
  5. Guidance on process approach
  6. Guidance on using PDCA
  7. Guidance on Plan Processes
  8. Guidance on Do Processes
  9. Guidance on Check Processes
  10. Guidance on Act Processes
  11. Inter-Organization Co-operation

To be published

- 27004
  - Emerging standard covering information security management measurement and metrics
- 27005
  - Emerging standard covering information security risk management
- 27006
  - Guidelines for the accreditation of organizations which offer certification and registration with respect to an ISMS

ISO 15408 Common Criteria

- The Common Criteria are the result of long developments in the USA, Canada and European countries (the Netherlands, France, Germany, United Kingdom), and aimed at supporting the specification of products with security requirements. First published in 1996, its second version was adopted by ISO as standard 15408 in 1998.
- The requirements to be defined are functional requirements, those related to desired security behaviours, and assurance requirements, which are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.
- The standard gives the possibility to select among seven evaluation assurance levels, which can be used for grouping components, or provide retrofit compatibility with existing products (first 4 levels), or develop specialised components.
- This standard supports purchasers of products in the definition and formulation of the requirements they necessitate; vendors or developers in the specification of their products, and third party evaluators in the verification and validation of products. In this way, the whole procurement process is assisted with common terminology and procedures.

Common Criteria

- It is understandable that several approaches to the security of industrial control have taken the Common Criteria as reference. However it should be considered that this standard, although technically important, has not been heavily applied in the real world.
- Verifying technical products against a standard that comprises functional and assurance procedures is very costly. Some significant criticisms are that the evaluations don't seem to add value while entail notable costs, that it doesn't have a noteworthy impact on the reduction of vulnerabilities, that the engineering efforts could be better employed in other technical tasks related to security.
- As a consequence, we can say that the Common Criteria might mature into a useful framework for the development and procurements of security devices.
- Nevertheless, it will take time and will be dependent on the evolution of the standard in other fields. In addition, the more immediate needs of the electric power sector seem to lie in the system evaluation area – and this is not currently supported by the Common Criteria. These will have to evolve, incorporating new assurance requirements.

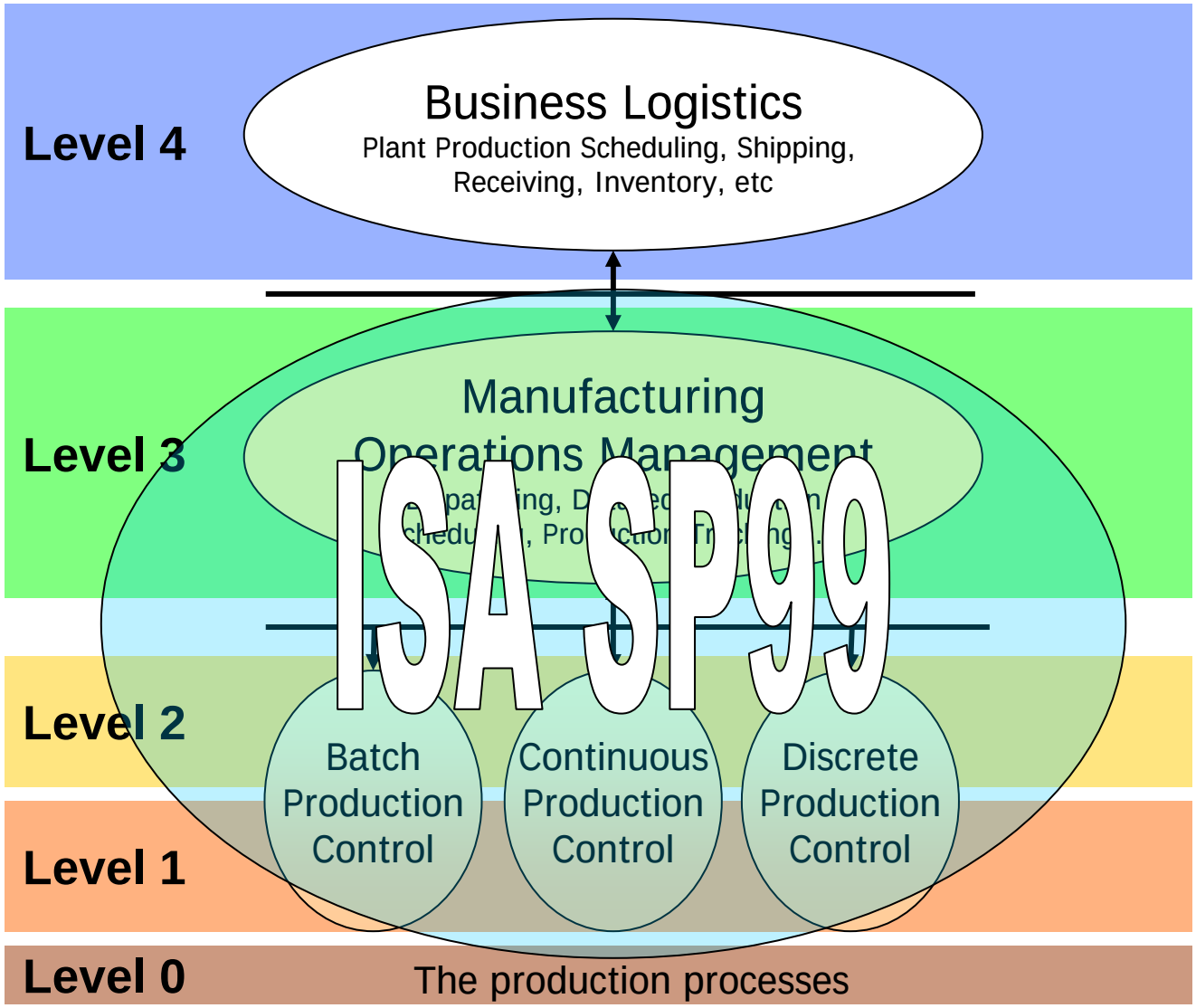
ISA SP99 Committee

La Security in ambito industriale

ISA SP99

- Manufacturing and Control Systems Security
- Two Technical Reports Published
  - ISA TR99.00.01
  - ISA TR99.00.02
  - Currently Available @ http://www.isa.org/securitystandards
- Standards al ballottaggio
  - ISA S99.00.01 – Models, Definitions, and Terminology
  - ISA S99.00.02 – Establishing a Manufacturing and Control System Security Program
- Proposte
  - ISA S99.00.03 – Operating a Manufacturing and Control Systems Security Program
  - ISA S99.00.04 – Specific Security Requirements for Manufacturing and Control Systems

ISA95 e ISA SP99



TR99.00.01

- ANSI/ISA-TR99.00.01-2004
  - *Security Technologies for Manufacturing and Control Systems*
  - Fornisce una valutazione e un assessment delle tecnologie correnti di sicurezza elettronica e dei vari tool per il manufactoring e l'ambiente dei sistemi di controllo (includendo lo sviluppo, l'implementazione, l'operatività e la manutenzione)
- In altre parole il TR identifica e valuta le tecnologie correnti e come possono essere usate nei Sistemi di Controllo

TR99.00.01 Purpose (continued)

- Ogni tecnologia è discussa in termini di:
  - Security Vulnerabilities Addressed by this Technology
  - Typical Deployment
  - Known Issues and Weaknesses
  - Assessment of Use in the Manufacturing and Control Systems Environment
  - Future Directions
  - Recommendations and Guidance
  - References”

TR99.00.01 - Technology Areas

- Authentication and Authorization
- Filtering/Blocking/Access Control
- Encryption and Data Validation
- Audit, Measurement, Monitoring and Detection Tools
- Operating Systems
- Physical Security

TR99.00.01 Authentication and Authorization

- Role Based Authorization Tools
- Password Authentication
- Challenge Response Authentication
- Physical/Token Authentication
- Smart Card Authentication
- Biometric Authentication
- Location Based Authentication
- Password Distribution and Management Technologies
- Device to Device Authentication

