MCIPLab.it

ROMA TRE UNIVERSITÀ DEGLI STUDI

Il Problema della Cyber Security nei Sistemi di Controllo: L'Approccio Strutturato degli Standard

Chiara Foglietta

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Email: chiara.foglietta@uniroma3.it

Evento: Gestione del Rischio in Sistemi Interdipendenti: la Problematica Cyber-Fisica

Data: 29 ottobre 2019

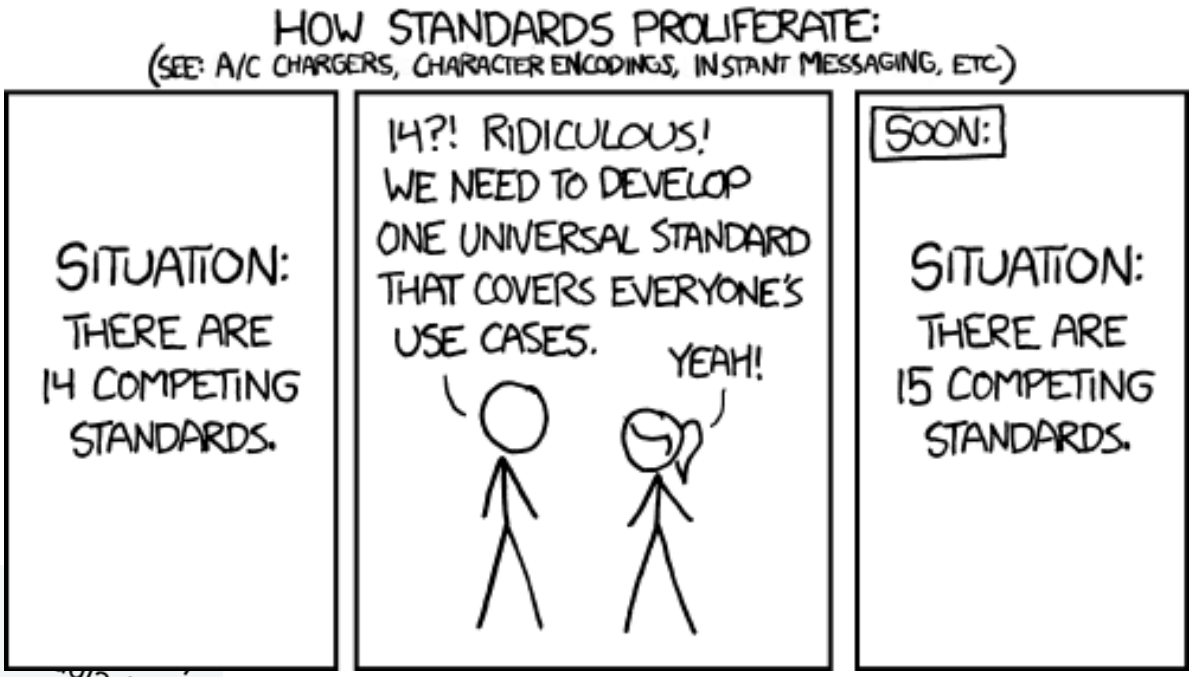
Operational vs. Information Technology

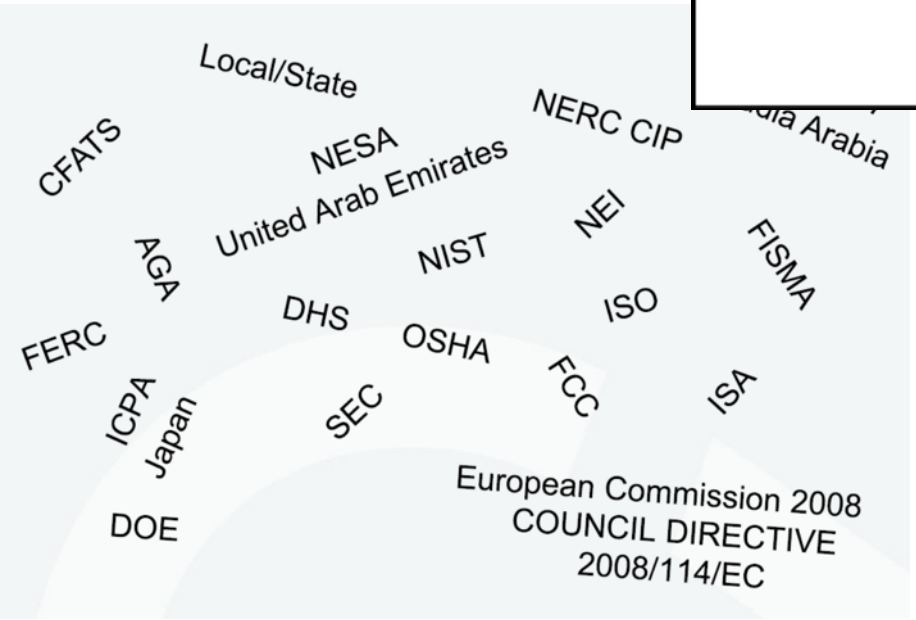
	Industrial Systems	Office IT
Protection target for security	Production resources, incl. logistics	IT- Infrastructure
Component Lifetime	Up to 20 years	3-5 years
Availability requirement	Very high	Medium, delays accepted
Real time requirement	Can be critical	Delays accepted
Physical Security	Very much varying	High (for IT Service Centers)
Application of patches	Slow / restricted by regulation	Regular / scheduled
Anti-virus	Uncommon, hard to deploy, white listing	Common / widely used
Security testing / audit	Increasing	Scheduled and mandated

Reti di Campo

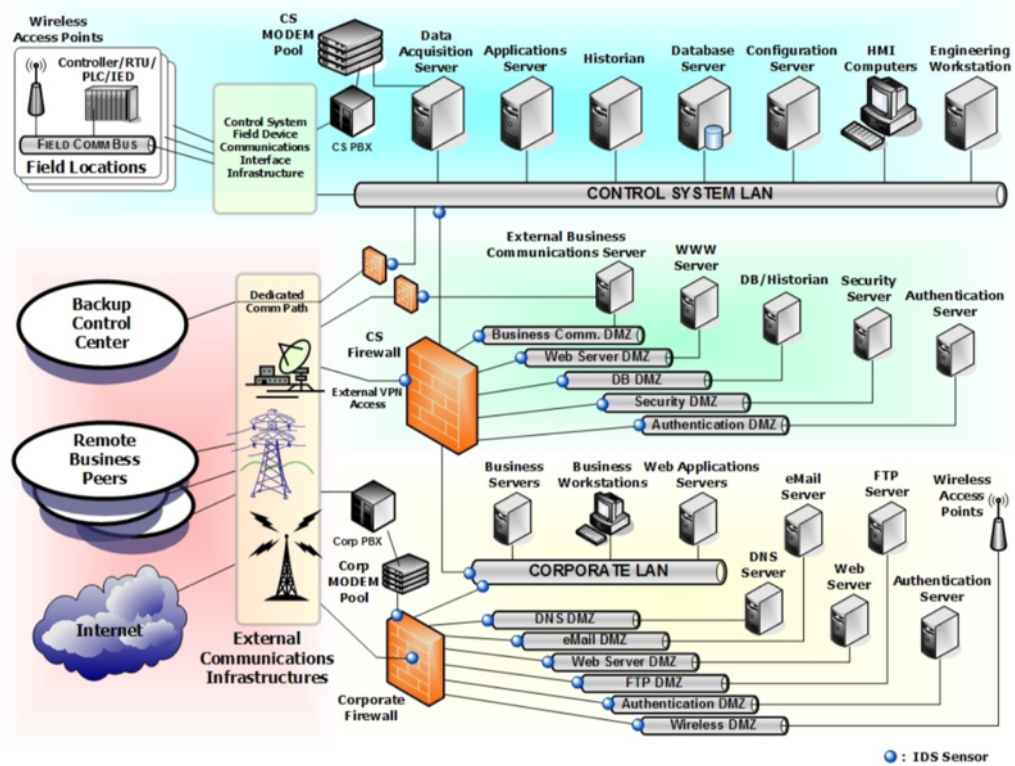
- Mancanza di autenticazione e di criptazione
- Consentono la programmabilità (vedi Modbus)
- Esiste la versione «sicura», ma è opzionale (vedi DNP3)
- Sistemi di autenticazione obsoleti (vedi OPC)
- Apertura di porte non necessarie
- Vulnerabilità di Ethernet, di IP e degli altri standard della pila ISO/OSI

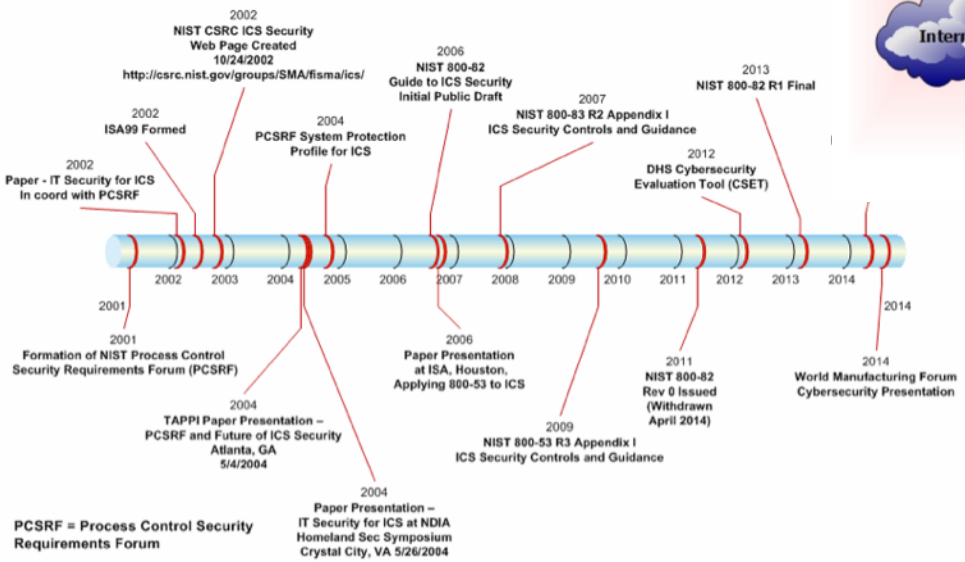
STANDARDS


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.


