Elementi essenziali e gestione della sicurezza informatica per il settore energetico

CSP001_C_E

PRESENTAZIONE DI:
CRISTINA ALCARAZ
UNIVERSITÀ DI MALAGA, SPAGNA

Ringraziamenti

- *Cofinanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili per essi.*
- *Accordo di progetto n. 101083594*

Argomento 2: Conoscenze fondamentali e tassonomia della sicurezza informatica energetica e corpus di conoscenze

Panoramica

- Definire la sicurezza informatica energetica e la sua importanza nel settore energetico
- Comprendere i vari componenti di un ecosistema di sicurezza informatica energetica
- Classificare le minacce e le vulnerabilità alla sicurezza informatica specifiche dei sistemi energetici
- Panoramica del corpus di conoscenze sulla sicurezza informatica

CSP001_C_E – ARGOMENTO 2:
Cristina Alcaraz, Università di Malaga, Spagna

Argomento 2: Conoscenze di base e tassonomia della sicurezza informatica energetica e corpus di conoscenze

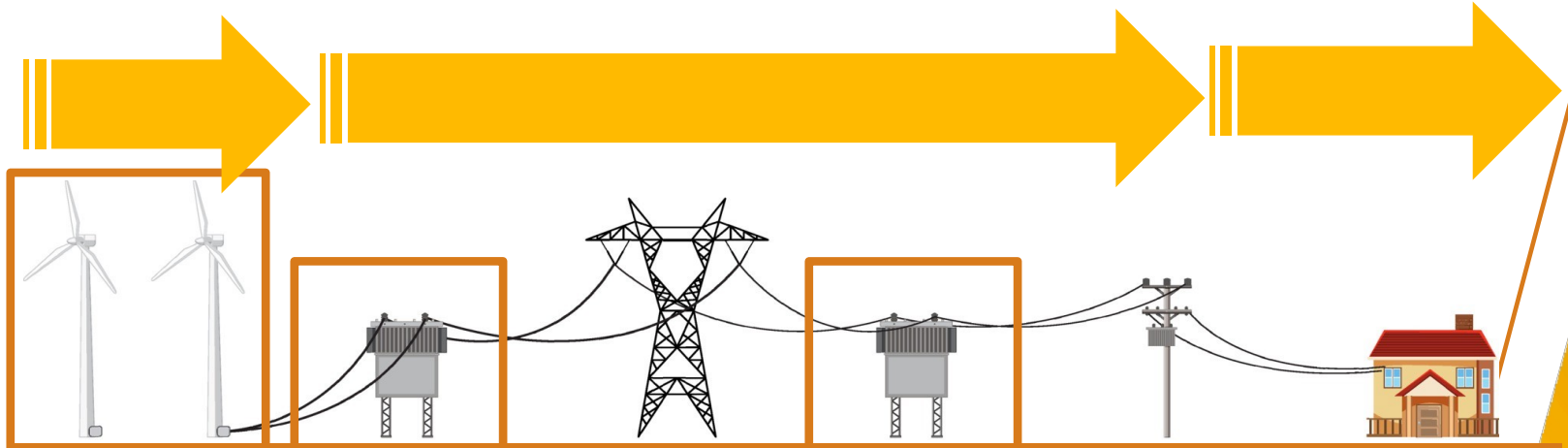
Panoramica

- Definire la sicurezza informatica energetica e la sua importanza nel settore energetico
- **Comprendere i vari componenti di un ecosistema di sicurezza informatica energetica**
- Classificare le minacce alla sicurezza informatica e le vulnerabilità specifiche dei sistemi energetici
- Panoramica del corpus di conoscenze sulla sicurezza informatica

Cristina Alcaraz, Università di Malaga, Spagna

Fasi operative tipiche dei sistemi di alimentazione elettrica

- I sistemi elettrici tradizionali seguono solitamente procedure sistematiche,
  - in cui una serie di apparecchiature industriali e dispositivi operativi sono configurati per **produrre e trasportare energia** agli utenti finali



Sia la produzione di energia elettrica che la sua trasformazione per il trasporto vengono effettuate nelle sottostazioni energetiche: *sottoreti fisiche distribuite intorno e in prossimità delle infrastrutture critiche, composte da sottoreti di controllo con controller, sensori, attuatori e altri componenti.*

Fonte dell'immagine: Vecteezy URL:https://www.vecteezy.com

Fasi operative tipiche dei sistemi di alimentazione

- Più specificamente, nei sistemi di alimentazione si distinguono tre fasi operative:
  - **La produzione di energia** comprende meccanismi e componenti in grado di generare grandi quantità di energia, con la capacità aggiuntiva di immagazzinarla e/o distribuirla tramite tralicci.