TR99.00.01 Filtering/Blocking/Access Control

- Dedicated Firewalls (Hardware Based)
- Host-based Firewalls (Software Based)
- Virtual Local Area Networks (VLANs)

TR99.00.01 Encryption Technologies and Data Validation

- Symmetric (Private) Key Encryption
- Public Key Encryption and Key Distribution
- Virtual Private Networks (VPNs)
- Digital Certificates

TR99.00.01 Audit, Measurement, and Monitoring and Detection Tools

- Log Auditing Utilities
- Virus/Malicious Code Detection
- Intrusion Detection Systems
- Network Vulnerability Scanners
- Network Forensics and Analysis Tools
- Host Configuration Management Tools
- Automated Software Management Tools

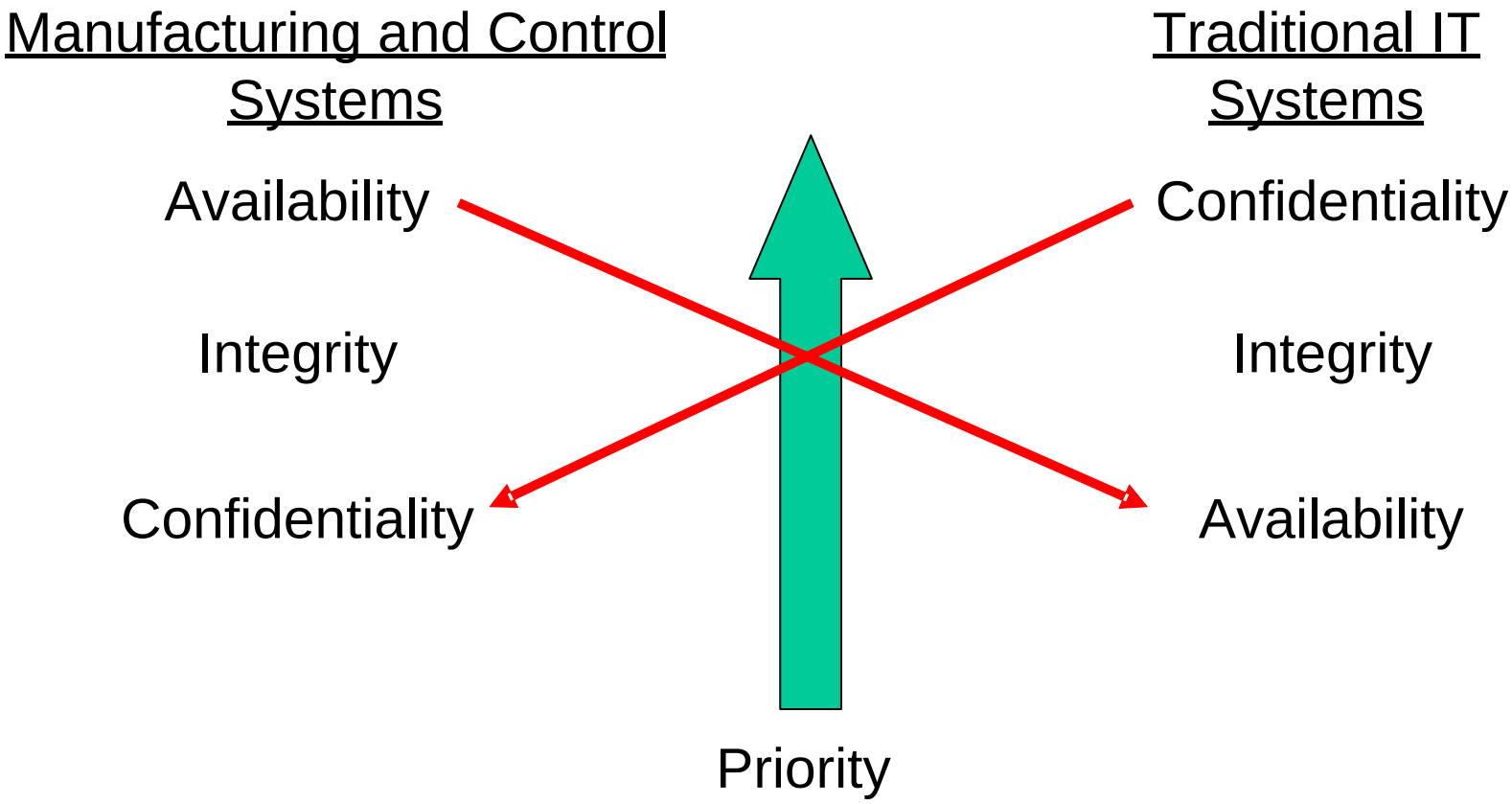
TR99.00.01 Computer Software

- Server and Workstation Operating Systems
- Real-time and Embedded Operating Systems
- Web and Internet Technologies

TR99.00.01 Physical Security Controls

- Physical Protection
- Personnel Security

ISA-TR99.00.01
Comparison of Objectives



ISA SP99

- ANSI/ISA-TR99.00.02-2004
  - *Integrating Electronic Security into the Manufacturing and Control Systems Environment*
  - Fornisce un framework per lo sviluppo di un programma di sicurezza elettronica e raccomanda una particolare organizzazione e struttura del piano di sicurezza.
  - L'informativa indica dettagliatamente quali elementi minimi includere e come, sia a livello di sito, sia a livello di entità.