Local/State
CFATS
NESA
NERC CIP
United Arab Emirates
AGA
NEI
NIST
FISMA
DHS
ISO
FERC
OSHA
FCC
ICPA
ISA
Japan
SEC
DOE
European Commission 2008
COUNCIL DIRECTIVE
2008/114/EC

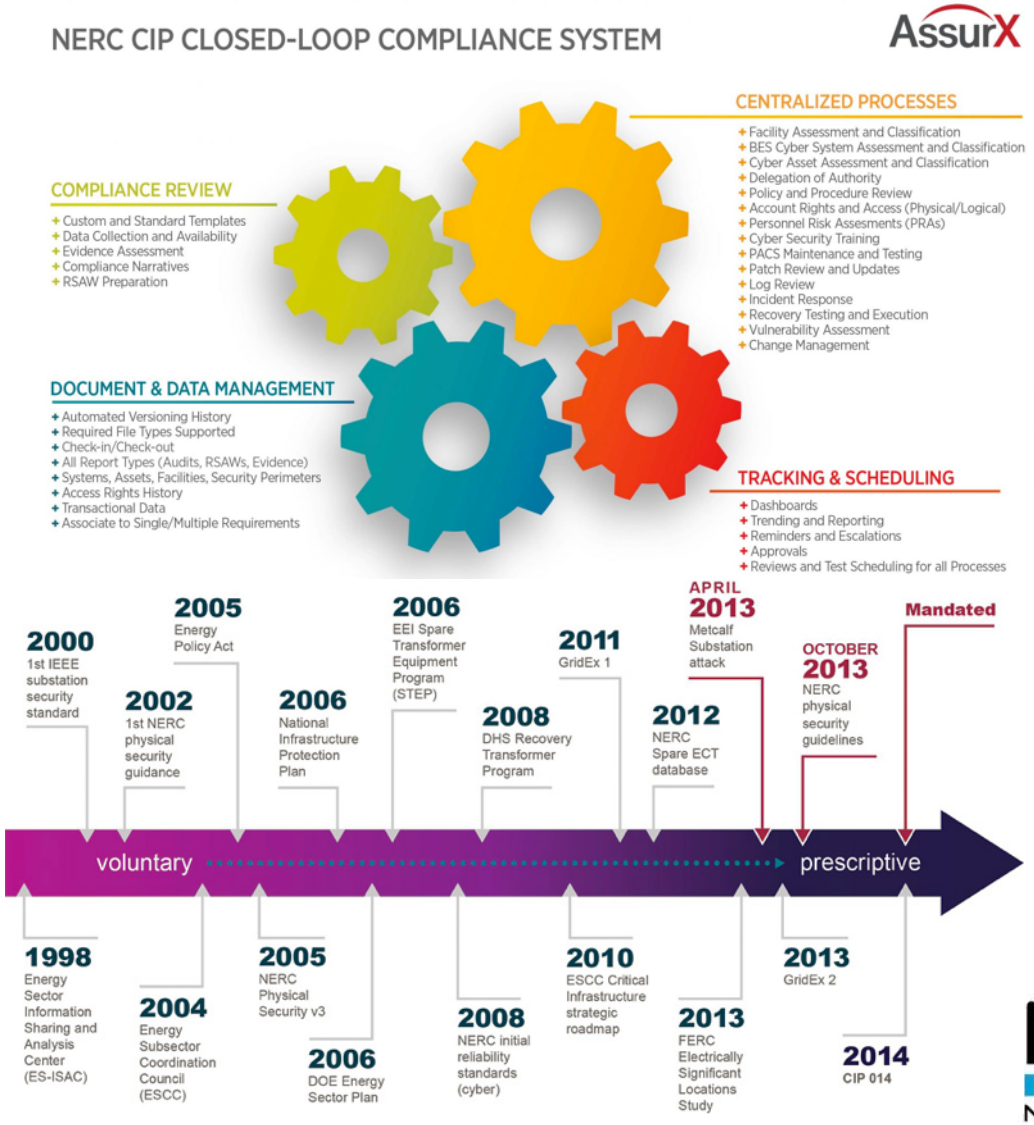
NIST – SP 800 - 82





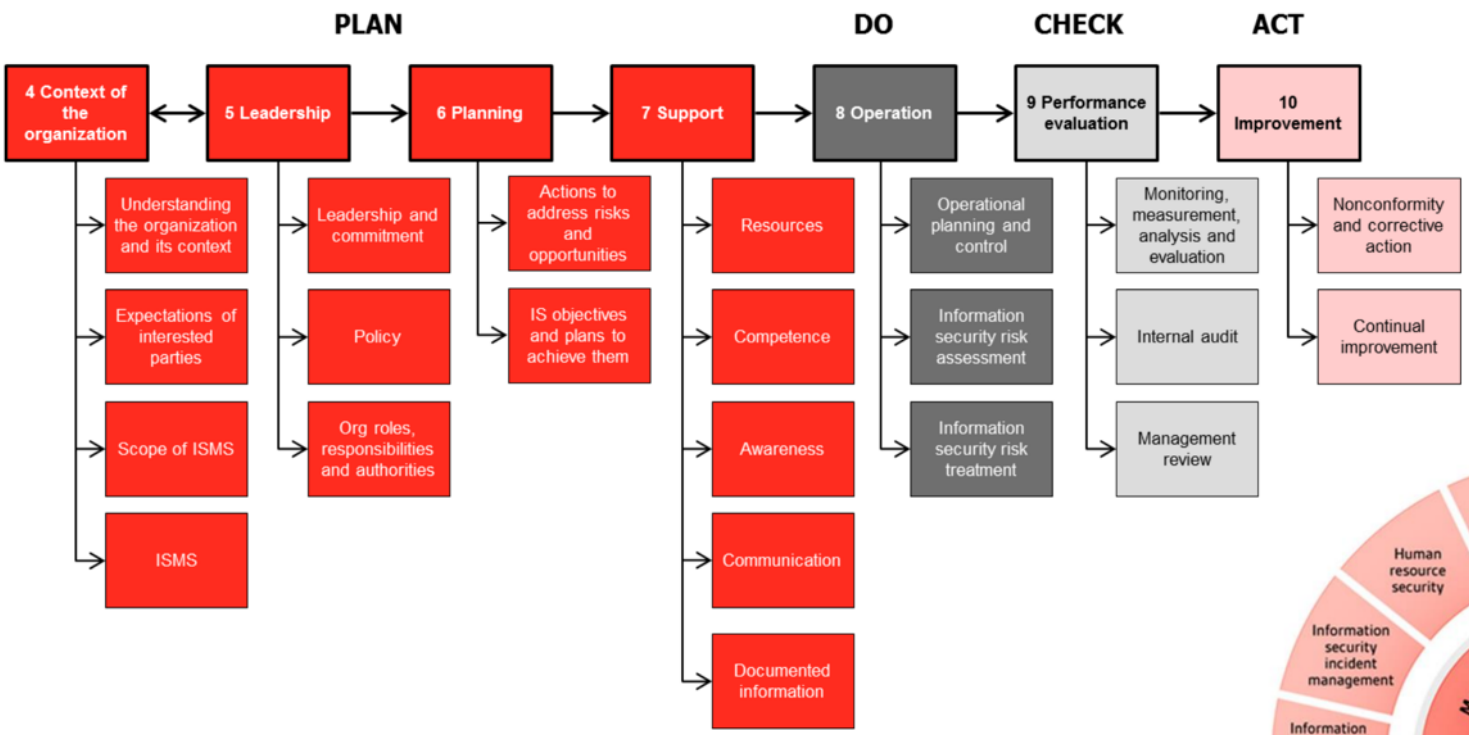
National Institute of Standards and Technology
U.S. Department of Commerce

