ASSOCIAZIONE IMPRESE ITALIANE
DI STRUMENTAZIONE

GARANTIRE LA CYBER RESILIENCE ATTRAVERSO LE NORMATIVE EMERGENTI

Focus nuovo regolamento macchine

Relatrici

Micaela CASERZA MAGRO

- Presidente GISI
- Direttore Tecnico - GFCC

Valentina MUSSI

- Cybersecurity & Digital Sales Manager - Bureau Veritas Italia

Normazione cybersecurity

Nuovo Reg.Macchine

CYBERSECURITY NELLA GESTIONE DELLA SICUREZZA MACCHINE

- La pubblicazione, nel giugno 2023, del nuovo Regolamento Macchine Ue 2023/1230 porta in primo piano il tema della **cyber security** e **dell'adozione di protocolli per prevenire e limitare le conseguenze di possibili attacchi informatici.**

- Il Regolamento, che entrerà in vigore il 20 gennaio 2027, "**stabilisce i requisiti di sicurezza e di tutela della salute per la progettazione e costruzione di macchine e prodotti correlati e quasi-macchine**" e ne disciplina la messa a disposizione e la messa in servizio all'interno dell'Unione europea (Art. 1, Regolamento Ue 2023/1230).

COSTRUTTORI

UTENTE-CLIENTE

Valutazione del rischio CYBER

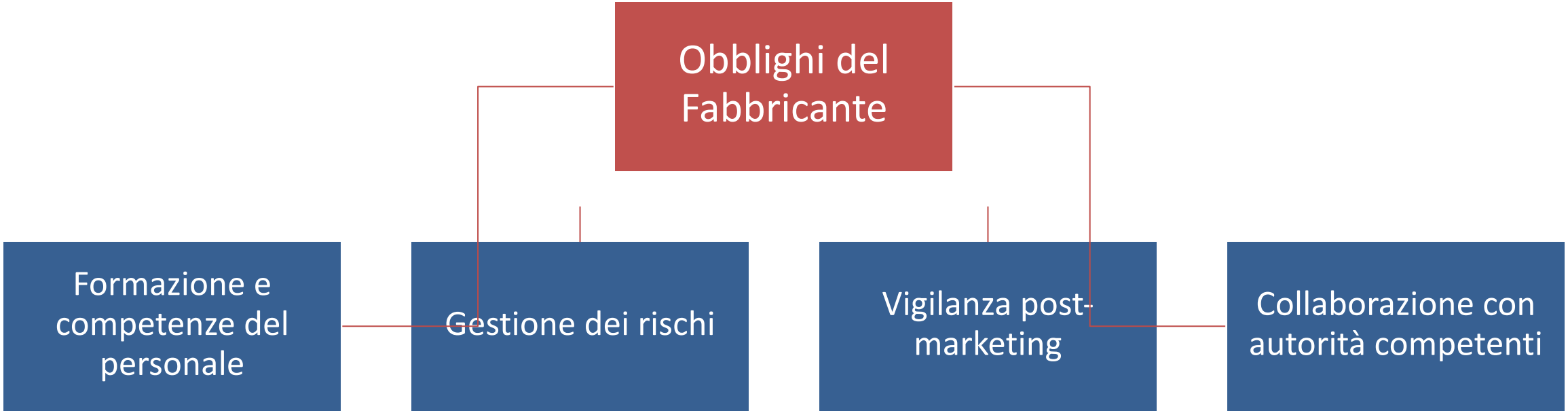
- Identificazione minacce
- Identificazione vulnerabilità
- Calcolo del rischio e contromisure

Fabbricanti

I fabbricanti dovranno soddisfare:

- Sorveglianza del mercato e notifiche di sicurezza
- Autorappresentazione e incaricati responsabili della conformità
- Documentazione tecnica e dichiarazione di conformità
- Marcatura CE
- Sicurezza dei dati e dei dispositivi connessi