SP99 TR99.00.02

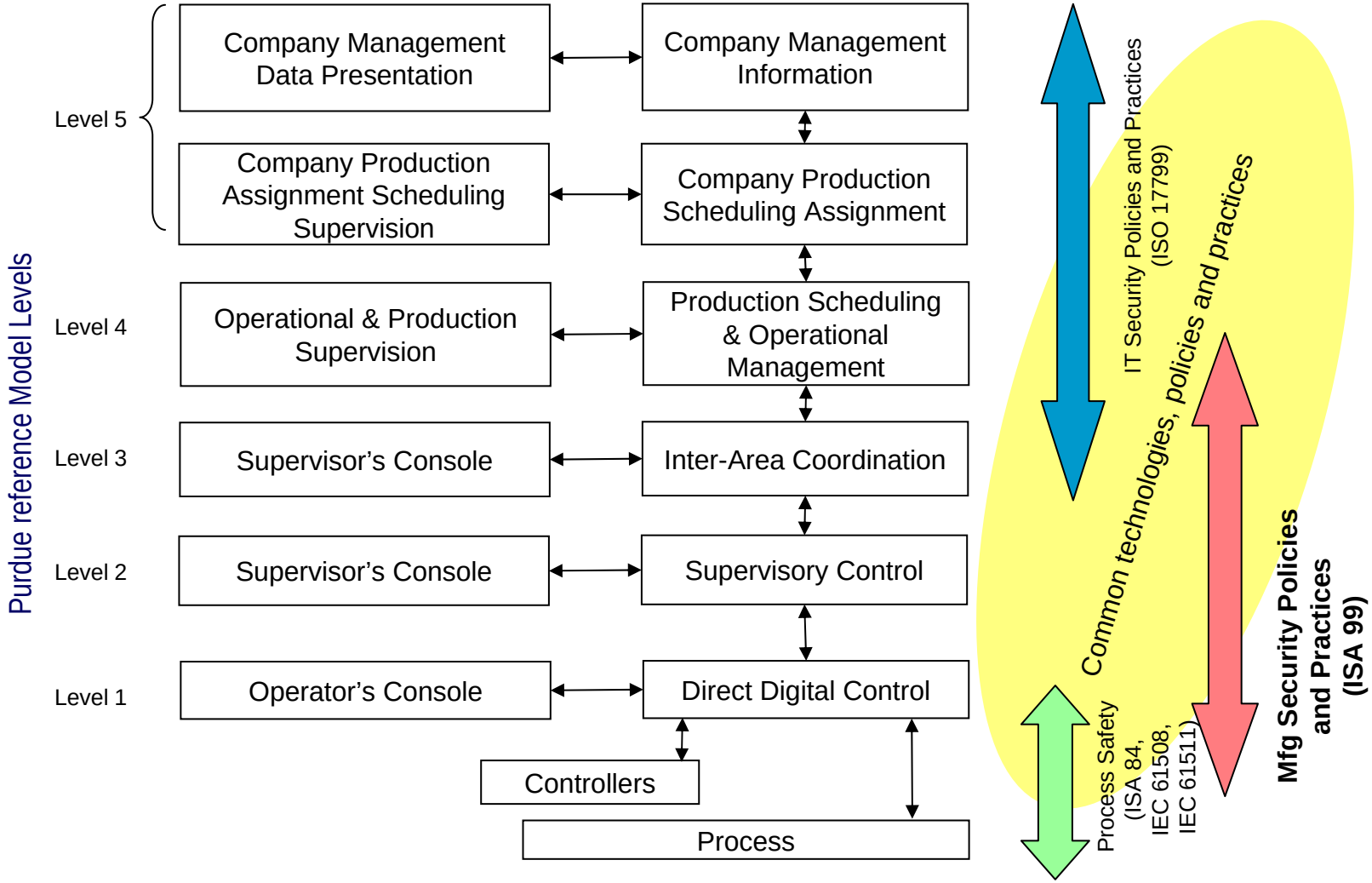
Art. 6.5

Special Considerations for Manufacturing and Control Systems

Manufacturing and Control System electronic security plans and programs are **consistent with**, and build on, **existing IT security** experience, programs, and practices. **However**, there are critical operational differences between IT and Manufacturing and Control Systems that influence how **specific measures** should be applied. (……).

Riassumendo i Security Standards

Scope of Security Standards



Altri Standard

GAMP

- Fondato da un gruppo di industrie farmaceutiche inglesi nel 1991 (**U.K. Pharmaceutical Industry Computer Systems Validation Forum**) stabilisce delle linee guida per lo sviluppo di sistemi automatizzati
- Nel 1994, GAMP in collaborazione con ISPE pubblica le prime GAMP guidelines
- Le GAMP diventano velocemente influenti in tutta Europa in quanto riconosciute come prodotto di qualità
- Nel 2000 è fondata GAMP America
- Sempre nel 2000 GAMP diventa formalmente un sub-comitato dell'ISPE
- All'aumentare dell'esperienza lo scope dell'organizzazione si è ampliato fino ad includere le aree precliniche e cliniche

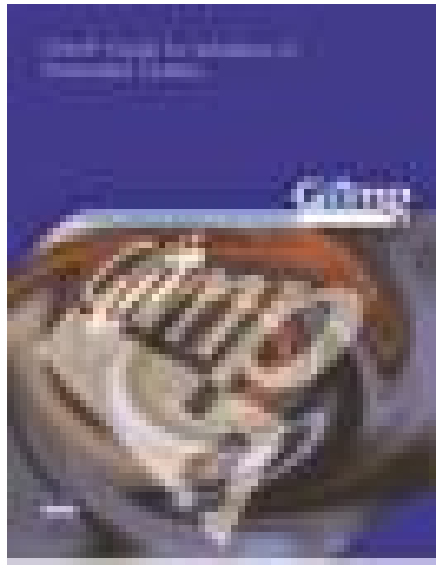
GAMP 4 e Security

La versione 4 del documento menziona in diversi punti la sicurezza (delle informazioni e delle persone) per gli "Automated System"

Appendix 03 ➡ **Guideline for Automated System Security**: come rendere sicuro un sistema da utilizzare in produzioni GxP.

1- Introduzione

- La linea guida descrive le misure da implementare perchè dati e sistemi automatizzati in ambiente regolamentato GxP siano protetti da incidenti dolosi o accidentali, accessi non autorizzati.
  - controllo continuo
  - integrità
  - disponibilità
  - riservatezza dei dati



2 - Ambito

- Si applica a tutti i sistemi automatizzati utilizzati in ambiente GxP e lo scopo include hardware, software, infrastruttura e dati memorizzati elettronicamente
- I controlli di sicurezza descritti includono sia mezzi elettronici che fisici.

3 - Responsabilità

- **Direzione** (User Company Management):
  - nomina un responsabile del sistema (System Owner) e si occuperà di analizzare gli eventuali incidenti e le azioni correttive richieste
- **Responsabile di sistema** (System Owner):
  - responsabile ultimo del sistema e dei dati gestiti. Si deve occupare della sicurezza del suo sistema (i requisiti da specificare, come vengono implementati e mantenuti, ecc.)
- **Gestore della piattaforma** (Platform Owner):
  - i sistemi consistono in software applicativo, eseguito su piattaforma hardware con sistemi operativi. Questa persona è responsabile dell'operatività quotidiana della piattaforma e della sua sicurezza
- **Utilizzatore** (End-user):
  - colui che utilizza il sistema, responsabile che la sicurezza sia mantenuta nella normale operatività del sistema automatizzato.

4 - Principi

- **Classificazione dei sistemi**
  - Il responsabile del sistema deve assicurarsi che il sistema venga classificato secondo la natura dei dati e dei record gestiti.

- **Consapevolezza degli utenti**
  - La Direzione deve assicurare attraverso un programma di formazione che tutti i collaboratori siano consapevoli della sicurezza ai quali sottoporre i sistemi automatizzati, e che le loro attività vengano monitorate.

Gestione degli incidenti

- Tutti gli incidenti di sicurezza devono essere riportati al responsabile del sistema ed al gestore della piattaforma.
- Incidenti gravi devono essere segnalati alla Direzione.
- Gli incidenti devono essere docum analizzati per determinare le mina

Politiche per la sicurezza delle informazioni

- L'organizzazione deve sviluppare politiche e procedure adeguate per l'accesso e la gestione dei sistemi. Tra gli argomenti da affrontare troviamo:
  - ✓ sicurezza fisica
  - ✓ accesso sicuro ai sistemi (id + password, ecc.)
  - ✓ sistemi di posta elettronica
  - ✓ risorse di rete condivise
  - ✓ accesso ad internet
  - ✓ uso di PC portatili
  - ✓ licenze software (acquisto ed installazione)
  - ✓ sistemi automatizzati esterni

5 – Requisiti del sistema e responsabilità

- **Requisiti operativi**
  - operatività e supporto organizzati
  - separazione tra ambienti di sviluppo, test, convalida e produzione
  - antivirus aggiornati su PC, server in rete, gateway
  - verifica di tutti i software installati

- **Requisiti per le comunicazioni**
  - controlli della sicurezza dei dati e crittografia
  - valutazione connessioni esterne a reti ecc.
  - verifica accessi dall'esterno con log dedicati
  - controllo degli scambi di dati con l'esterno
  - valutazione rischi di accesso da parte di terze parti

- **Requisiti per la sicurezza fisica ed ambientale**
  - proteggere fisicamente da accessi non autorizzati
  - proteggere le copie dei dati creati dai sistemi
  - controllare i media rimuovibili utilizzati

- **Requisiti per l'efficacia della sicurezza**
  - test periodici su piattaforma, sistemi ed applicazioni per verificare l'efficacia dei controlli di sicurezza
  - test di sicurezza e di penetrazione effettuato regolarmente da parte di personale specializzato

Requisiti per il controllo accessi

- proteggere sistemi e piattaforma con controllo accessi
- proteggere i dati personali secondo legge
- controllare l'accesso ai dati regolamentati
- controllo accessi (id e password)
- controllo utenti registrati che hanno accesso al sistema con procedure e registrazioni scritte
- controllo periodico delle liste utenti con accesso ai sistemi
- gestione controllata delle password
- screen saver automatico con password
- password cambiata regolarmente e formata da caratteri alfanumerici e di lunghezza minima

Requisiti per il monitoraggio del sistema

- log di sistema con data, ora e id che includa: accessi, variazioni sui record e parametri di sistema
- Audit Trail con data, ora, operatore, azioni e variazioni effettuate
- controllo regolare di log e audit trail
- protezione log e audit trail

Requisiti per la continuità di funzionamento

- analisi del rischio documentata all'inizio dello sviluppo
- backup dei record elettronici regolamentati
- protezione delle copie di back-up in luogo diverso
- verificare regolarmente le copie di backup
- stilare un piano per la gestione di emergenze

NIST

- NIST PCSRF (**Process Control Security Requirements Forum**)
  - Applicazione dei Common Criteria allo sviluppo dei criteri di sicurezza dei sistemi di controllo industriali
  - Draft: “System protection Profile for Industrial Control Systems”
    - designed to present a cohesive, cross-industry, baseline set of security requirements for new industrial control systems, is available for download and review. The SPP-ICS is designed to be an industry voice to the industrial control system vendors and system integrators, defining the security capabilities that are desired in new products and systems.