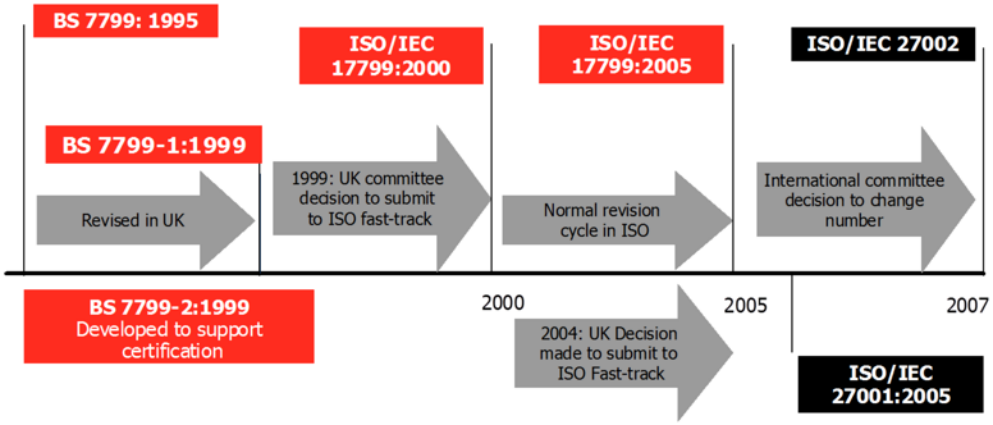
NERC CIP

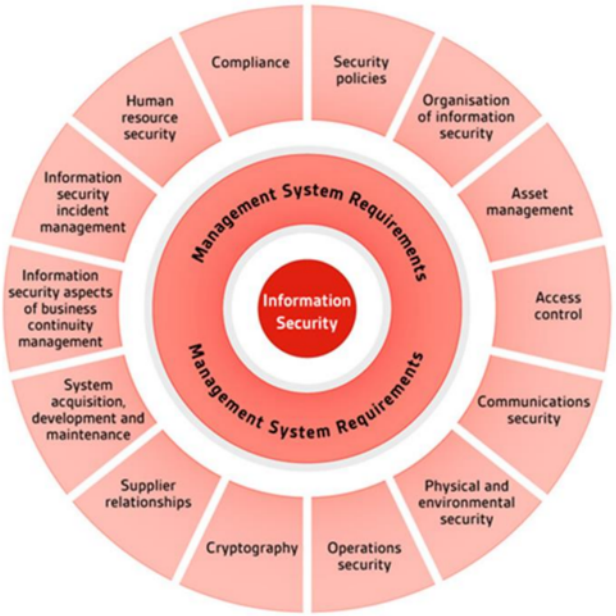


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

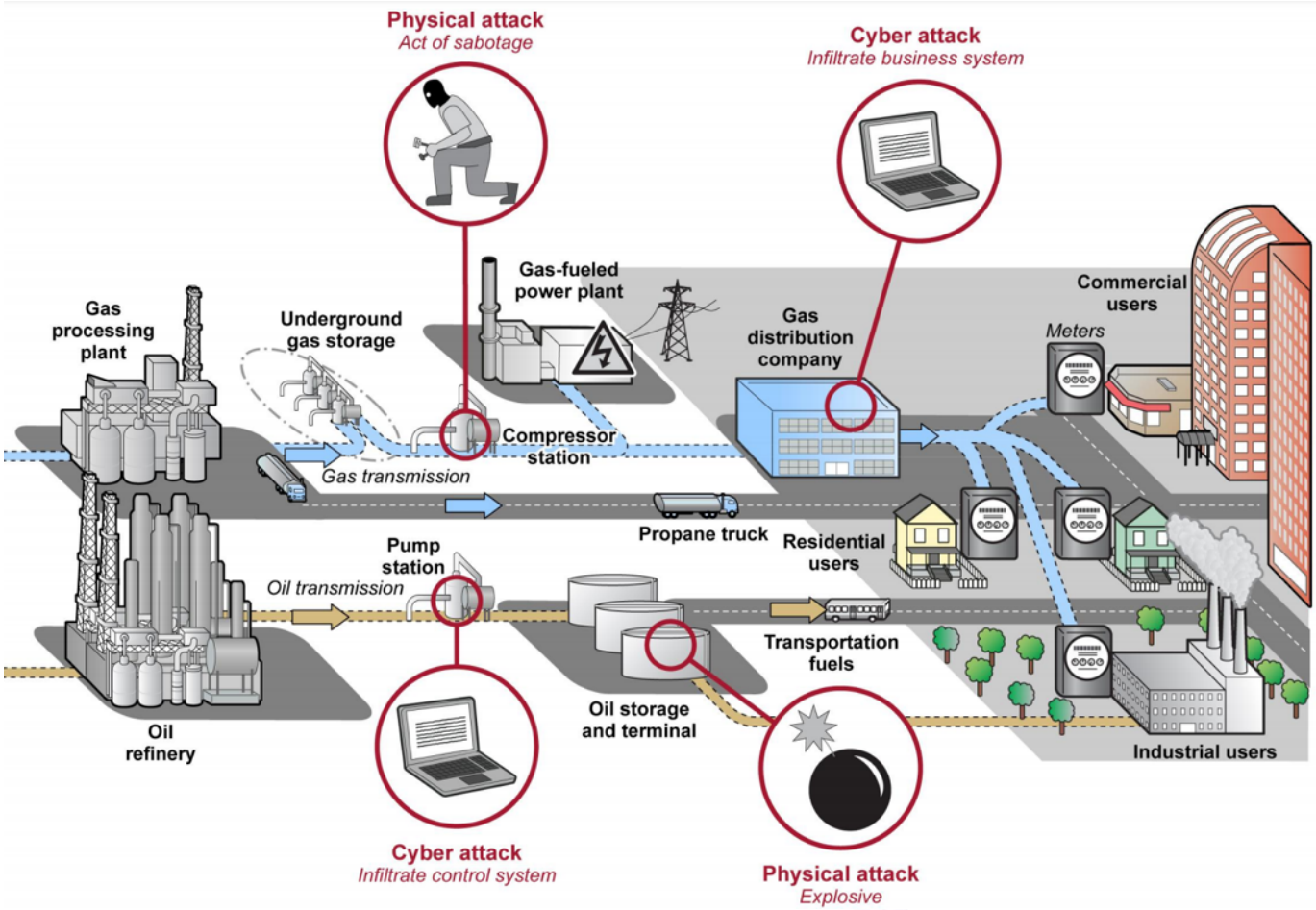
ISO/IEC 27002:2005





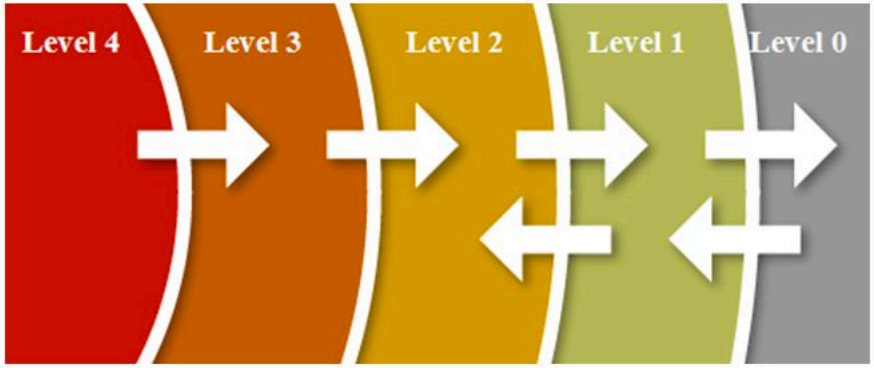


CFATS



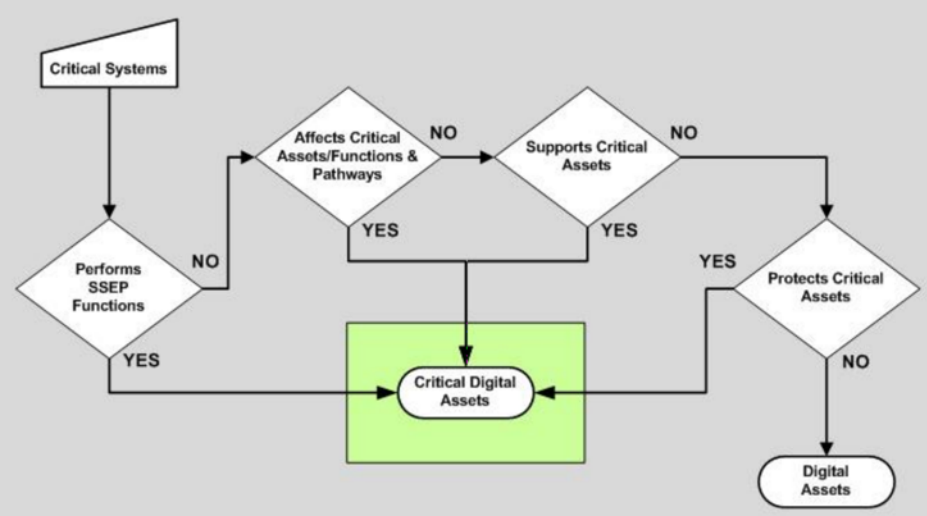
CFATS
Chemical Facility Anti-Terrorism Standards

NUCLEAR REGULATORY COMMISSION

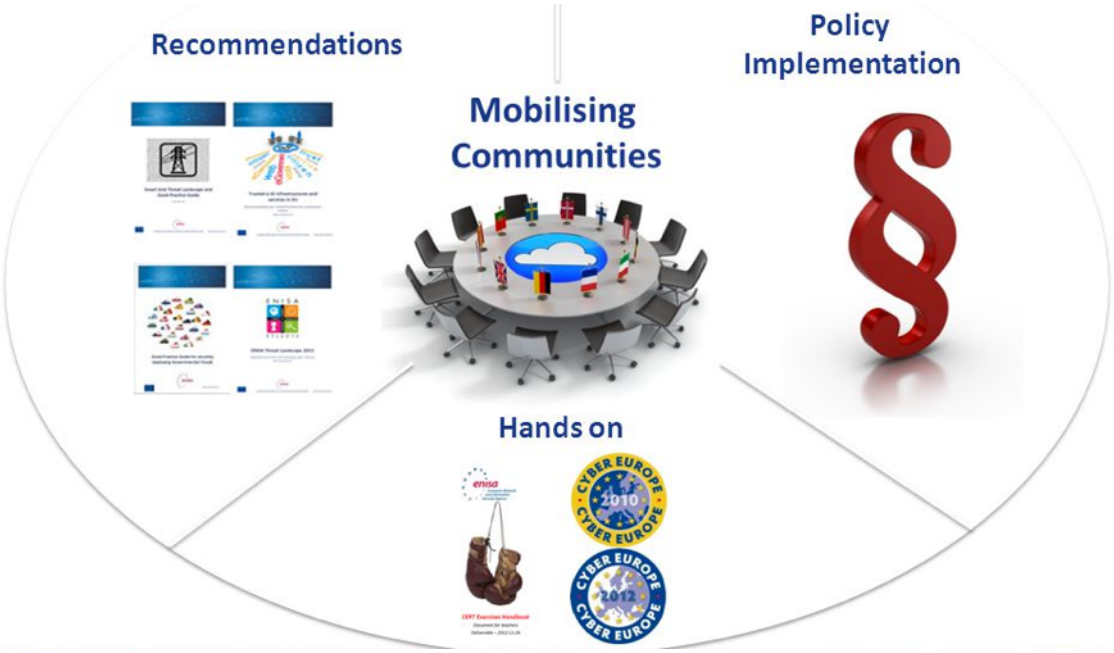


Level 4: Vital Area
Level 3: Protected Area
Level 2: Owner-Controlled Area
Level 1: Corporate Accessible Area
Level 0: Public Accessible Area