Fasi operative tipiche dei sistemi di alimentazione

- Più specificamente, nei sistemi di alimentazione elettrica si distinguono tre fasi operative:
  - **La produzione di energia** comprende meccanismi e componenti in grado di generare grandi quantità di energia, con la capacità aggiuntiva di immagazzinarla e/o distribuirla tramite tralicci
  - **La trasmissione di energia** ha lo scopo di trasportare grandi quantità di elettricità con carichi elevati su lunghe distanze (tramite tralicci) ed è supportata principalmente da sistemi di stoccaggio e generazione nelle sottostazioni

Fasi operative tipiche dei sistemi di alimentazione

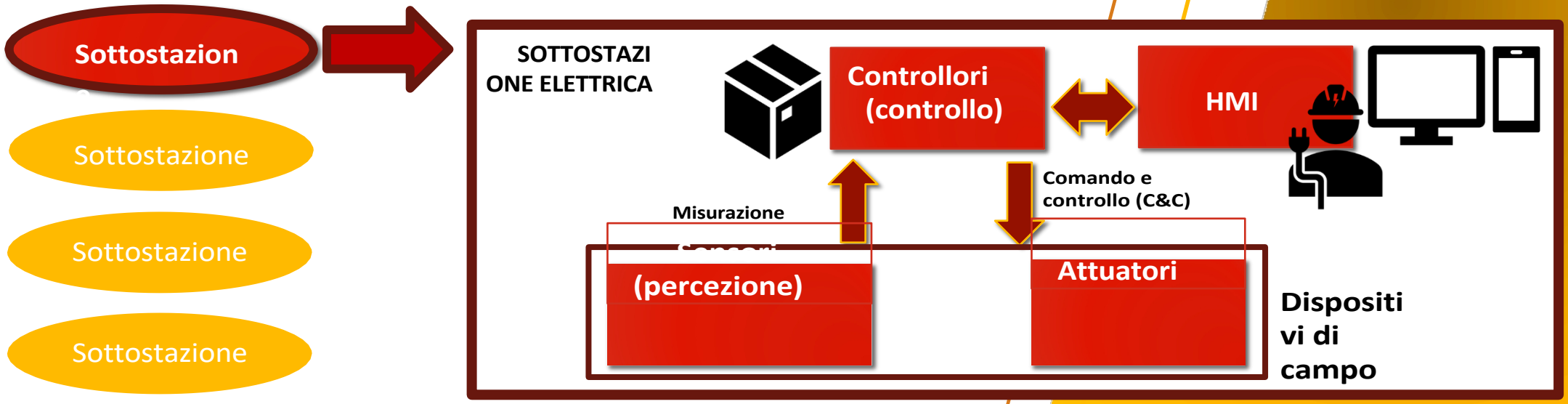
- Più specificamente, nei sistemi di alimentazione elettrica si distinguono tre fasi operative:
  - **La produzione di energia** incorpora meccanismi e componenti in grado di generare grandi quantità di energia, con la capacità aggiuntiva di immagazzinarla e/o distribuirla tramite tralicci
  - **La trasmissione di energia** ha lo scopo di trasportare grandi quantità di elettricità con carichi elevati su lunghe distanze (tramite tralicci) ed è supportata principalmente da sistemi di stoccaggio e generazione nelle sottostazioni
  - **La distribuzione dell'energia** consiste nel trasporto di elettricità a un'intensità accettabile per il suo consumo finale, probabilmente con il supporto di sistemi di stoccaggio e generazione nelle sottostazioni situate vicino agli utenti finali

Fasi operative tipiche dei sistemi di alimentazione elettrica

- Riassumendo:
  - **La produzione di energia** comprende meccanismi e componenti in grado di generare grandi quantità di energia, con l'ulteriore capacità di immagazzinarla e/o distribuirla tramite tralicci – PER PRODURRE GRANDI QUANTITÀ DI ENERGIA
  - **La trasmissione di energia** mira a trasportare grandi quantità di elettricità con carichi elevati su lunghe distanze (tramite tralicci) e si avvale principalmente di sistemi di stoccaggio e generazione presso sottostazioni – PER INTENSIFICARE IL VOLUME PER IL SUO TRASPORTO
  - **La distribuzione dell'energia** consiste nel trasportare l'elettricità a un'intensità accettabile per il suo consumo finale, probabilmente con il supporto di sistemi di stoccaggio e generazione nelle sottostazioni situate vicino agli utenti finali - PER RIDURRE IL VOLUME PER IL SUO CONSUMO