MS-ISAC

- Multi-State Information Sharing and Analysis Cente
  - **Cyber Security Procurement Language for Control Systems**

Electric Power

- IEEE 1402 “IEEE Guide for Electric Power Substation Physical and Electronic Security”
- IEEE Std C37.1-1994 – “IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control” (currently under revision)
- IEC 62210 “Initial Report from IEC TC 57 ad-hoc WG06 on Data and Communication Security”
- IEC 62351 “Data and Communication Security”
- IEC/EN 61508 “Functional safety of electrical/ electronic/programmable electronic safety-related systems”
- IEC 61443 “Security for Industrial Process Measurement and Control”.
- NERC 1200 “Urgent Action Standard 1200 – Cyber Security”
- NERC 1300 “Cyber Security,” also known as CIP-002-1 through CIP-009-1 - updated
- NERC Security Guidelines “Security Guidelines for the Electricity Sector”
- FERC SSEMP “Security Standards for Electric Market Participants (SSEMP).”

Oil and Gas

- API 1164 “SCADA Security”
- API “Security Guidance for the Petroleum Industry”
- API “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries”
- AGA Report No. 12 Part 1 “Cryptographic Protection of SCADA Communications Background, Policies & Test Plan”
- AGA Report No. 12 Part 2 “Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications”
- AGA Report No. 12 Part 3 “Cryptographic Protection of SCADA Communications: Protection of Networked Systems”
- AGA Report No. 12 Part 4 “Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components.”

NISCC (National Infrastructure Security Co-ordination Center)
CPNI (Center for the Protection of National Infrastructures)

Good Practice Guide

Process Control and SCADA Security

Schema

- 1 *Introduction*
- *2 Securing Process Controll and Data Systems*
- *3 Understand Bussiness Risk*
- *4 Impement Secure Architecture*
- *5 Establish Responce Capabilities*
- *6 Improve Awareness and Skills*
- *7 manage Third Part Risk*
- *8 Engage Projects*
- *9 Establish Ongoing Governance*

3 Understand Bussiness Risk

- To gain a thorough understanding of the risk confronting the business from threats to process control systems in order to identify and drive the appropriate level of security protection required.
  - ***Understand the system***
  - ***Understand the threats***
  - ***Understand the impacts***
  - ***Understand the vulnerabilities***

4 Implement Secure Architecture

- To implement technical and associated procedural security protection measures, commensurate to the business risk, that will provide a secure operating environment for the process control systems

- ☑ ***Network Architecture***
- ☑ ***Firewalls***
- ☑ ***Remote access***
- ☑ ***Anti-virus***
- ☑ ***E-mail and Internet Access***
- ☑ ***System hardening***
- ☑ **Backups and recovery**
- ☑ **Physical security**
- ☑ **System monitoring**
- ☑ **Wireless networking**
- ☑ **Security patching**
- ☑ **Personnel background checks**
- ☑ **Passwords & accounts**
- ☑ **Document security framework**
- ☑ **Security scanning**
- ☑ **Starters and leavers process**
- ☑ **Management of change**
- ☑ **Security testing**
- ☑ **Device connection procedures**

5 Establish Responce Capabilities

- To establish procedures necessary to monitor, evaluate and take appropriate action in response to a variety of electronic security events.

6 Improve Awareness and Skills

- To increase process control security awareness throughout the organisation and to ensure that all personnel have the appropriate knowledge and skills required to fulfill their role.
  - ***Increase awareness***
  - ***Establish training frameworks***
  - ***Develop working relationship***

7 Manage Third Part Rissk

- To ensure that all security risks from vendors, support organisations and other third parties are managed.
  - ***Identify third parties***
  - ***Manage risk from vendors***
  - ***Manage risk from support organisations***
  - ***Manage risk in the supply chain***

8 Engage Projects

- To ensure that all projects and initiatives that may impact the process control systems are identified early in their life cycle and include, appropriate security measures in their design and specification.

9 Establish Ongoing Governance

- To provide clear direction for the management of process control system security risks and ensure ongoing compliance and review of the policy and standards
  - ***Define roles and responsibilities***
  - ***Develop policy and standards***
  - ***Ensure compliance with policy and standards***
  - ***Update policy and standards***