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment



ENISA



enisa
European Network and Information Security Agency

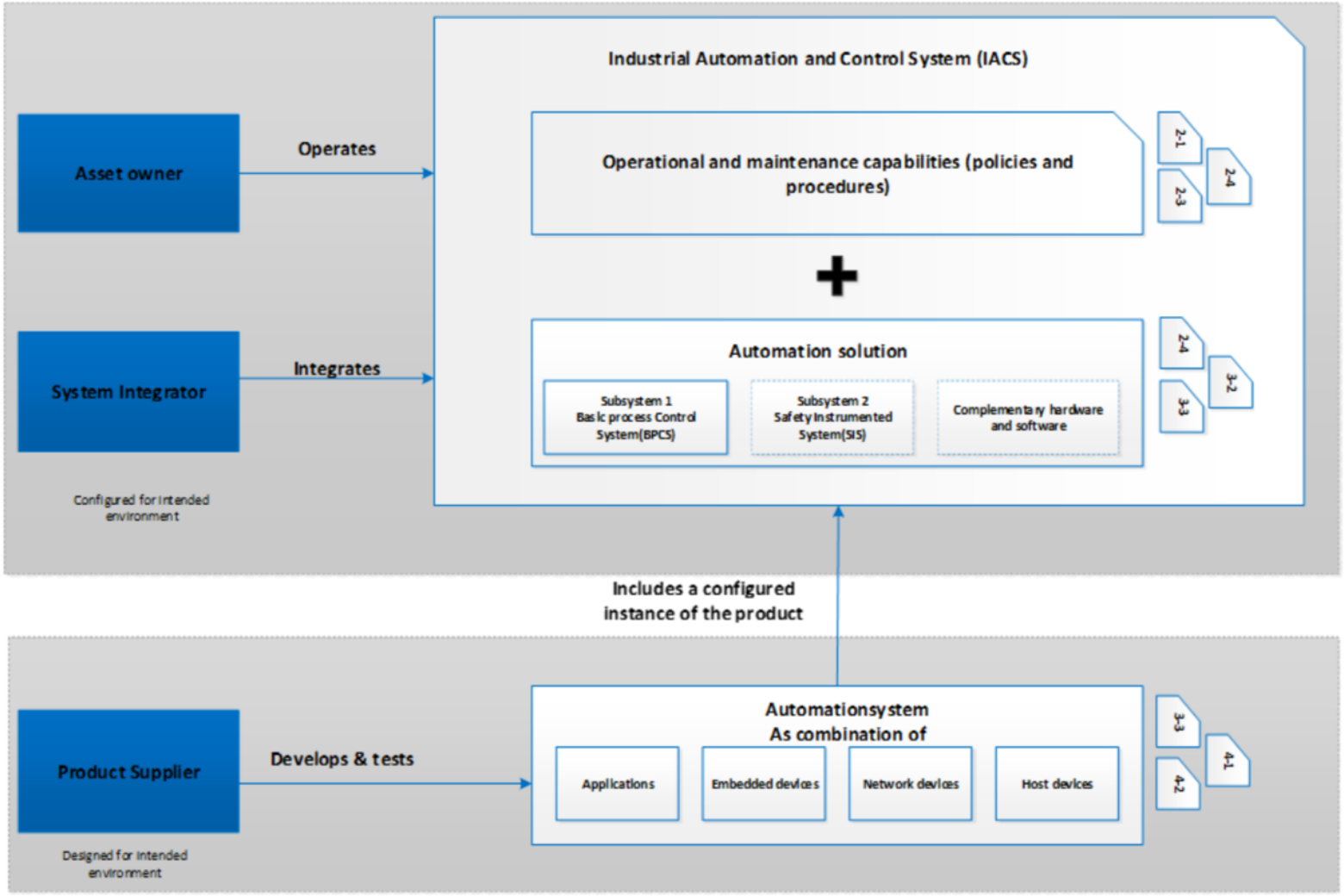
IEC 62443

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

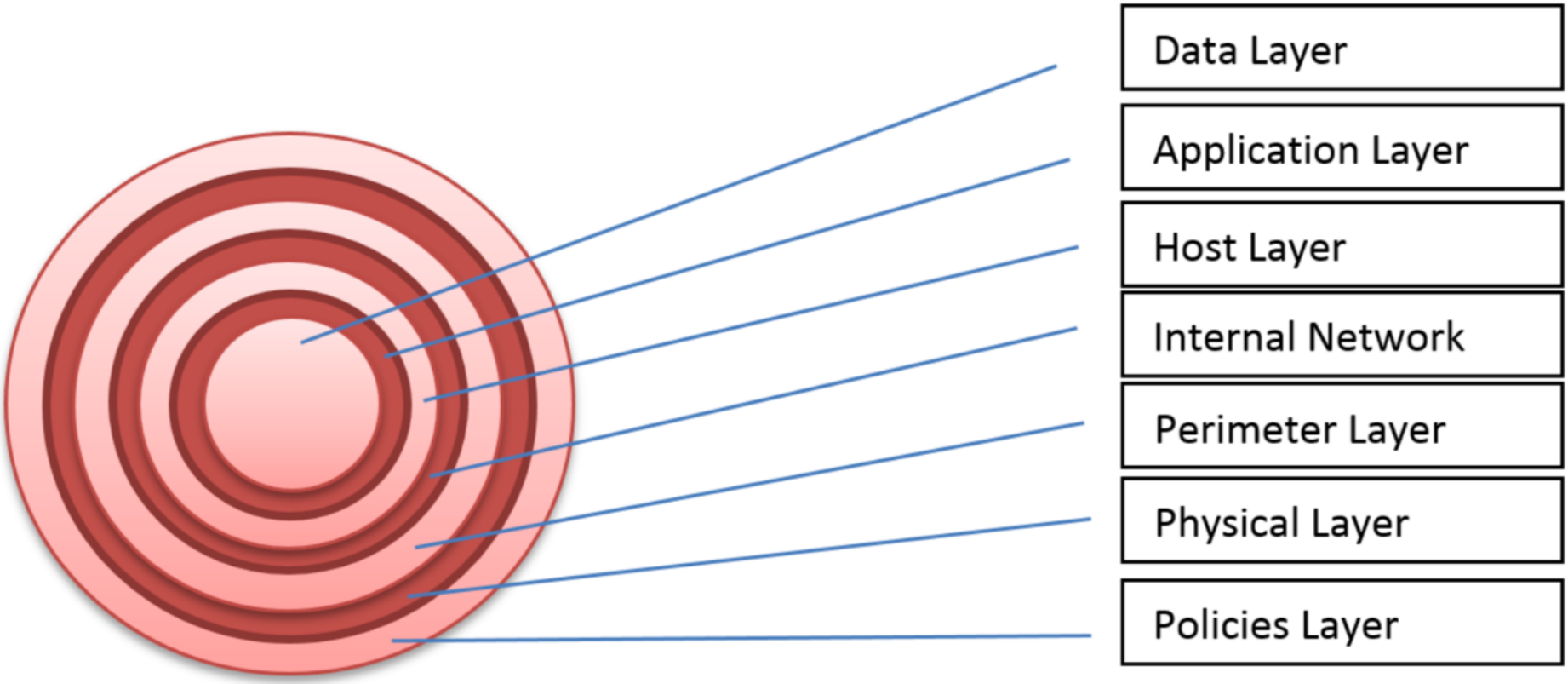
IEC 62443 Series

General		Management System		Industrial IT Security, IACS		Embedded Security, Component	
1-1	Termininology, concepts and models	2-1	Establishing an IACS Security program	3-1	Security technologies for IACS	4-1	Product development requirements
1-2	Master glossary of terms and abbreviations	2-2	Operating an IACS security program	3-2	Security risk assessment and system design	4-2	Technical security requirements for IACS components
1-3	System security compliance metrics	2-3	Patch Management in the IACS environment	3-3	System security requirements and security levels		
		2-4	Requirements for IACS solution suppliers				

