HITACHI
Inspire the Next

Industry 4.0:
quale protezione per i sistemi always on?

4 ottobre 2018 – Security Summit

Michele Onorato

Security Office Manager

Hitachi Systems CBT

Agenda

HITACHI
Inspire the Next

1. Scenario
2. Framework di riferimento ISA/IEC 62443
3. Metodologia e approccio alla sicurezza degli ambienti IACS
4. Criteri di dimensionamento

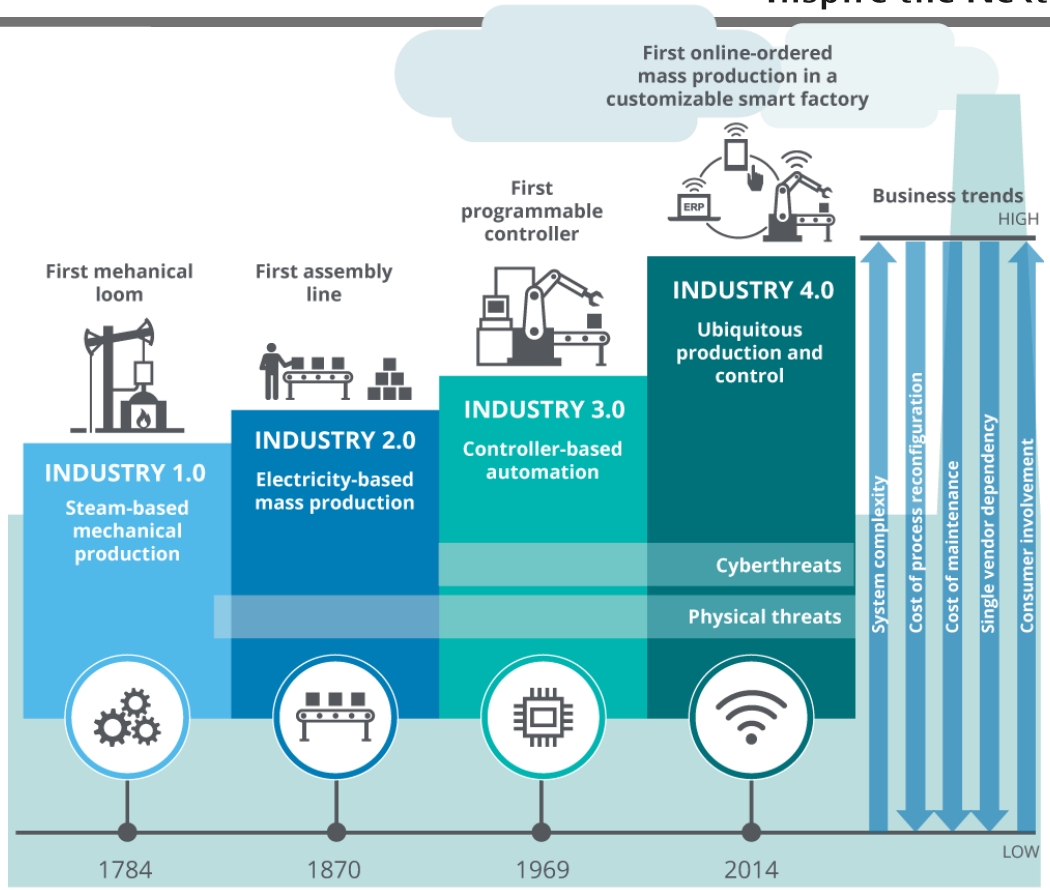
Human * IT

1. Scenario

Overview

HITACHI
Inspire the Next

L’evoluzione del business implica una rivisitazione delle supply chain e dei processi industriali. I **sistemi di produzione** (**OT**) sono sempre più connessi e quindi **esposti** a **minacce mutuate dal mondo IT**, avendo perso l’isolamento che ne garantiva la sicurezza intrinseca fino a ieri