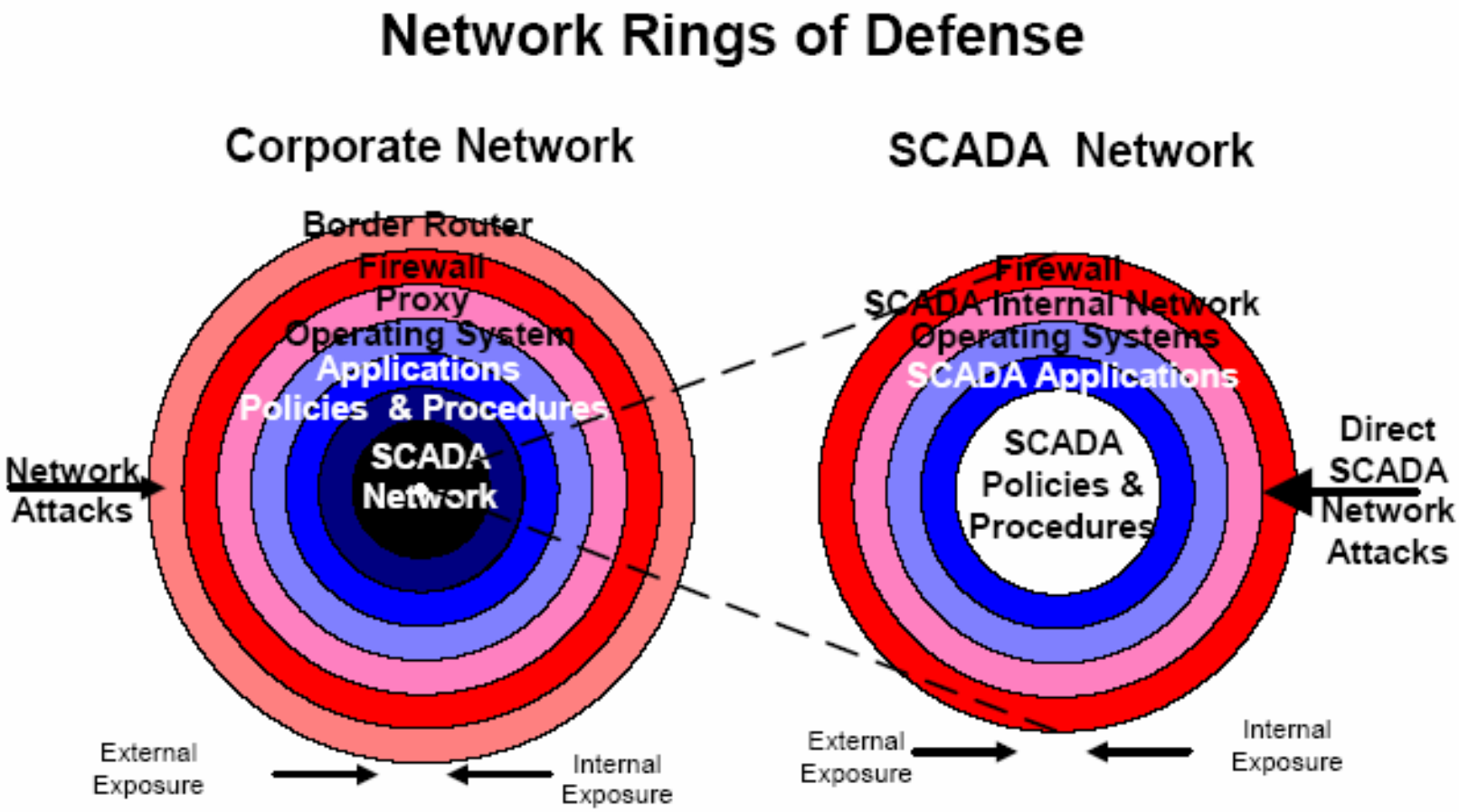
Sugli Standard

Standard

- Gli standard possono aiutare la protezione dei sistemi SCADA in molti modi:
  - Aiutando a stabilire una base concettuale comune tra tutti gli stakeholders: operatori, vendors, certificatori, autorità, etc.
  - Supportando i processi ingegneristici: dalla specifica all'acquisto, dall'operatività alla manutenzione
  - Incoraggiando lo sviluppo di un mercato di prodotti e servizi per la sicurezza con livelli di affidabilità verificabili
- Purtroppo, c'è un gap temporale tra la disponibilità degli standard e la loro applicazione. Gli sforzi attuali per gli standard SCADA sono troppo recenti per essere sicuri della loro efficacia.
- Nel frattempo, molti settori continueranno a sviluppare i propri sistemi lasciando molte opportunità a cyber-attacchi e failures vari

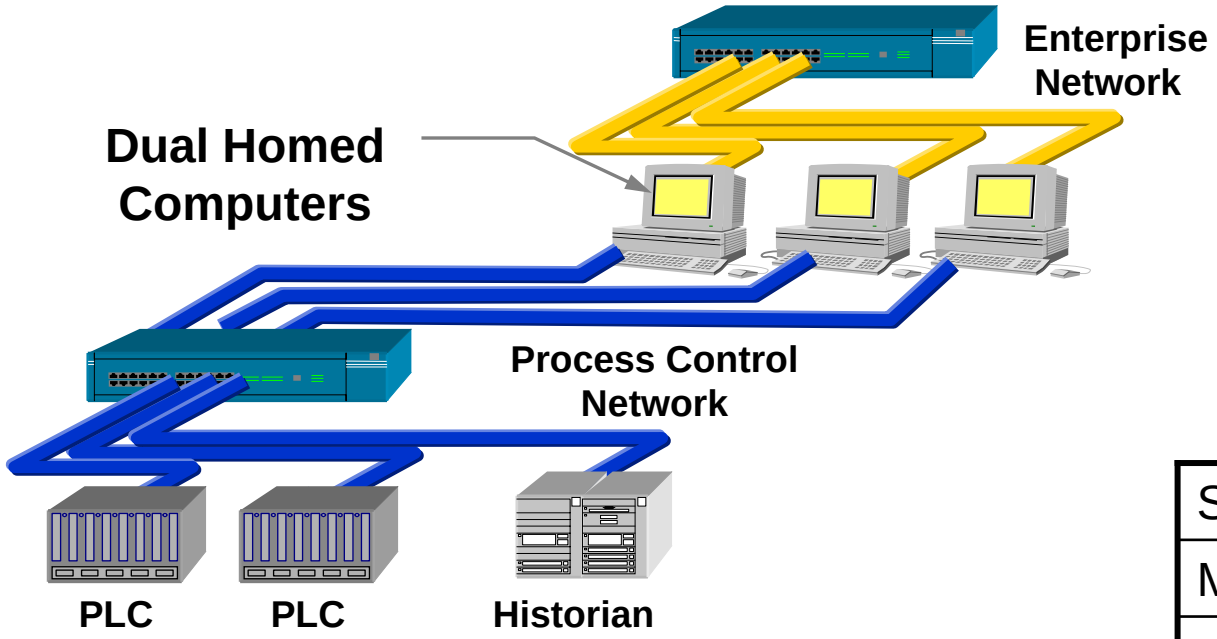
Approcci alla protezione

Segregazione reti



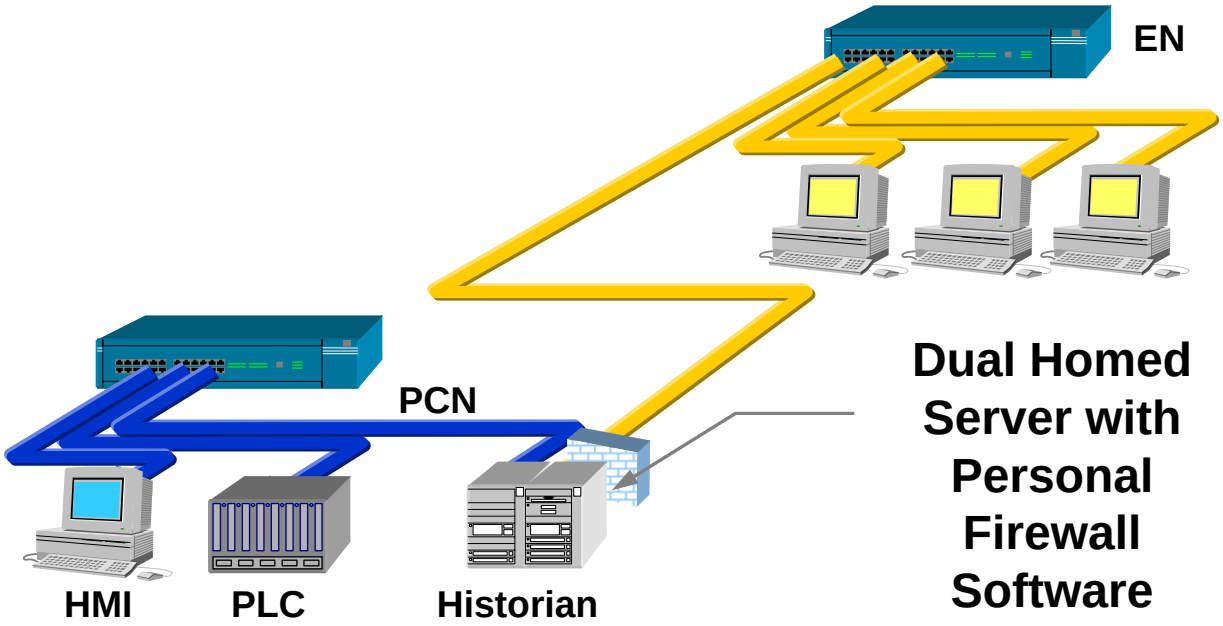
"Rings of Defense" for Corporate and SCADA Networks – www.dyonyx.com