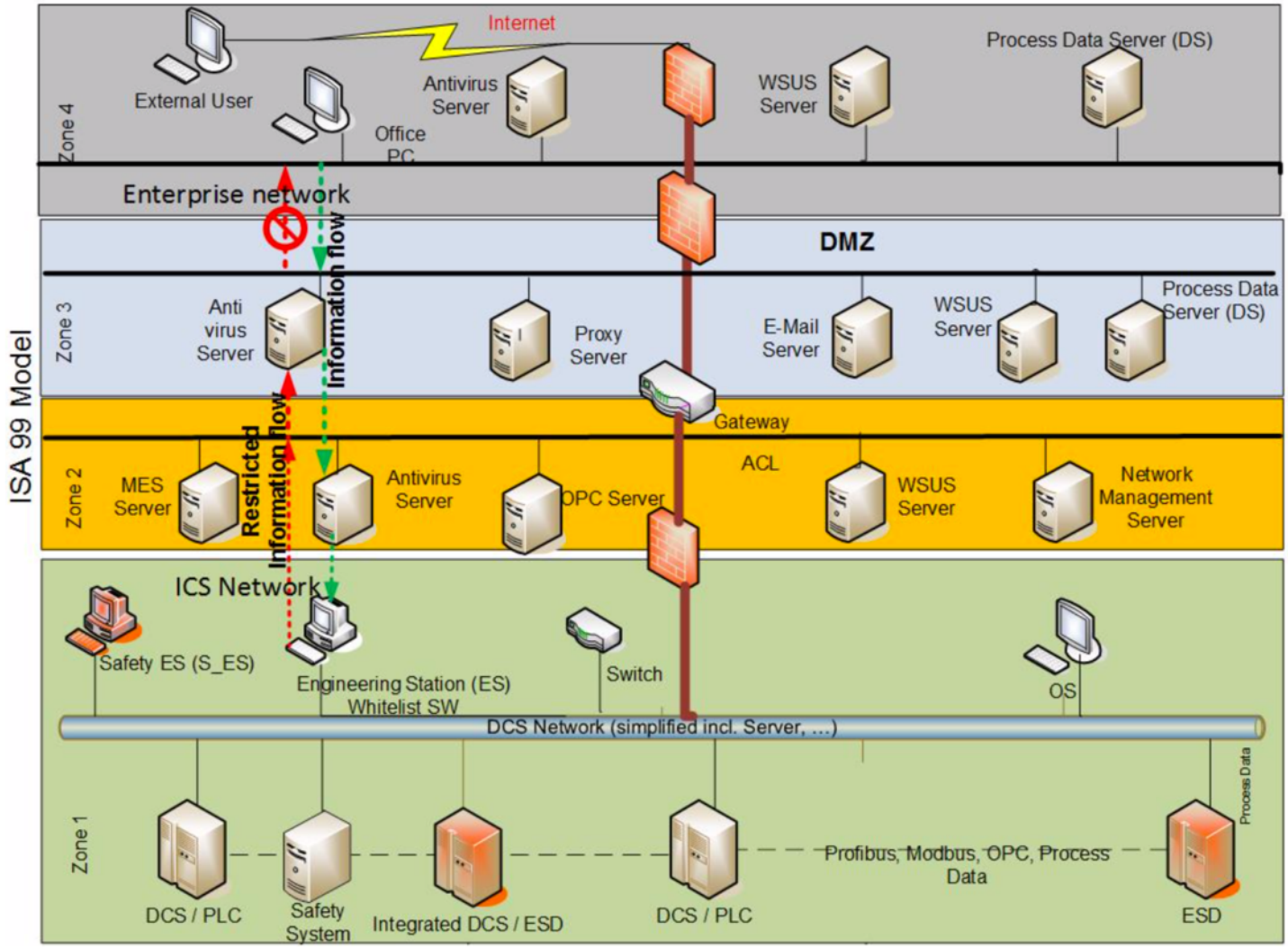
I Ruoli nella IEC 62443



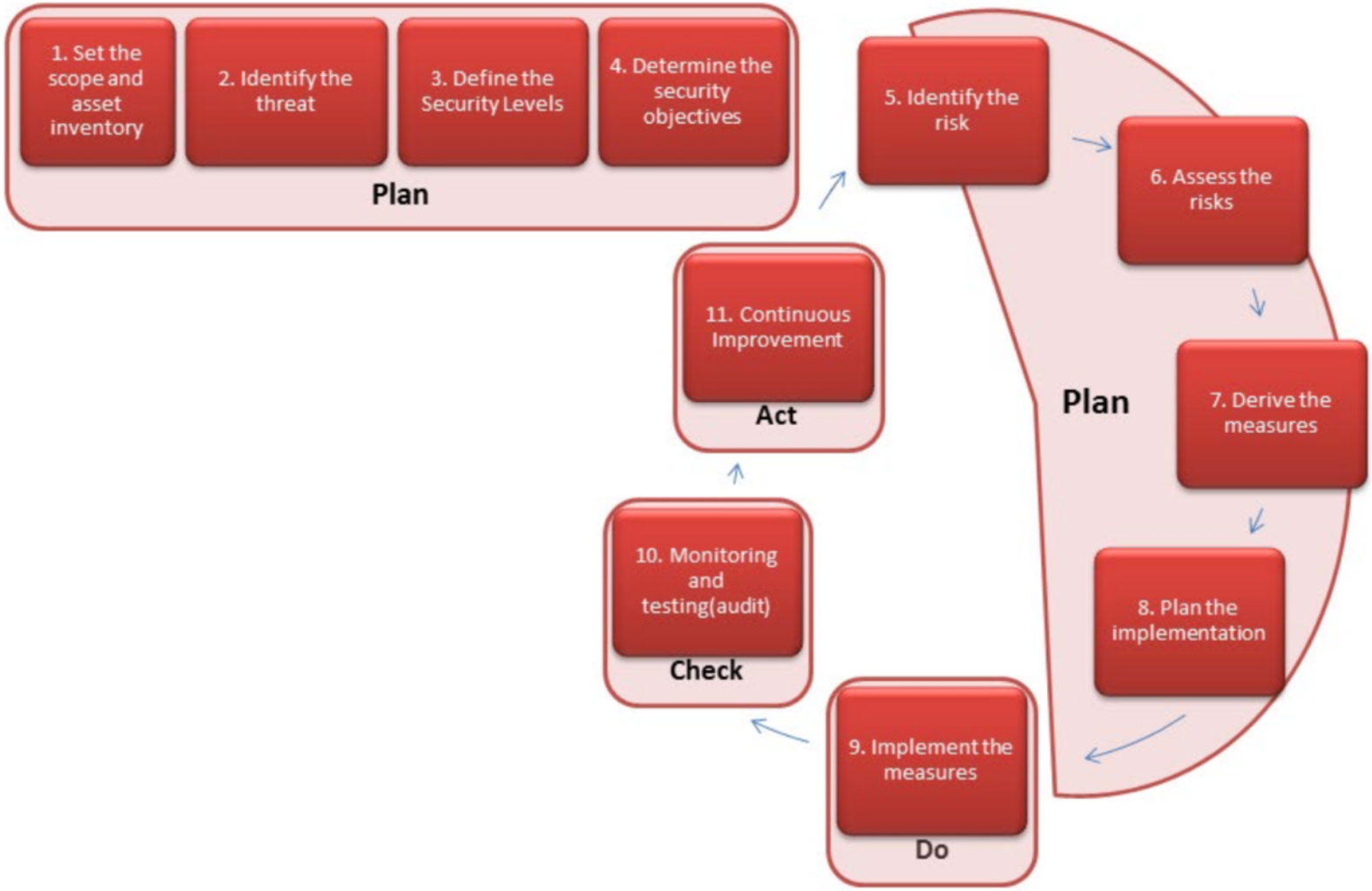
Defense in Depth



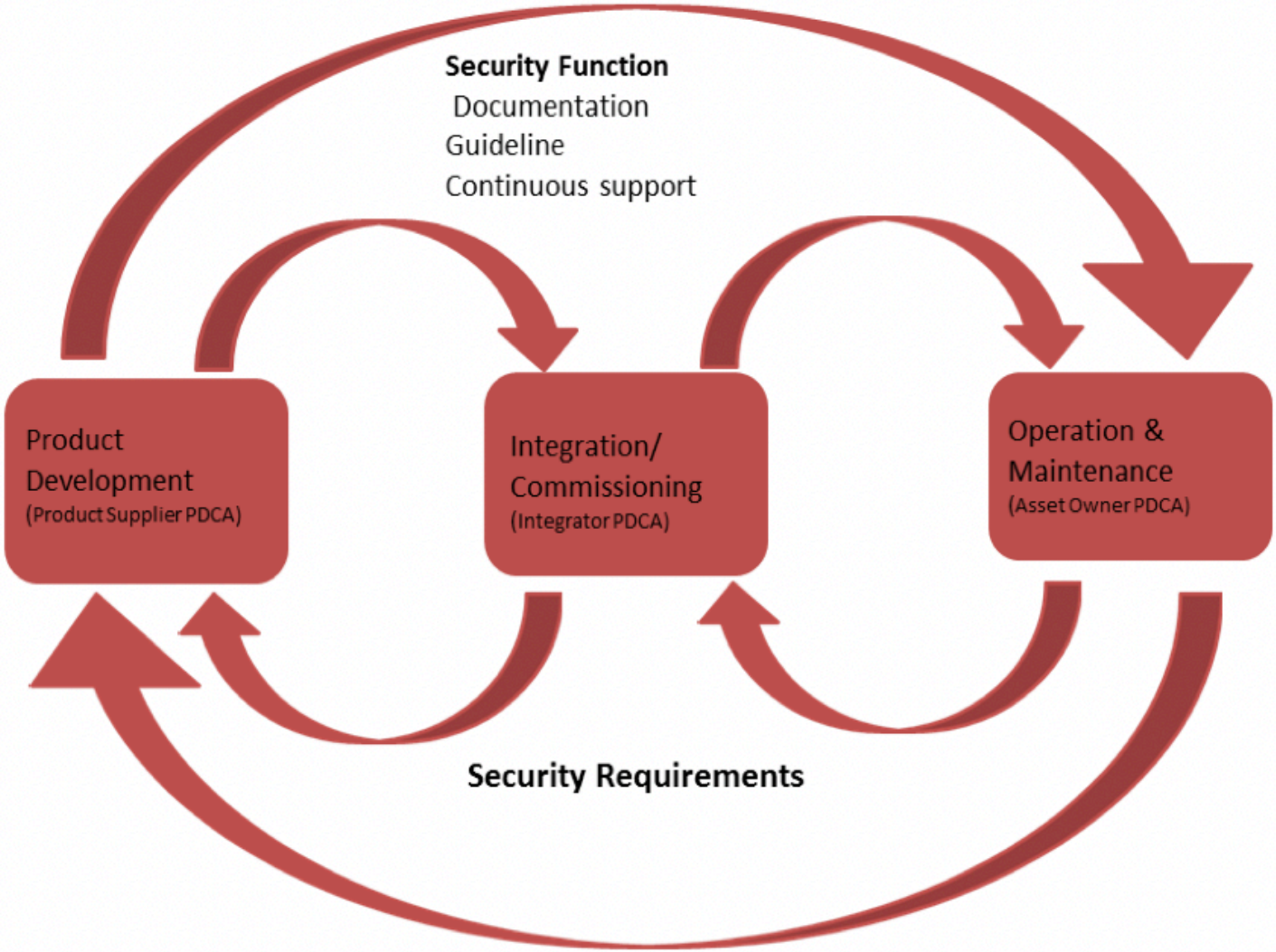
ZONE E CONDUITS



Ciclo di Vita



Ciclo di Vita



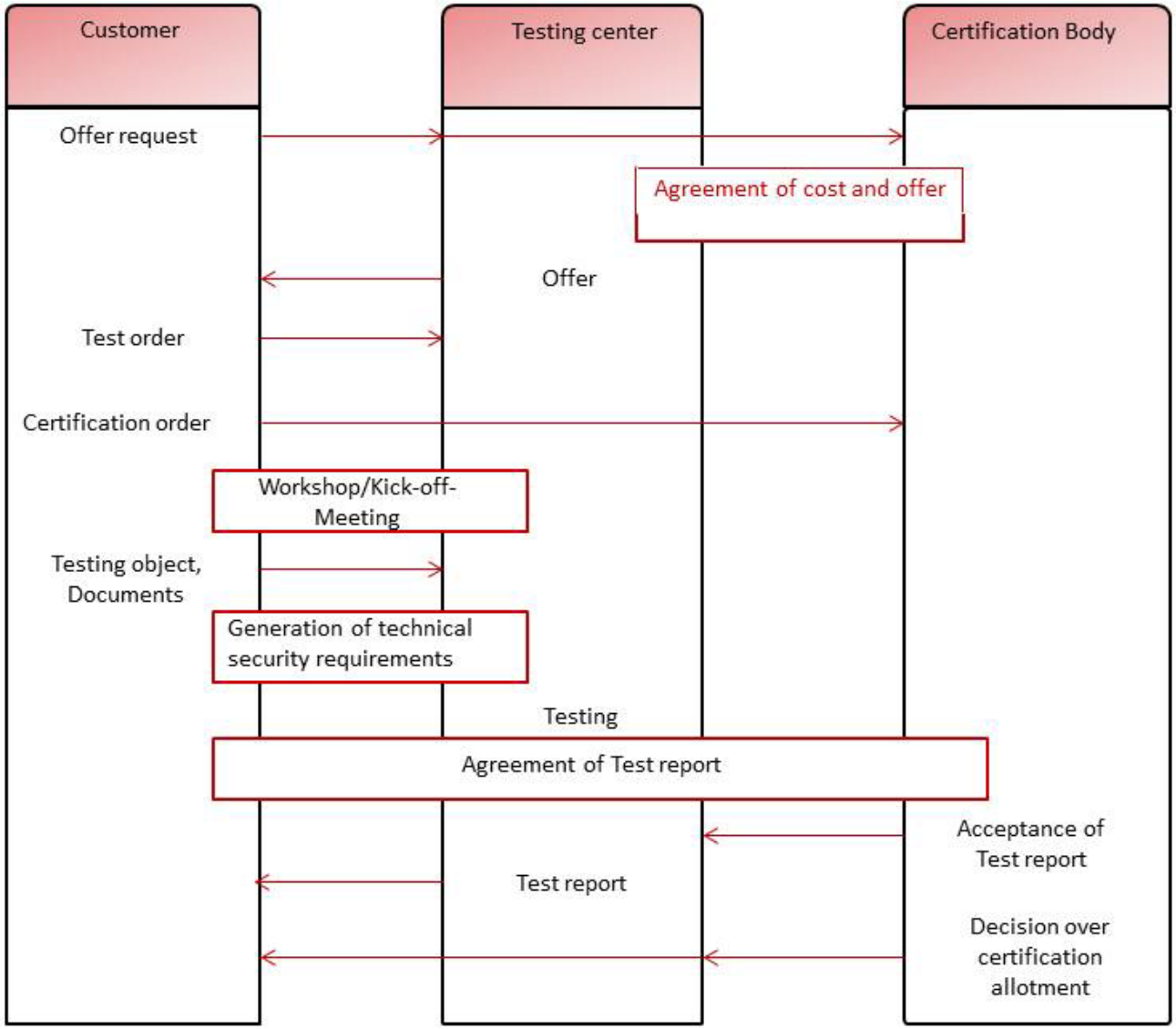
Livello di Sicurezza

Security Level	Description	Target	Skills	Motivation	Means
SL1	Capability to protect against casual or coincidental violation	Misconfiguration	No awareness	Confusion	No ojective
SL2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation	No security measures implemented, hacker	Basic	Low	Straight forward
SL3	Capability to protect against intentional violations using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Only moderate security measures implemented, high level hacker	Industrial specific	Average	Intentional