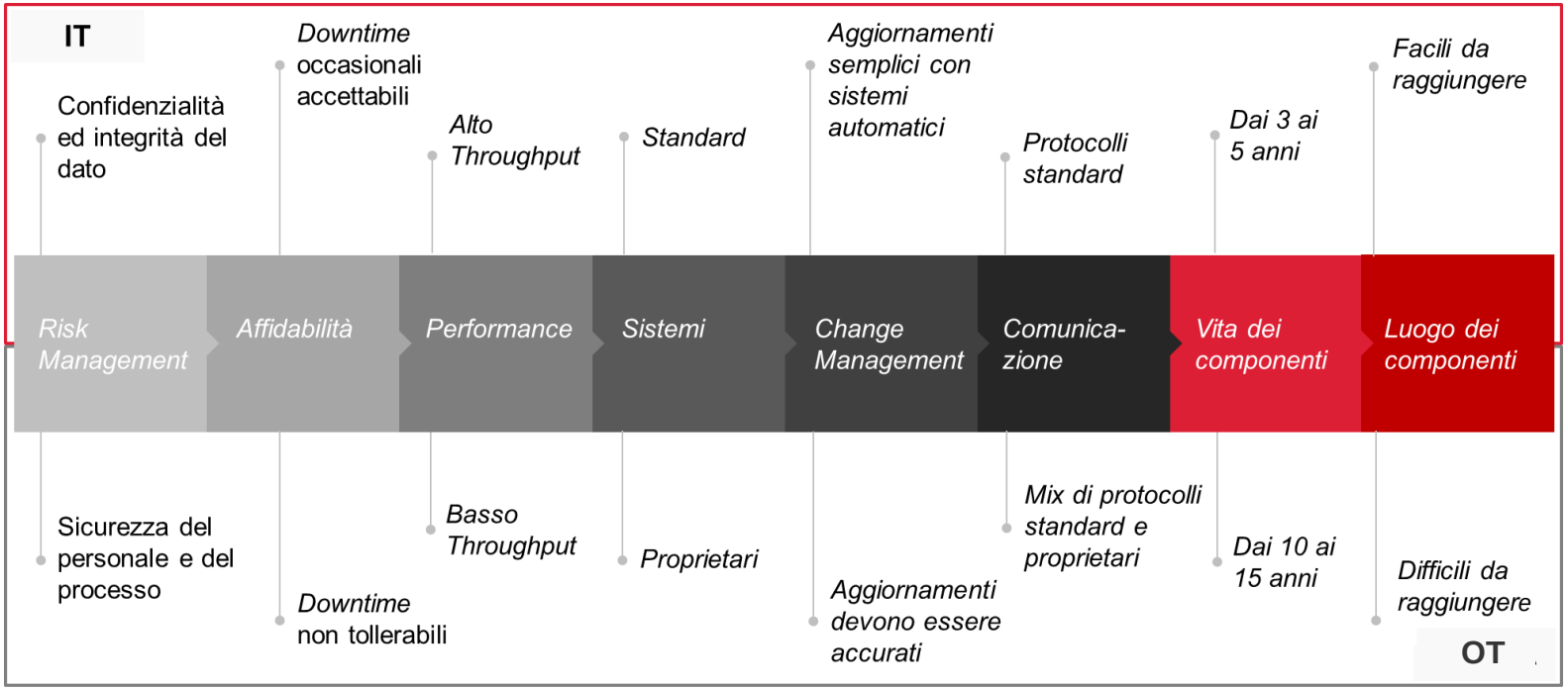
Source: Deloitte.

Human * IT

Distinzione tra ambienti IT e OT

HITACHI
Inspire the Next

Gli **ambienti IT** e **OT** hanno diverse declinazioni delle infrastrutture tecnologiche, ma dal punto di vista della sicurezza devono comunque convergere verso una **governance comune**, tesa ad abilitare una visione e gestione integrata dei due ambienti



Human * IT

Sicurezza negli ambienti a forte automazione industriale

HITACHI
Inspire the Next

PLANT SECURITY
- *Protezione dell'accesso fisico*
- *Processi e linee guida*
- *Servizio di sicurezza per la protezione degli impianti di produzione*

NETWORK SECURITY
- *Cell protection, DMZ e manutezione remota*
- *Firewall e VPN*

SYSTEM INTEGRITY
- *System hardening*
- *Autenticazione e use adiministration*
- *Patch management*
- *Rilevamento di attacchi*
- *Protezione di accesso integrata nell'automazione*