#1 Dual Homed Servers/Workstations



Security	1
Manageability	2.5
Scalability	1

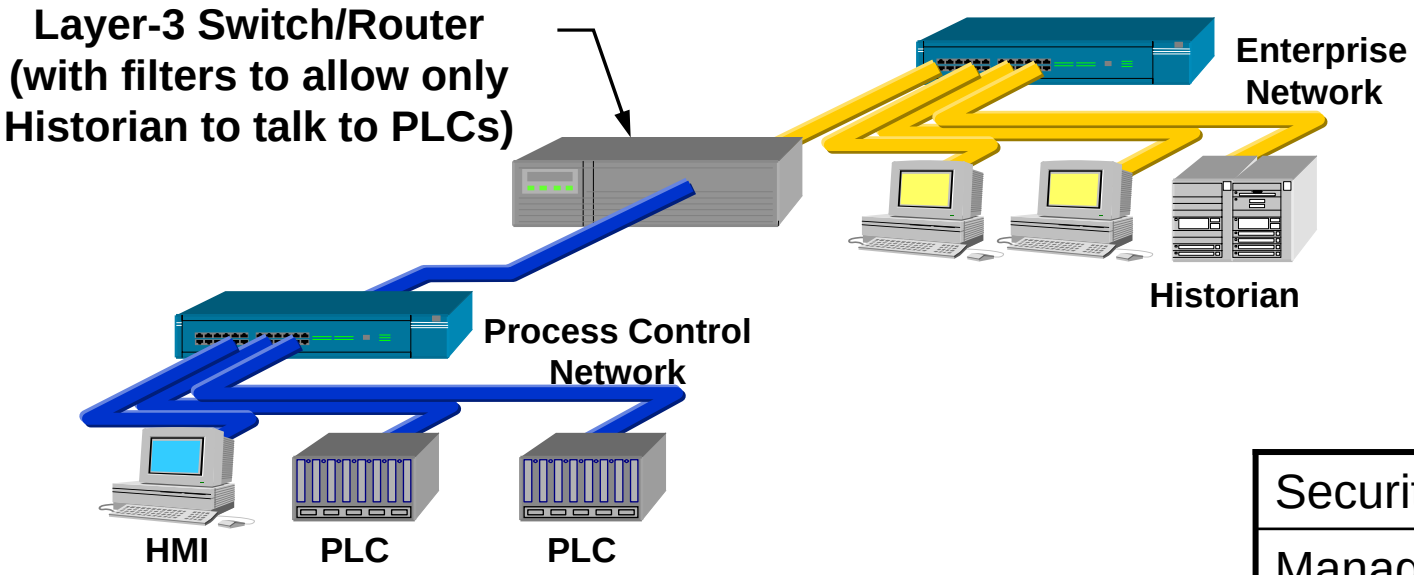
#2 Dual-Homed Server with Personal Firewall Software



Dual Homed Server with Personal Firewall Software

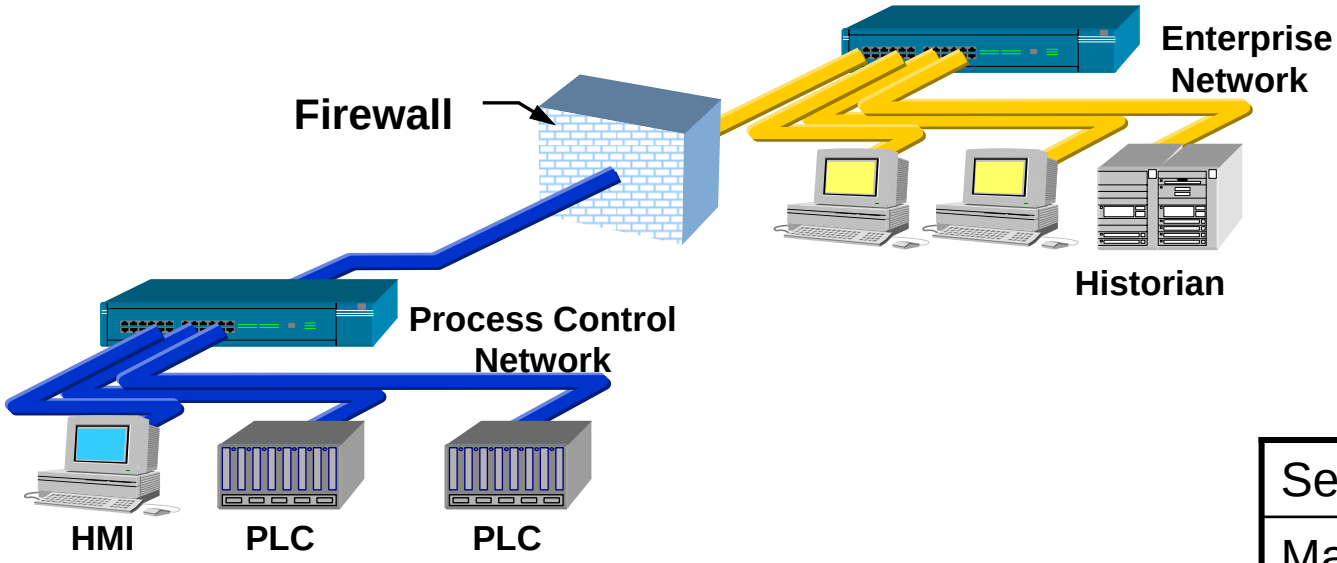
Security	2
Manageability	1
Scalability	1

#3 Router/Layer-3 Switch



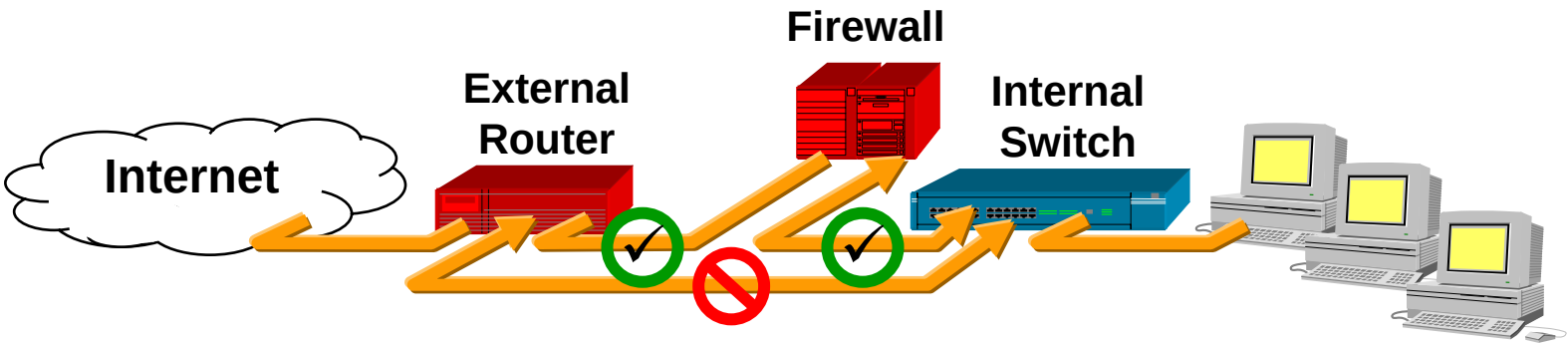
Security	2
Manageability	2
Scalability	4

#4 Single Two-Port Firewall



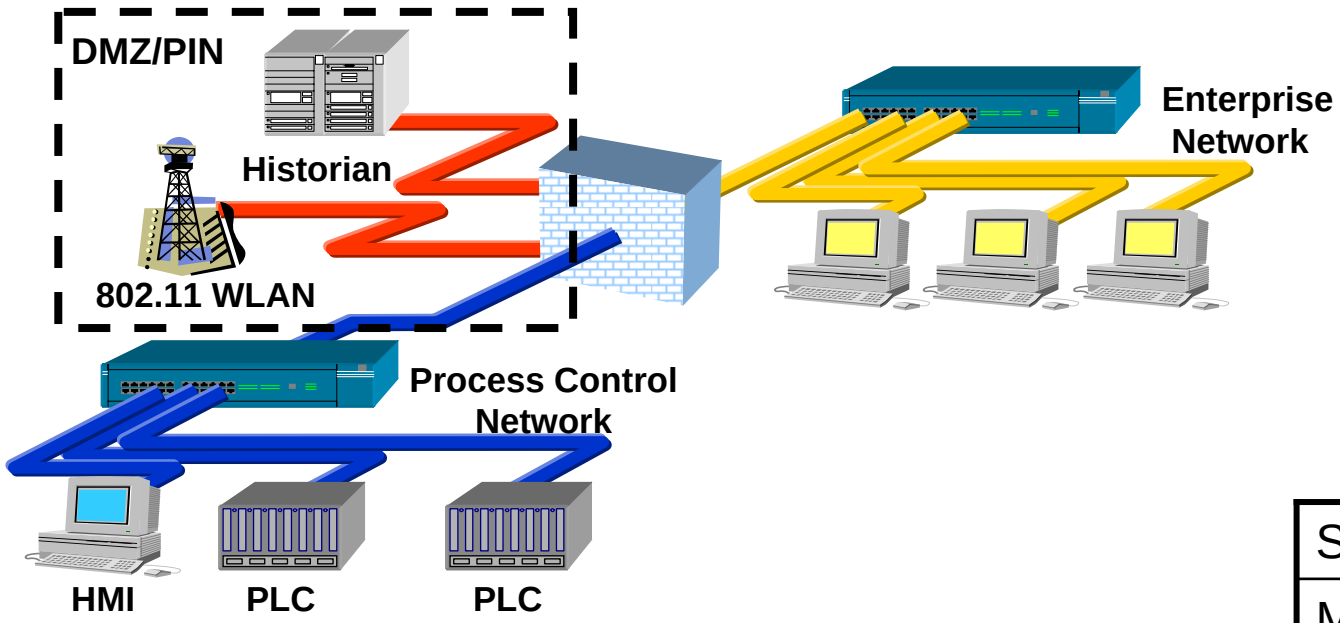
Security	3
Manageability	5
Scalability	4