Obblighi - fabbricante



Utente – Cliente

End user

Formazione e competenze del personale

Valutazione dei rischi abilitata

Preparazione di un ambiente sicuro

IEC 62443

General	**IEC 62443-1-1** Terminology, Concepts and Models	**IEC TR-62443-1-2** Master Glossary of Teams and Abbreviations	**IEC 62443-1-3** System Security Conformance Metrics	**IEC 62443-1-4** IACS Security Lifecycle and use-cases	
Policies & Procedures	**IEC 62443-2-1** Establishing an Industrial Automation and Control System Security Program	**IEC TR-62443-2-2** Master Glossary of Teams and Abbreviations	**IEC TR-62443-2-3** System Security Conformance Metrics	**IEC TR-62443-2-4** IACS Security Lifecycle and use-cases	**IEC 62443-2-5** Implementation Guidance for IACS Asset Owners
System	**IEC TR-62443-3-1** Terminology, Concepts and Models	**IEC 62443-3-2** Master Glossary of Teams and Abbreviations	**IEC 62443-3-3** System Security Conformance Metrics		
Component	**IEC 62443-4-1** Product Development Requirements	**IEC 62443-4-2** Technical Security Requirements for IACS Components			

APPROCCIO INTEGRATO

Ruoli:

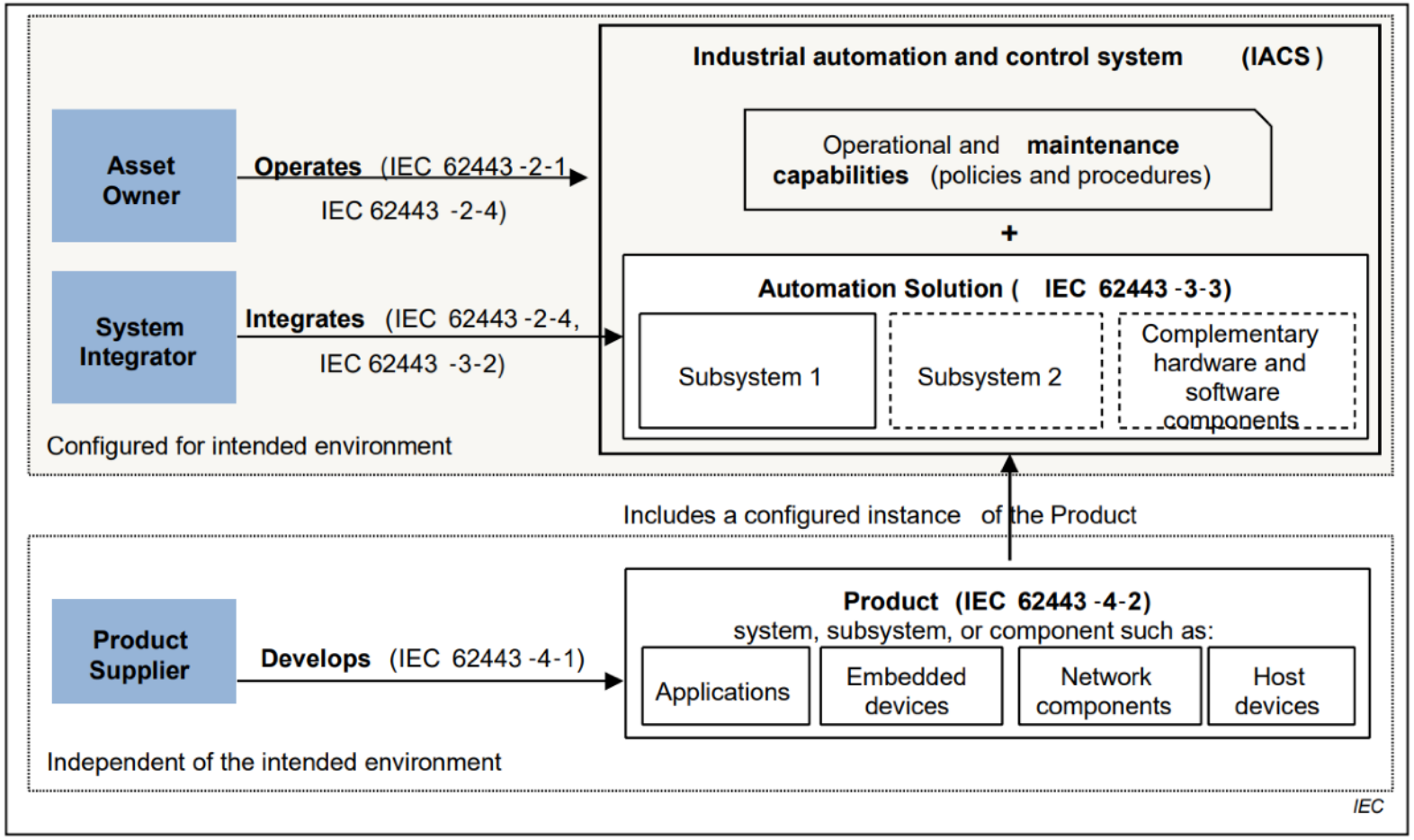
1. **Manufacturer**
2. **Service provider**
3. **Asset owner**