Il concetto di DIFESA A STRATI è una strategia di sicurezza in cui diversi livelli di difesa si sovrappongono attorno al sistema di automazione industriale da proteggere

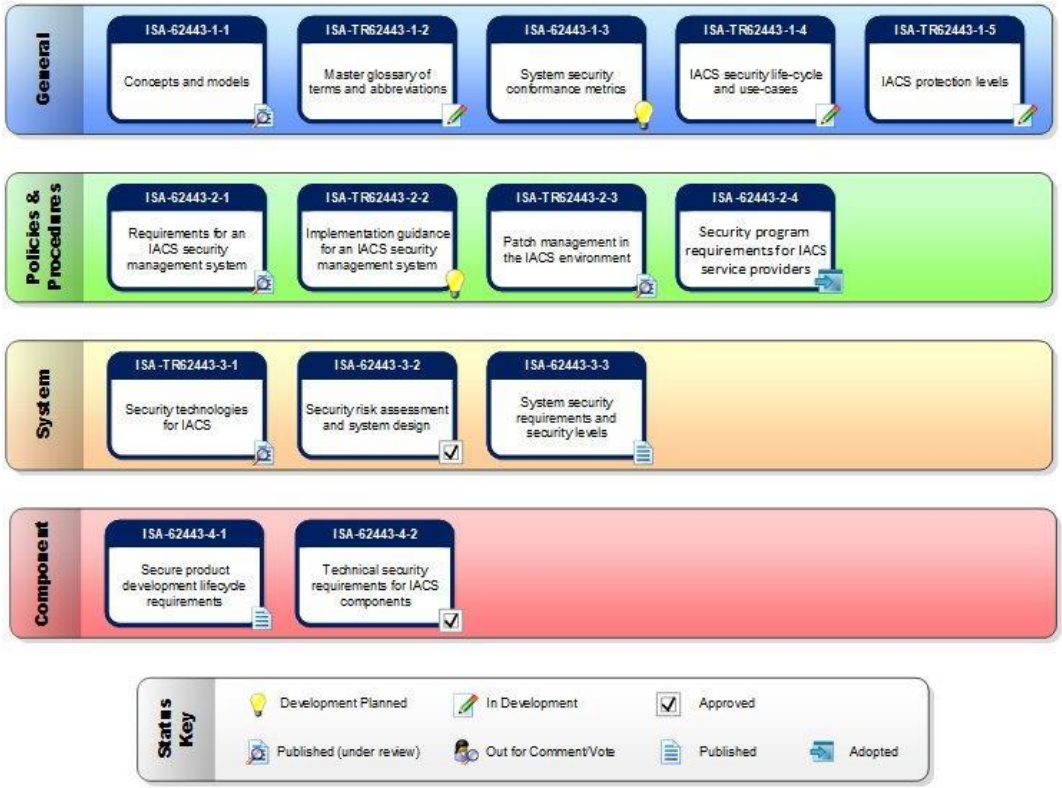
Human * IT

2. Framework di riferimento ISA/IEC 62443

Applicazione dello standard ISA/IEC 62443 e benefici

HITACHI
Inspire the Next

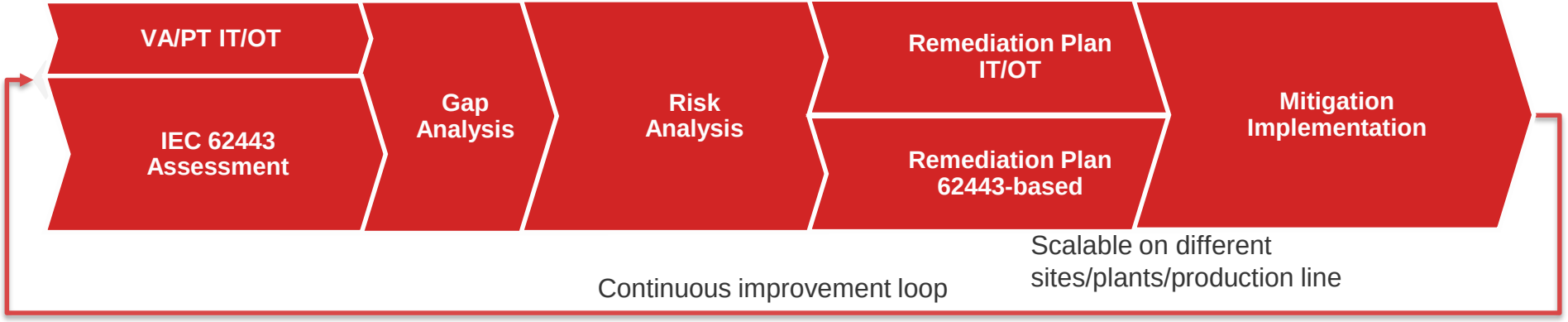
Un numero sempre maggiore di società ad alto livello di industrializzazione guarda con interesse allo **standard ISA/IEC 62443**, poiché rende possibile l'esecuzione di **assessment** per infrastrutture di **controllo industriali** (basate su sistemi SCADA, DCS, PLC, ecc) e di valutarne il livello di rischio