SL4	Capability to protect against intentional violations using sophisticated means with extended resources, IACS specific skills and high motivation	Economical Damage	Industrial specific	High	Aggressive

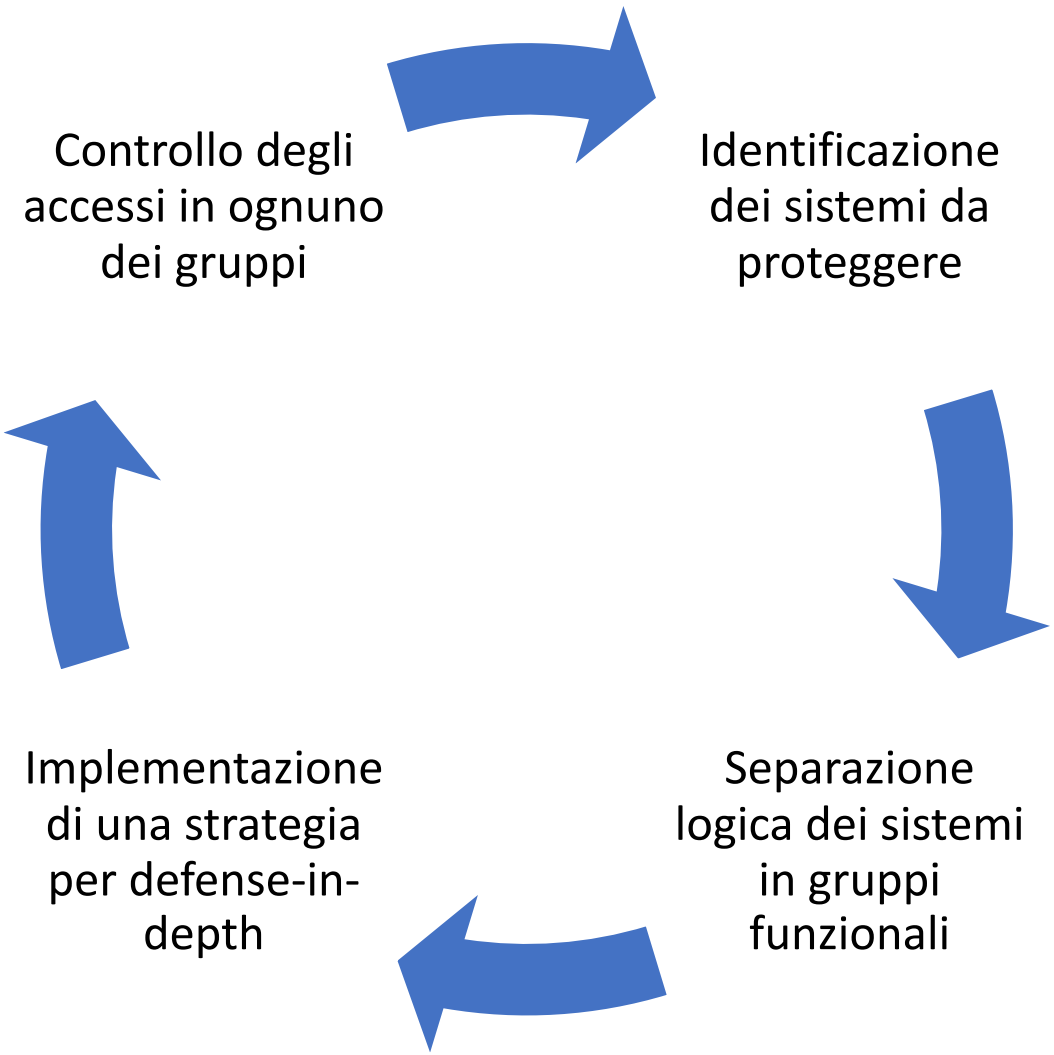
LIVELLO DI MATURITÀ

Maturity Level	Category	Description
ML 1	Initial	Capability of performing a service without a documented process that is poorly controlled
ML 2	Managed	Capability of performing a service in a formal documented characterized process with evidence of expertise and trained personnel
ML 3	Defined	Capability of performing ML2 level including evidence of practicing the process e.g. Documented process plus list of participants in the training of personnel
ML 4	Improved	Capability of performing ML3 level including demonstration of continuous improvement e.g. internal audit report