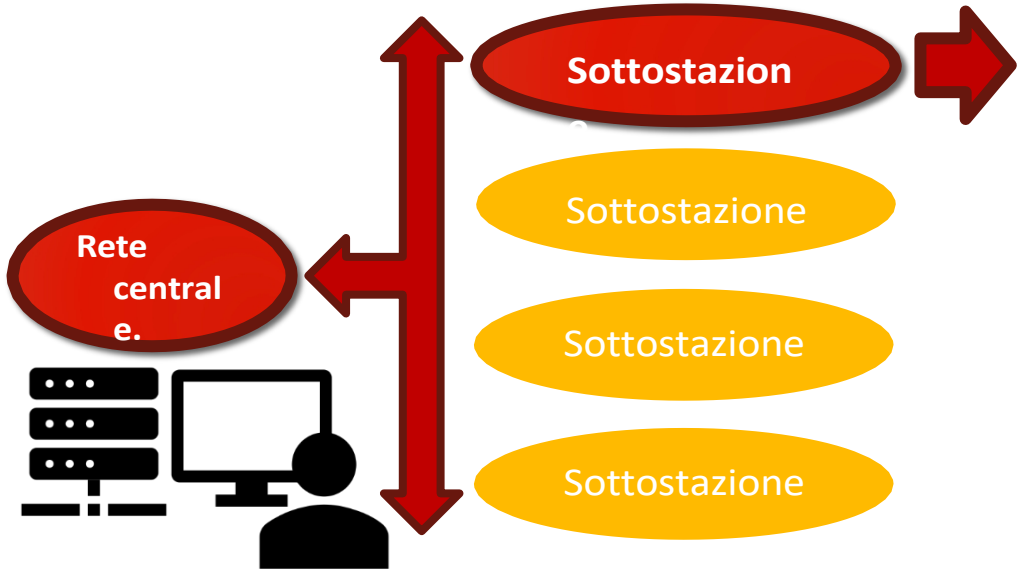
Tecnologie operative tipiche dei sistemi di alimentazione

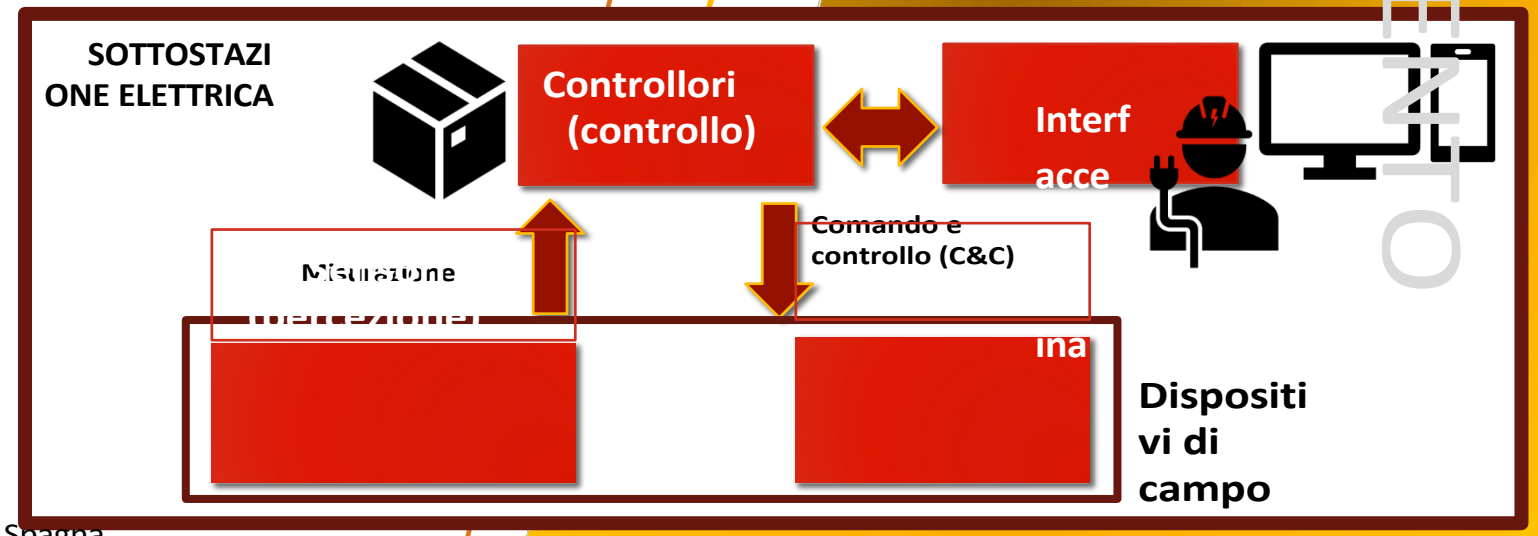
- Ogni sottostazione si basa su una serie di tecnologie operative di gestione (OT), quali:
  - **Dispositivi di campo** quali sensori e attuatori
  - **Controller** quali unità terminali remote (RTU) / controllori logici programmabili (PLC) collegati a dispositivi di campo
  - **Interfacce uomo-macchina** (HMI)