Human * IT

Approccio metodologico

Un **approccio integrato** alla sicurezza che indirizzi le peculiarità degli ambienti OT ed i requisiti di sicurezza dei sistemi industriali IEC62443, può garantire elevati **livelli di protezione e mitigazione del rischio**:



L'approccio si concretizza nell'associare le raccomandazioni ISA/IEC 62443 con i rischi industriali.
*Per ciascun **asset industriale** significativo (impianto, factory, pool di apparati critici) viene prodotta una **valutazione del rischio** con relativa severity*

3. Metodologia e approccio alla sicurezza degli ambienti IACS

Modello di valutazione del rischio

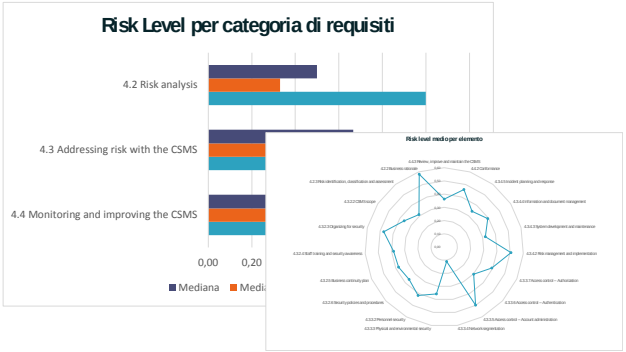
HITACHI
Inspire the Next

62443 Requirements Assessment → **Compliance Maturity** → **Risk Evaluation** → **Risk Classification & Reporting**

Requirement ID	Requirements
4.2.2.1	preventive actions
4.2.3.1	Select a risk assessment methodology
4.2.3.2	Provide risk assessment background information
4.2.3.3	Conduct a high-level risk assessment
4.2.3.4	Identify the IACS
4.2.3.5	Develop simple network diagrams
4.2.3.6	Prioritize systems
4.2.3.7	Perform a detailed vulnerability assessment
4.2.3.8	Identify a detailed risk assessment methodology
4.2.3.9	Conduct a detailed risk assessment
4.2.3.10	Identify the reassessment frequency and triggering criteria

Requirement ID	Control	Contr. value	Vulnerab.
4.2.2.1	The organization should develop a high-level business rationale, as a basis for its effort to manage IACS cyber security, which addresses the unique dependence of the organization on IACS.	1	4
4.2.3.1	The organization shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to their IACS assets.	2	3
4.2.3.2	The organization should provide participants in the risk assessment activity with appropriate information including methodology training, before beginning to identify the risks.	3	2
4.2.3.3	A high-level system risk assessment shall be performed to understand the financial and HSE consequences in the event that availability, integrity or confidentiality of the IACS is compromised.	4	1
4.2.3.4	The organization shall identify the various IACS, gather data about the devices to characterize the nature of the security risk and group the devices into logical systems.	NA	0
4.2.3.5	The organization shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types and general locations of the equipment.	4	1

Physical Damage		
Fire	Water Damage	Pollution - Dust - Corrosion - Freezing
2	1	3
IA	A	A
8,00	3,00	9,00
32,00	12,00	36,00
24,00	9,00	27,00
16,00	6,00	18,00
8,00	3,00	9,00
0,00	0,00	0,00
8,00	3,00	9,00
16,00	6,00	18,00