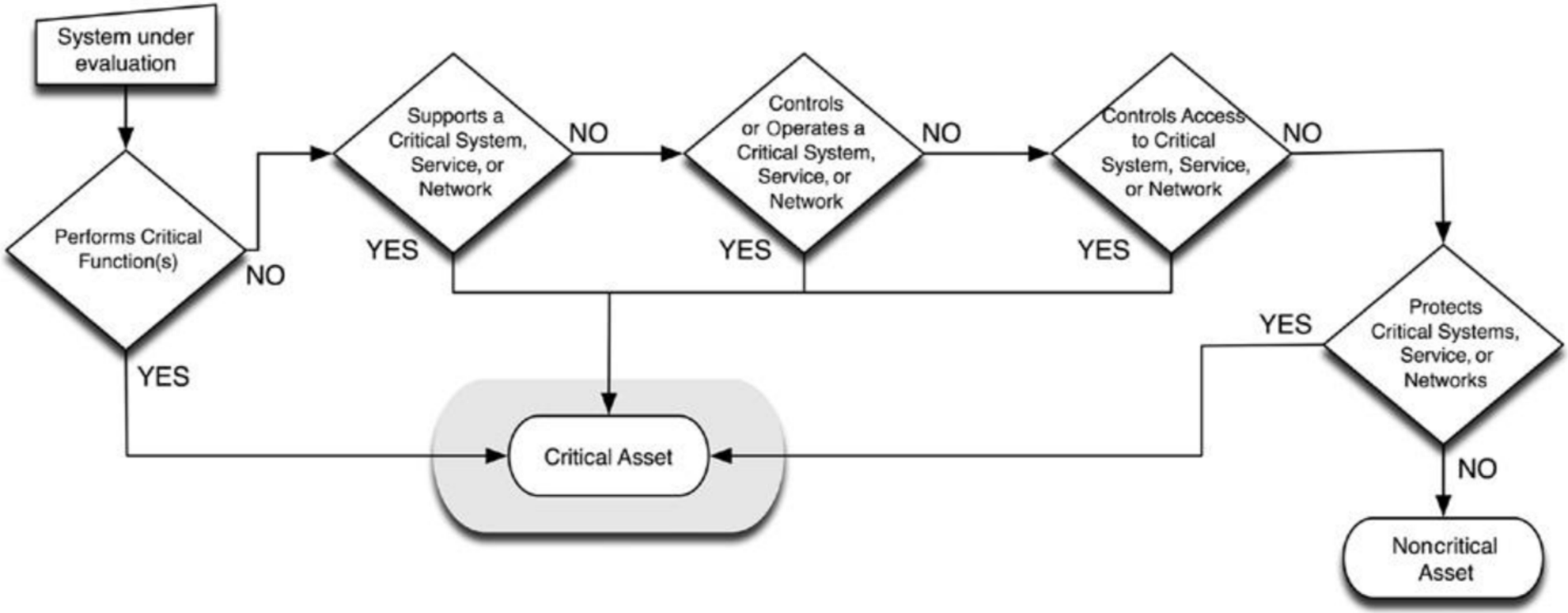
CERTIFICAZIONE



RACCOMANDAZIONI

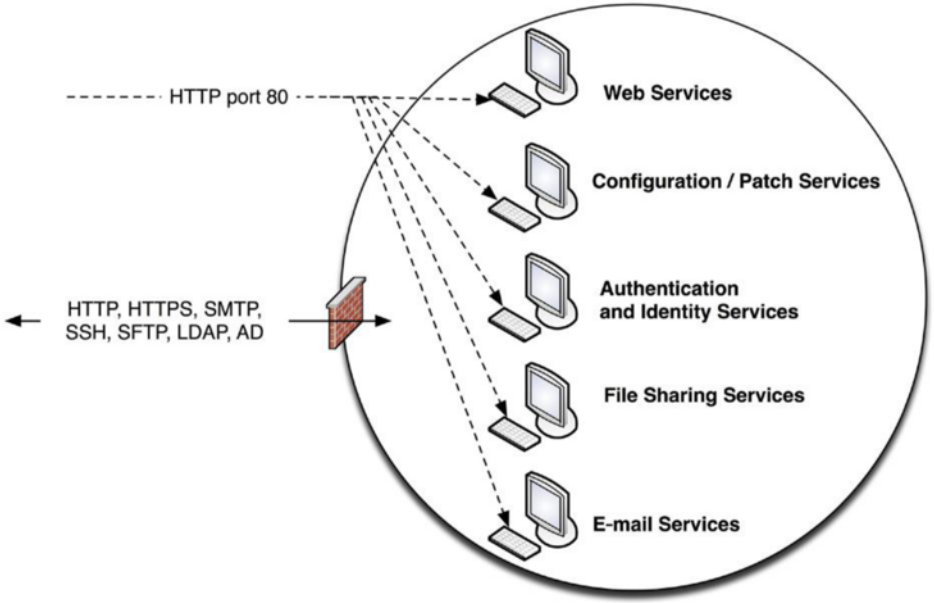


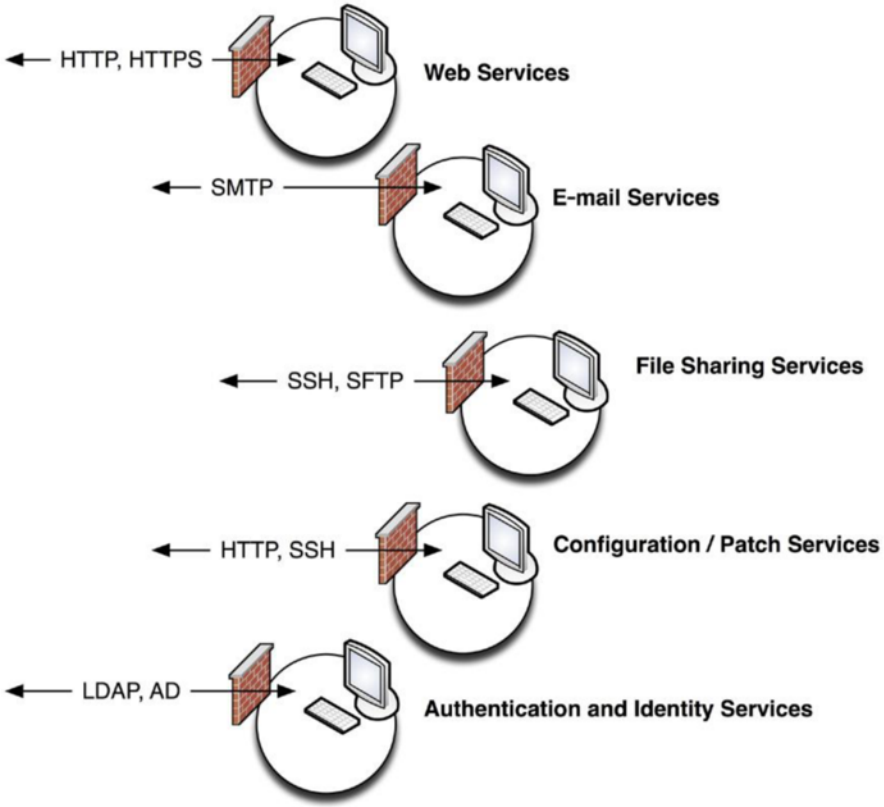
IDENTIFICAZIONE DEGLI ASSETS



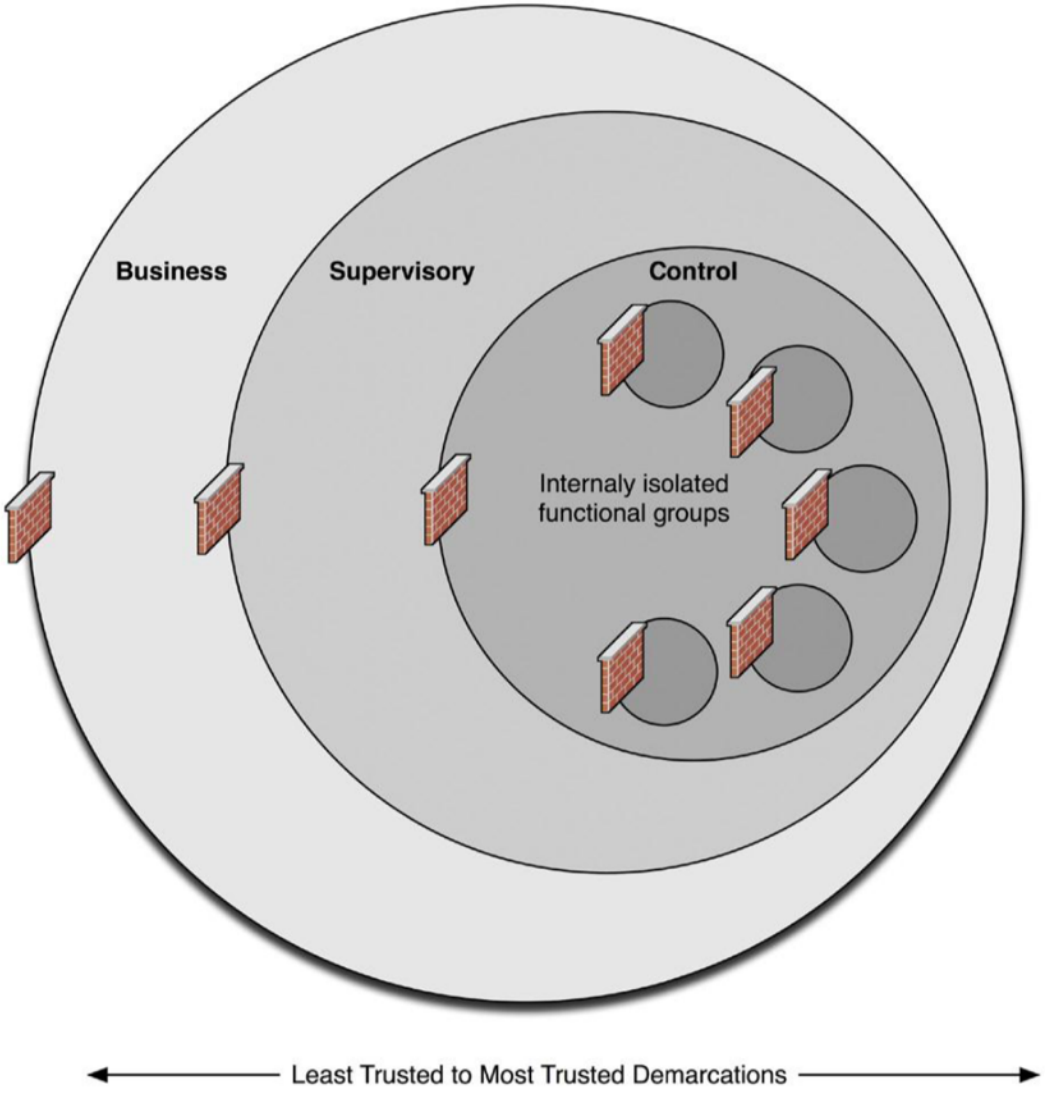
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SEPARAZIONE & SEGMENTAZIONE