DEFINIZIONE DEI RUOLI: ASSET OWNER, SERVICE PROVIDER, MANUFACTURER

Ruoli e competenze

Ruoli:

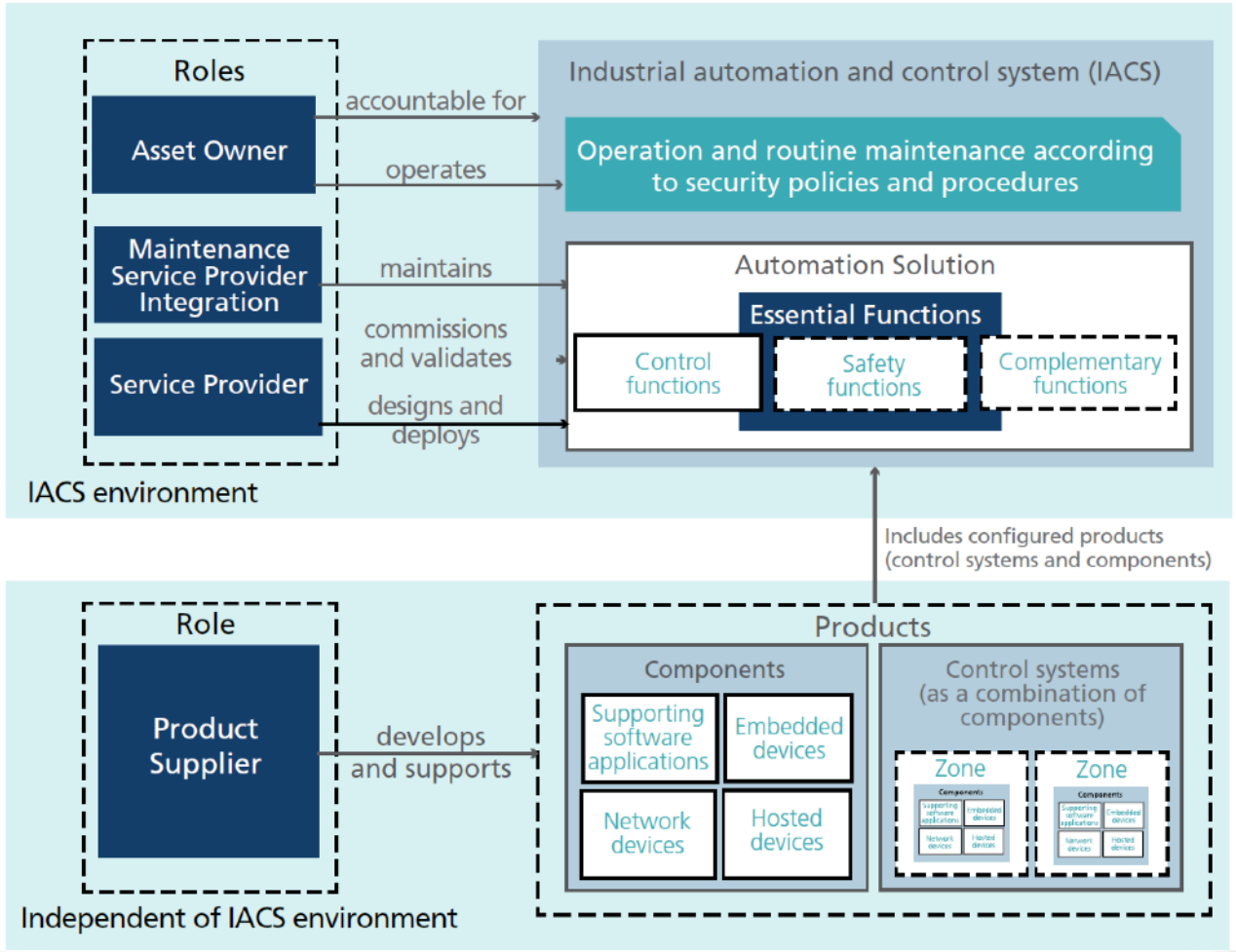
1. Manufacturer
2. Service provider
3. Asset owner