Tecnologie operative tipiche dei sistemi di alimentazione

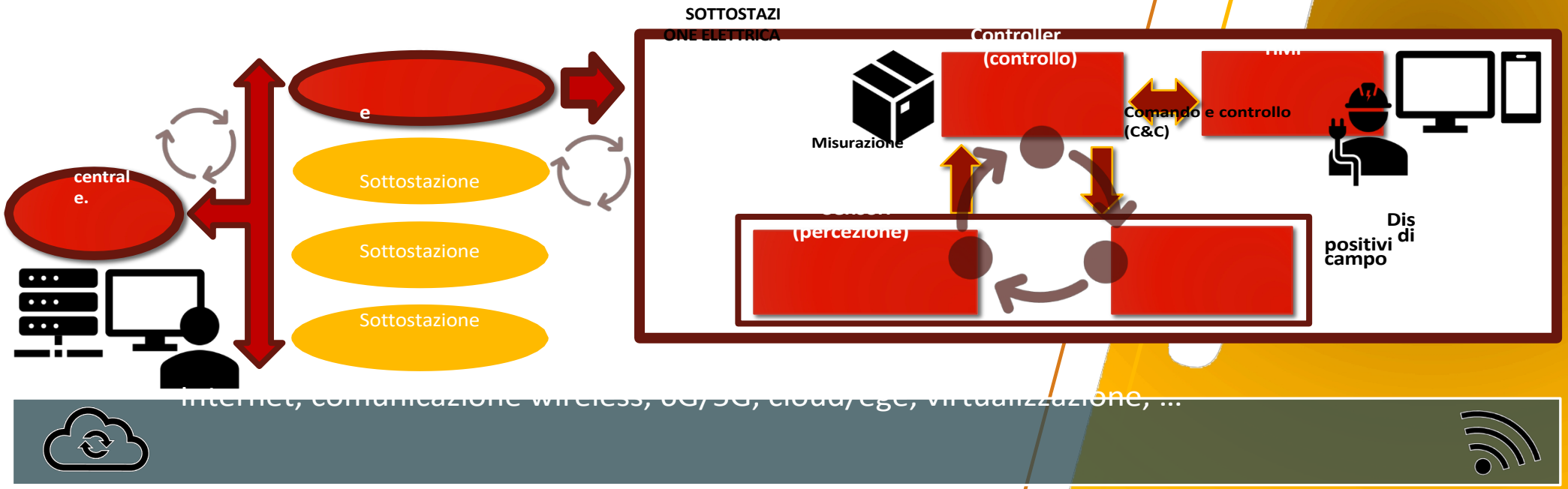
- Pertanto, grazie ai controllori, gli operatori umani possono avere **un quadro chiaro dello stato dell'intero sistema (o di una sua parte)** e controllarlo localmente o da remoto.
  - Gli operatori umani devono ricevere le informazioni (dinamiche/processi fisici) dal contesto tramite sensori e controllori
  - Gli operatori umani devono agire sul contesto tramite controllori e attuatori