#5 Router/Firewall Combination



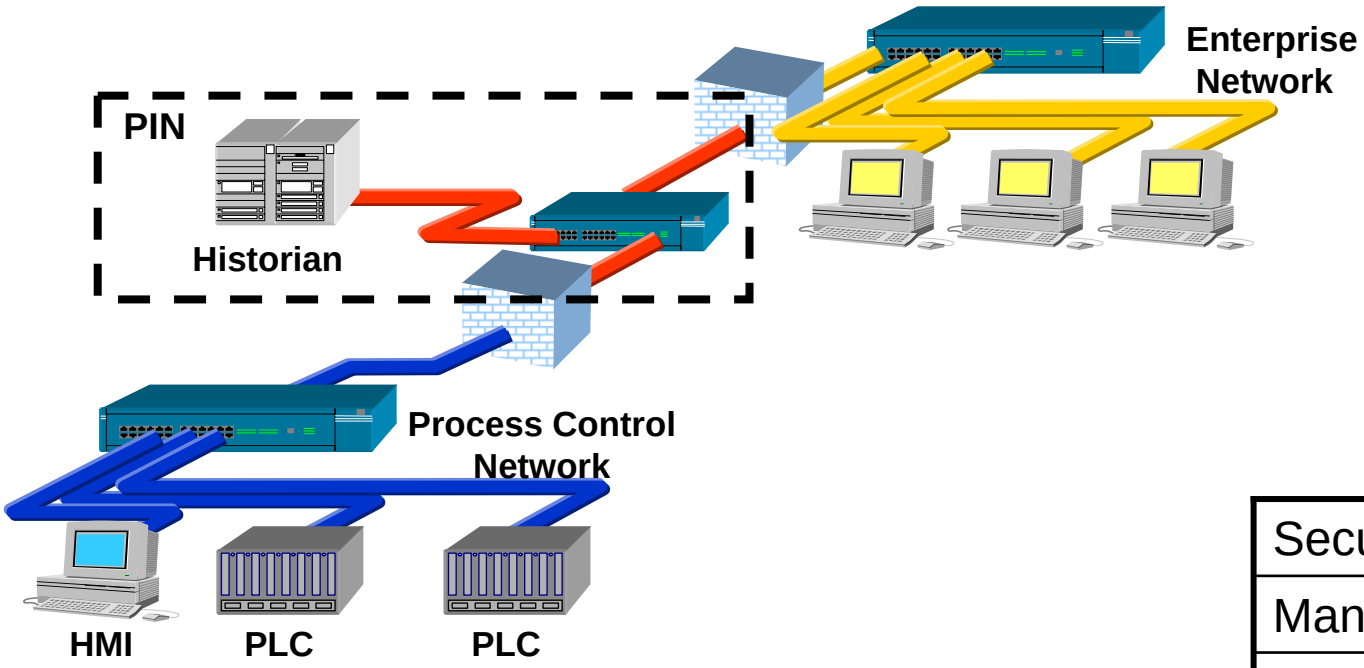
Security	3.5
Manageability	3
Scalability	4

#6 Firewalls with DMZ



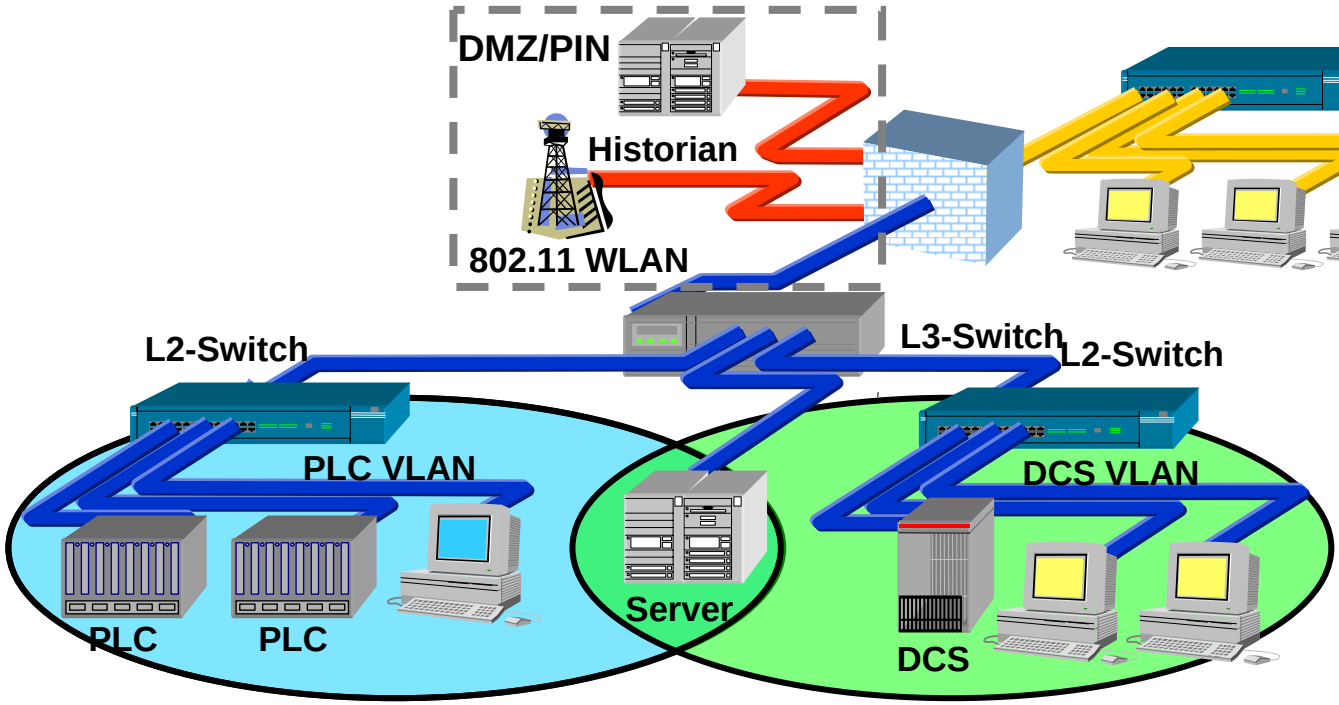
Security	4
Manageability	4.5
Scalability	4