Framework

I **service provider** sono coinvolti dal commissionamento (system integrator)

Fino alla manutenzione (maintenance service provider)



METRICHE PER LA VALUTAZIONE DEGLI ASPETTI DI SECURITY: MATURITY LEVEL E SECURITY LEVEL

Security Level

LE MINACCE

- **Livello 0**
  - ➢ Non sono necessari né specifici requisiti né protezioni di sicurezza
- **Livello 1**
  - ➢ Necessaria protezione contro errori accidentali (errori degli impiegati)
- **Livello 2**
  - ➢ Necessaria protezione contro azioni volontarie compiute da soggetti con mezzi comuni, poche risorse, skills generiche riguardo I sistemi di controllo e bassa motivazione (Hacker amatoriali)
- **Livello 3**
  - ➢ Necessaria protezione contro azioni volontarie compiute da soggetti con mezzi sofisticati, risorse moderate, skill specifiche riguardo I sistemi di controllo e moderata motivazione (Hacker professionisti, hacktivisti)
- **Livello 4**
  - ➢ Necessaria protezione contro azioni volontarie compiute da soggetti con mezzi sofisticati, risorse estese, skill specifiche riguardo I sistemi di controllo e alta motivazione (nazioni e terroristi)

Security Level

7 REQUISITI FONDAMENTALI

1. **Identification and authentication control (IAC)**
   - ➢ Capacità di identificare ed autenticare in maniera affidabile tutti gli utenti (umani, dispositivi e processi software)
2. **Use control (UC)**
   - ➢ Capacità di assegnare privilegi/ autorizzazioni ad un utente precedentemente autenticato
3. **System integrity (SI)**
   - ➢ Garanzia che il sistema non venga manipolato
4. **Data confidentiality (DC)**
   - ➢ Garanzia delle confidenzialità
5. **Restricted data flow (RDF)**
   - ➢ Capacità di segmentare la rete dividendola in zone e condotti per limitare il traffico di rete e ridurre la superficie di attacco
6. **Timely response to events (TRE)**
   - ➢ Capacità di rispondere ad eventuali attacchi
7. **Resource availability (RA)**
   - ➢ Garantire la disponibilità del sistema

Security Level

LE DECLINAZIONI

➢ Vanno a formare un «security vector» dove viene indicato il livello di sicurezza richiesto per ognuno di questi. Esso ha il seguente formato:

- SL-? ([FR,] domain) = {IAC UC SI DC RDF TRE RA} dove:
  - SL-?: può essere SL-T, SL-A, SL-C
  - FR: indica quali FR sono presenti
  - Domain: dominio di applicazione che può rifersi all'intero sistema, a un sottosistema o ad un componente
  - {IAC UC SI DC RDF TRE RA} : contiene il livello di sicurezza richiesto

➢ Alcuni esempi:

- SL-C(SIS Engineering Workstation) = { 3 3 2 3 0 0 1 }
- SL-C(RA, FS-PLC) = 4

➢ 3 tipi di SL :

Target SL (SL-T)

Achieved SL (SL-A)

Capability SL (SL-C)

Maturity Level

LE DECLINAZIONI

➢ Le parti dello standard 2-4, 3-2, 4-1, dove sono presenti i requisiti richiesti in termini di processi, policies e procedure vengono valutate tramite i maturity level.

➢ **Vengono definiti 4 livelli:**

1. Livello **iniziale**: quanto richiesto nel requisito è presente, ma viene svolto in una maniera non documentata;
2. Livello **gestito**: le policies e procedure sono state scritte ed il personale è stato formato ed ha le competenze tali da soddisfare quel requisito;
3. Livello **definito**: si aggiunge al livello precedente che il processo è stato applicato almeno una volta;
4. Livello **ottimizzabile**: il processo si può misurare ed è possibile applicare un continuo miglioramento.

Grazie per la Vostra partecipazione e attenzione

GISI
ASSOCIAZIONE IMPRESE ITALIANE
DI STRUMENTAZIONE