I requisiti ISA/IEC 62443 si declinano su varie dimensioni:

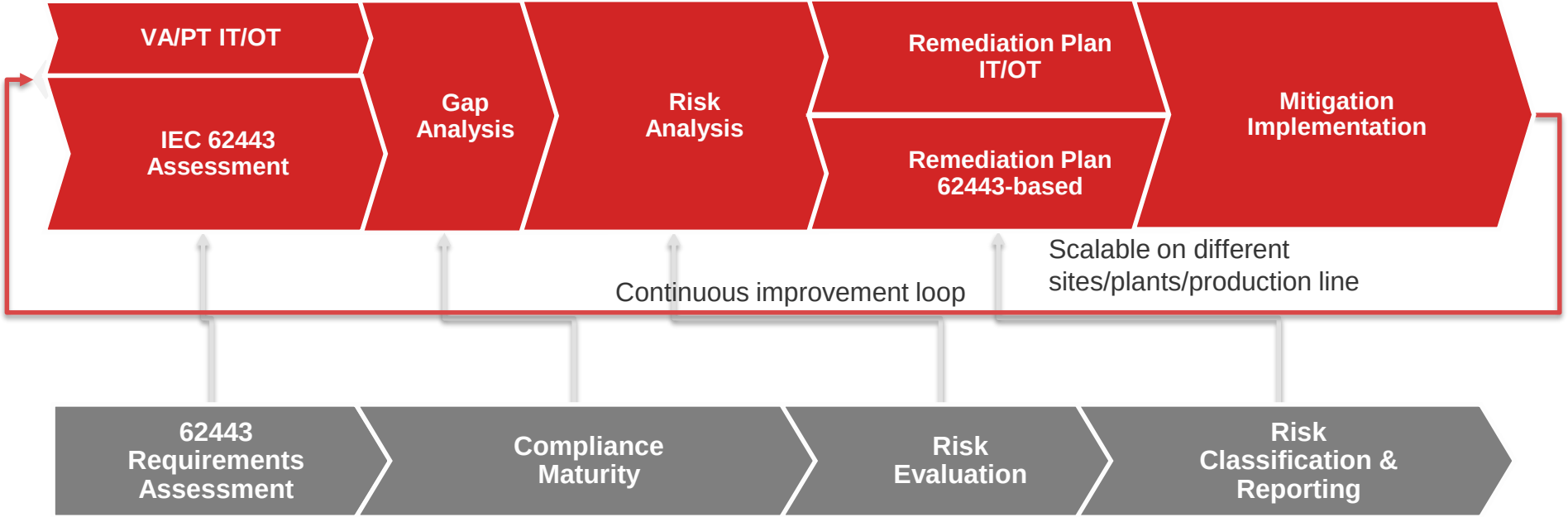
- **ISA/IEC 62443-2-1**, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- **ISA/IEC 62443-3-3**, Security for Industrial Automation and Control Systems: System security requirements and security levels

Human * IT

Integrazione con approccio metodologico

HITACHI
Inspire the Next

Il framework IACS **semplifica** la complessità nel **processo di valutazione del rischio degli impianti** industriali ad alta automazione, in accordo ad un **processo rigoroso di mapping** dei requisiti dettati dalla 62443 sui controlli necessari a mitigare i rischi



Human * IT

4. Criteri di dimensionamento

Parametri di dimensionamento

La **definizione del perimetro** di intervento è un'**attività complessa** e **difficilmente standardizzabile** vista la diversità intrinseca degli impianti industriali, anche afferenti a simili tipologie di business

Un esempio di elementi da considerare come input per una stima di dimensionamento affidabile può essere fatta a partire dai seguenti elementi infrastrutturali:

- Numeri di host di gestione afferenti all'area produttiva
- Numero isole produttive
- Lunghezza linee di produzione
- Altro

Grazie

Michele Onorato
Security Office Manager

Human*IT

Superior service empowered by combining
the strength of our people and information technology.

Hitachi Systems CBT S.p.A.

HITACHI

Inspire the Next