#7 Paired Firewalls



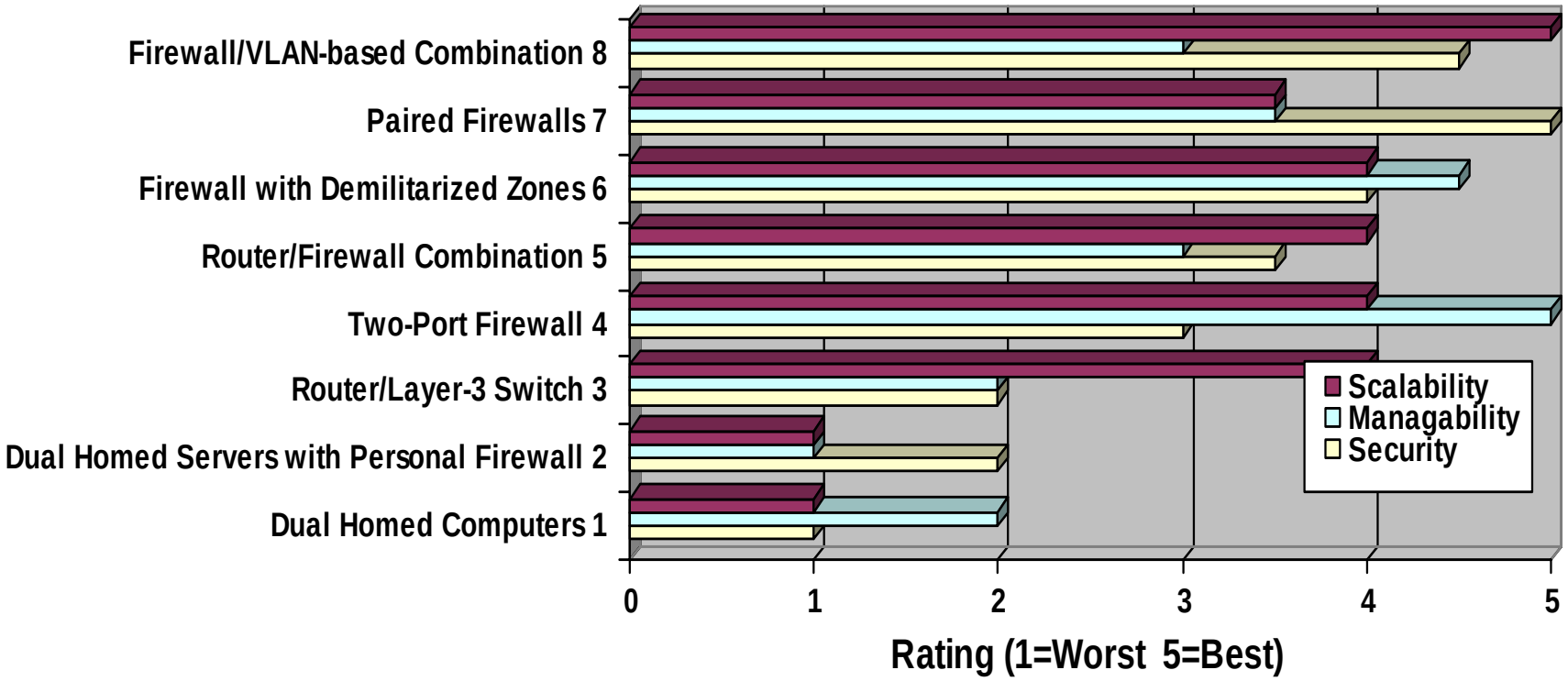
Security	5
Manageability	3
Scalability	3.5

#8 Firewall / VLAN-based Combinations

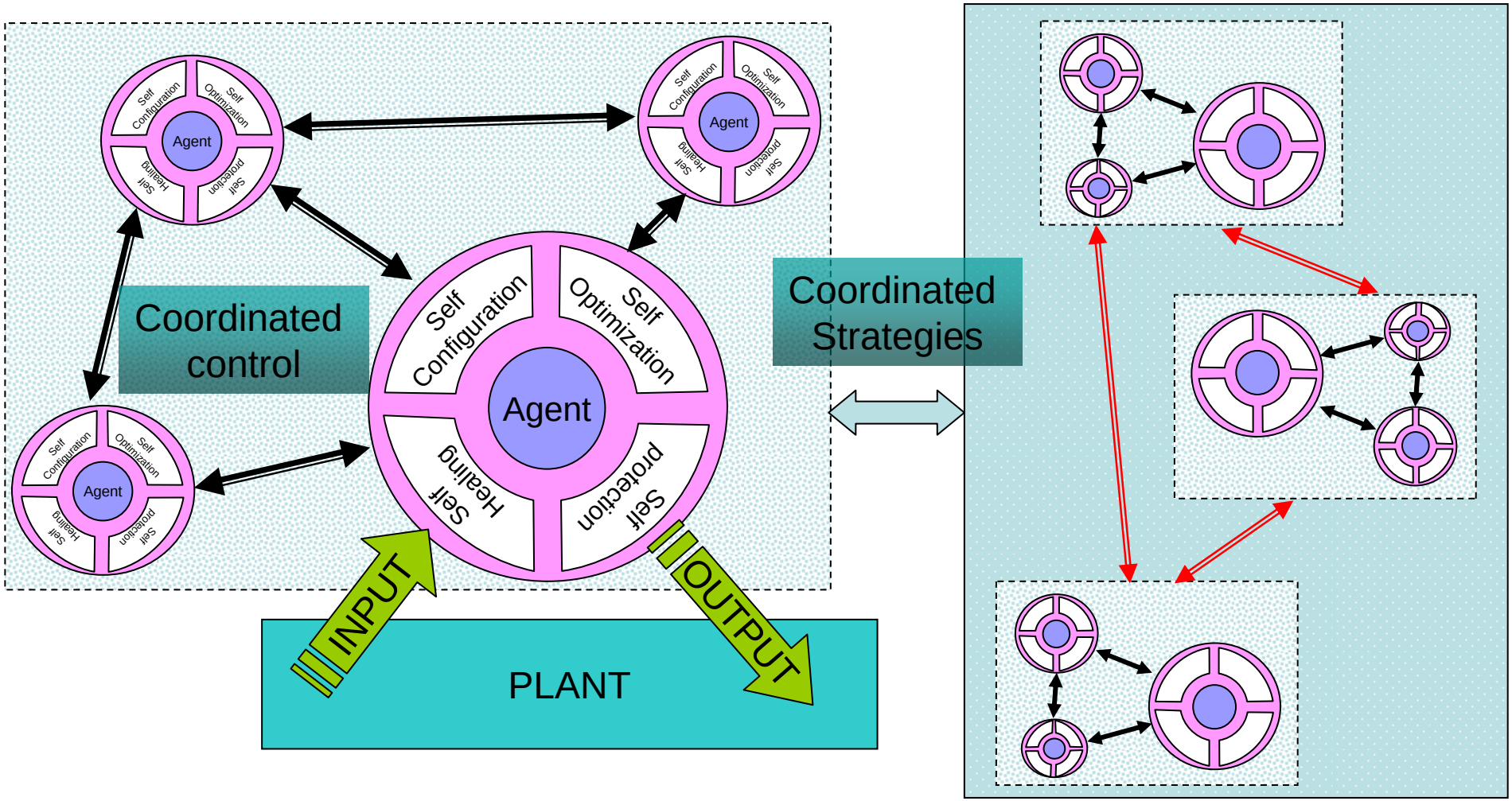


Security	4.5
Manageability	3
Scalability	5

The Ratings


Firewall/VLAN-based Combination 8
Paired Firewalls 7
Firewall with Demilitarized Zones 6
Router/Firewall Combination 5
Two-Port Firewall 4
Router/Layer-3 Switch 3
Dual Homed Servers with Personal Firewall 2
Dual Homed Computers 1
Scalability
Managability
Security
0
1
2
3
4
5
Rating (1=Worst 5=Best)

Agenti Autonomi



Cosa fare: metodi ed analisi ad hoc

- **Assessment**: verifica congruità di sistemi, rete, infrastruttura
- Test di **vulnerabilità**
- Analisi e valutazione dei **rischi**: vulnerabilità, minacce, incidenti e danni potenziali
- **Policy** di Security e di risposta ad incidenti
- **Business Continuity** & **Disaster Recovery** Plan
- **Protezione**
- **Monitoraggio**
- **Audit**
- **Riesame** periodico