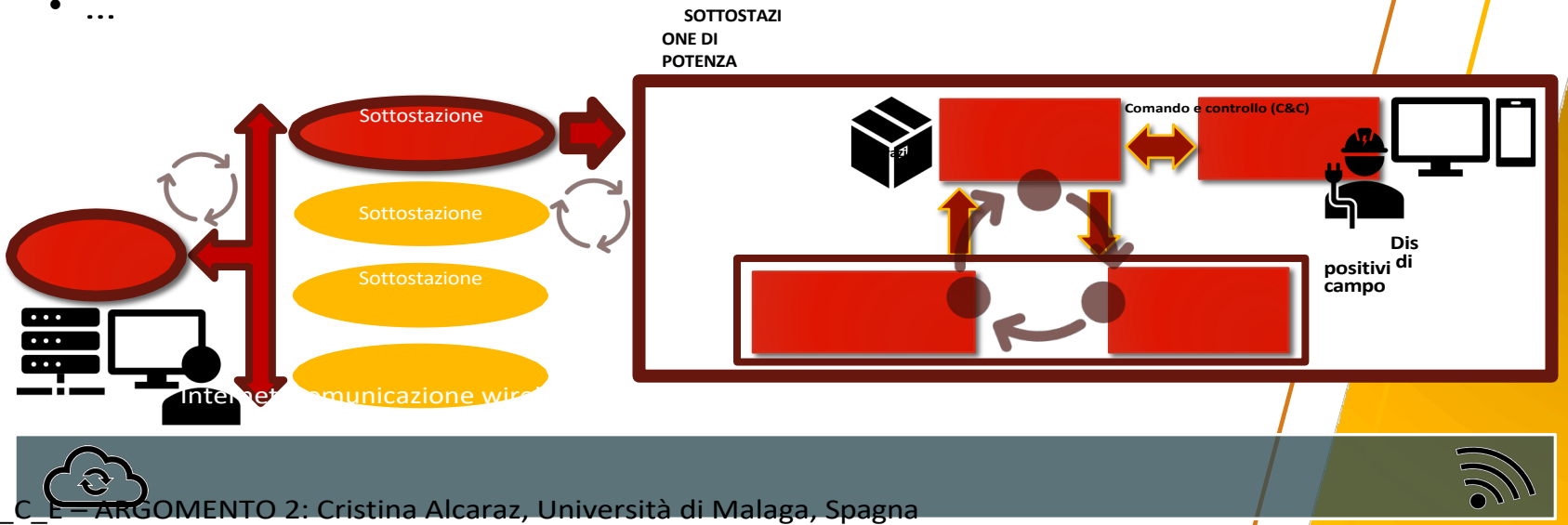
Tecnologie operative tipiche dei sistemi di alimentazione

- Per ottenere questo tipo di controllo, emergono diversi tipi di **tecnologie dell'informazione e della comunicazione (TIC)**
  - Grazie alle TIC, gli operatori umani possono monitorare e controllare (localmente/da remoto) i processi/dispositivi fisici installati in prossimità delle infrastrutture critiche, creando una sorta di rete centrale a circuito chiuso



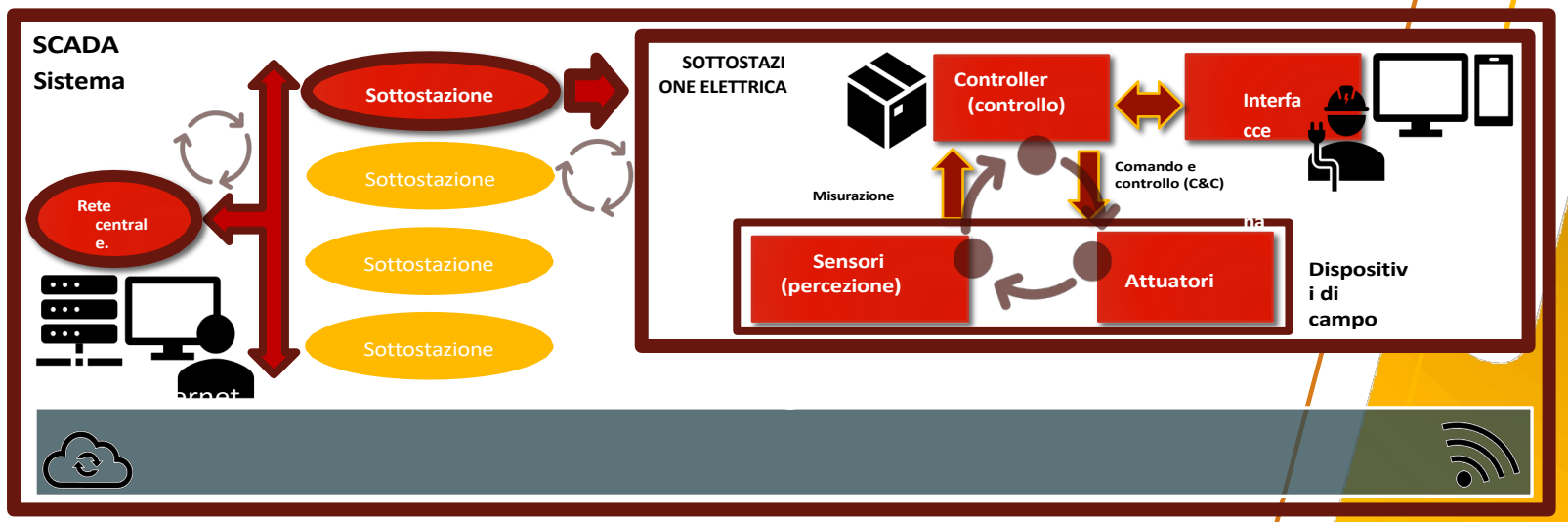
Tecnologie operative tipiche dei sistemi di alimentazione