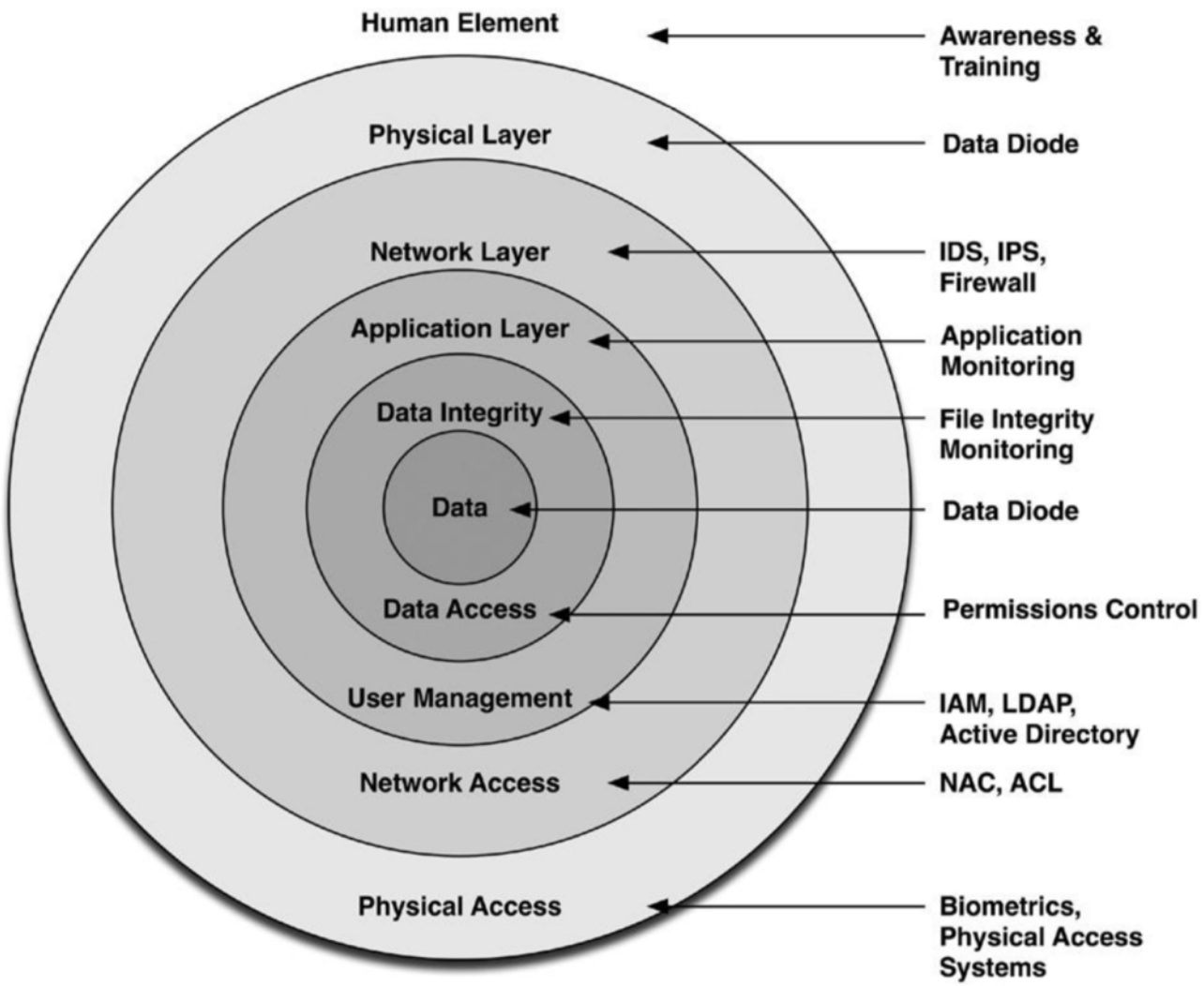




SEPARAZIONE & SEGMENTAZIONE



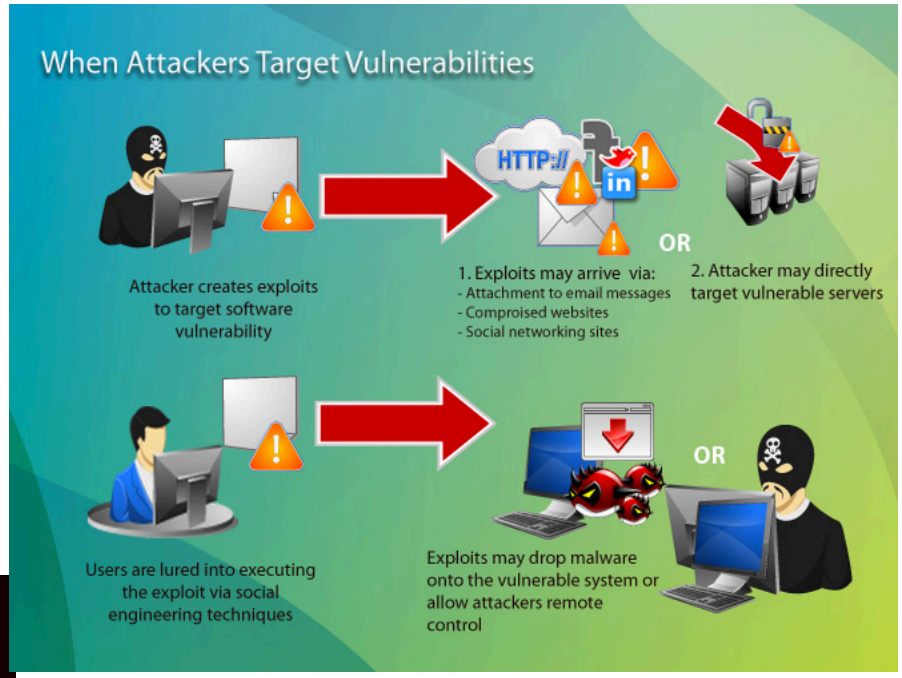
Defense in Depth



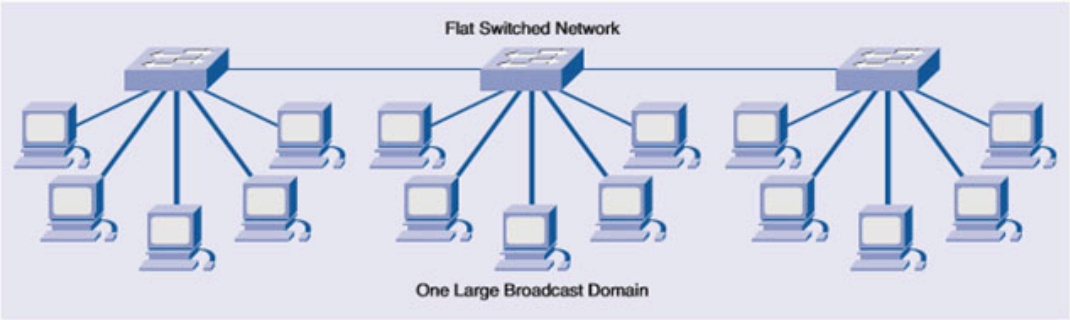
Controllo Degli Accessi

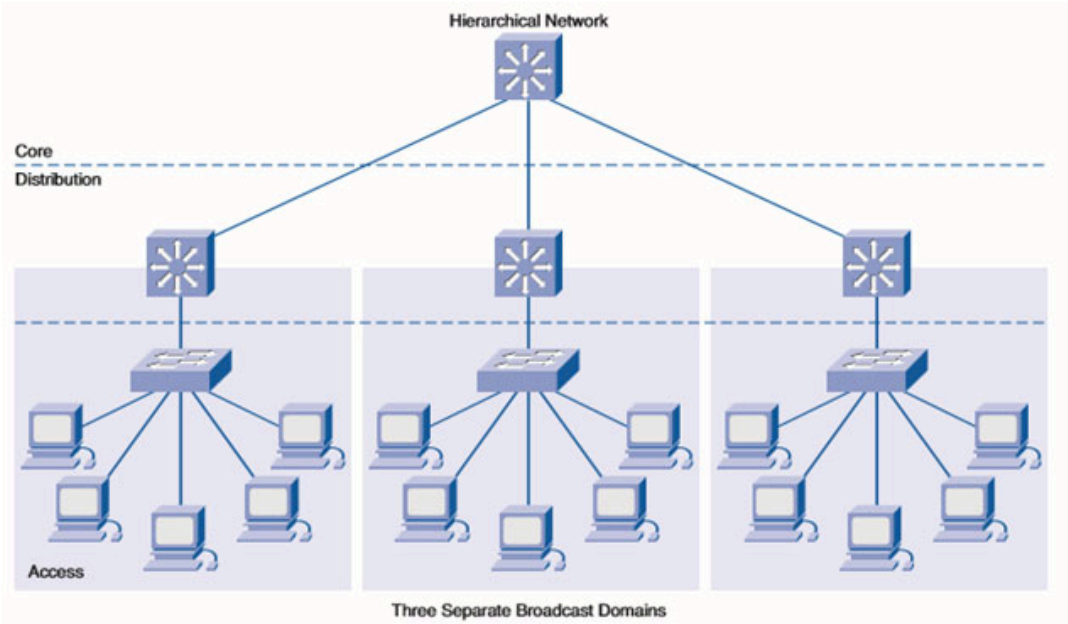
Good	Better	Best
User accounts are classified by authority level	User accounts are classified by functional role	User accounts are classified by functional role and authority
Assets are classified in conjunction with user authority level	Assets are classified in conjunction with function or operational role	Assets are classified in conjunction with function and user authority
Operational controls can be accessed by any device based on user authority	Operational controls can be accessed by only those devices that are within a functional group	Operational controls can only be accessed by devices within a functional group by a user with appropriate authority

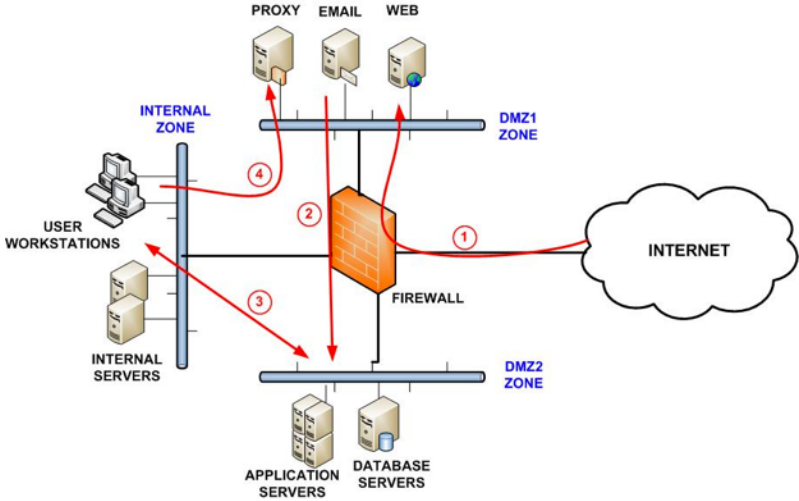
Software non Aggiornato



Non Adeguata Segmentazione della Rete

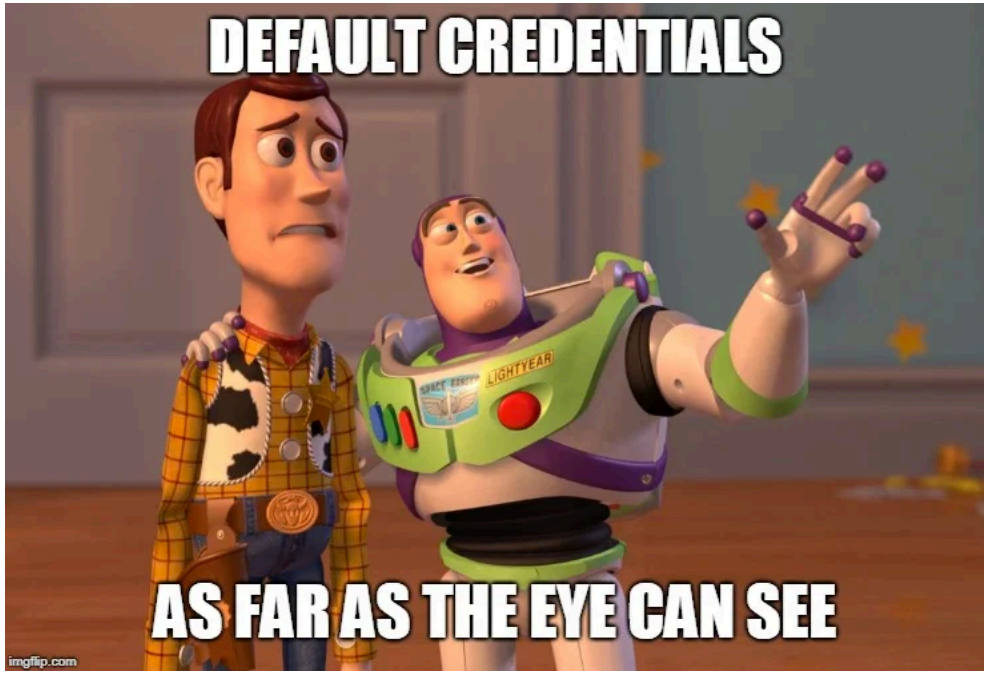






MANCANZA DI SICUREZZA

Controllo degli Accessi Debole



Monitoraggio Insufficiente

SPEAKER: CHIARA FOGLIETTA

EMAIL: CHIARA.FOGLIETTA@UNIROMA3.IT