- L'interconnessione di sistemi e componenti può essere effettuata tramite:
  - Comunicazione seriale o TCP/IP
  - Server gateway/backend
  - Infrastrutture cloud/edge
  - Protocolli di comunicazione industriale: ModbusTCP, DNP3, IEC 104, S7, OPC UA,…
  - Protocolli di comunicazione IoT: MQTT, CoAP, HTTPS, ecc.
  - …



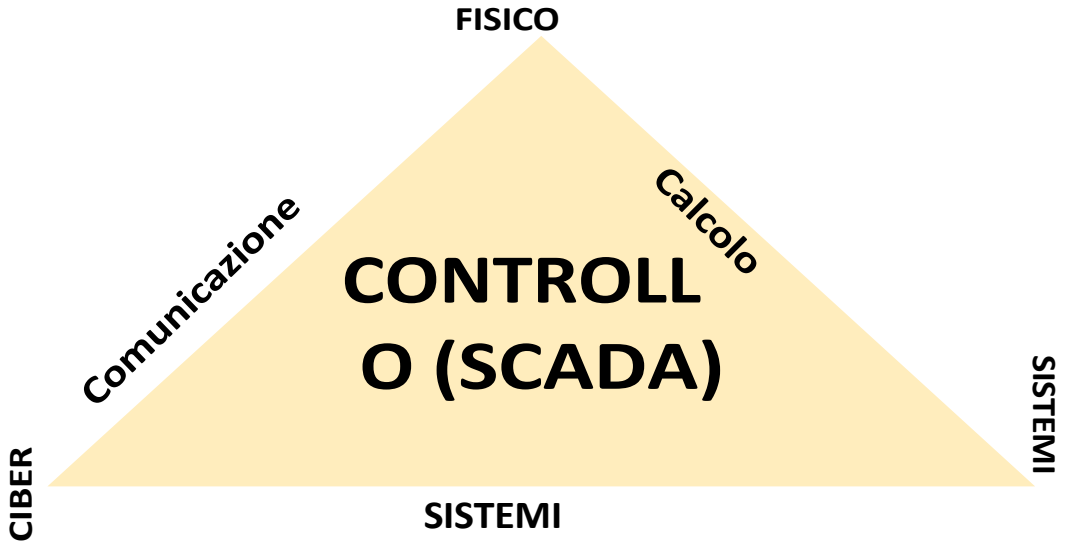
Tecnologie operative tipiche dei sistemi di alimentazione

- L'unione di queste sottoreti dà origine al concetto di sistemi **SCADA (Supervisory Control and Data Acquisition, controllo di supervisione e acquisizione dati).**
- I sistemi SCADA sono reti in grado di:
  - Elaborare grandi volumi di dati provenienti da controller o gateway (I)IoT
  - Analizzare e modificare gli stati dell'ambiente osservato tramite i controller o i gateway (I)IoT



Nuova concettualizzazione del controllo nei sistemi di alimentazione

- Ora, da una prospettiva olistica, possiamo introdurre il noto concetto di "Sistema **Cyber-Fisico**" (CPS), introdotto da Helen Gill della National Science Foundation degli Stati Uniti nel 2006
  - Lei concepisce il termine CPS come il modo di combinare e integrare il calcolo con i processi fisici, ma anche la comunicazione.

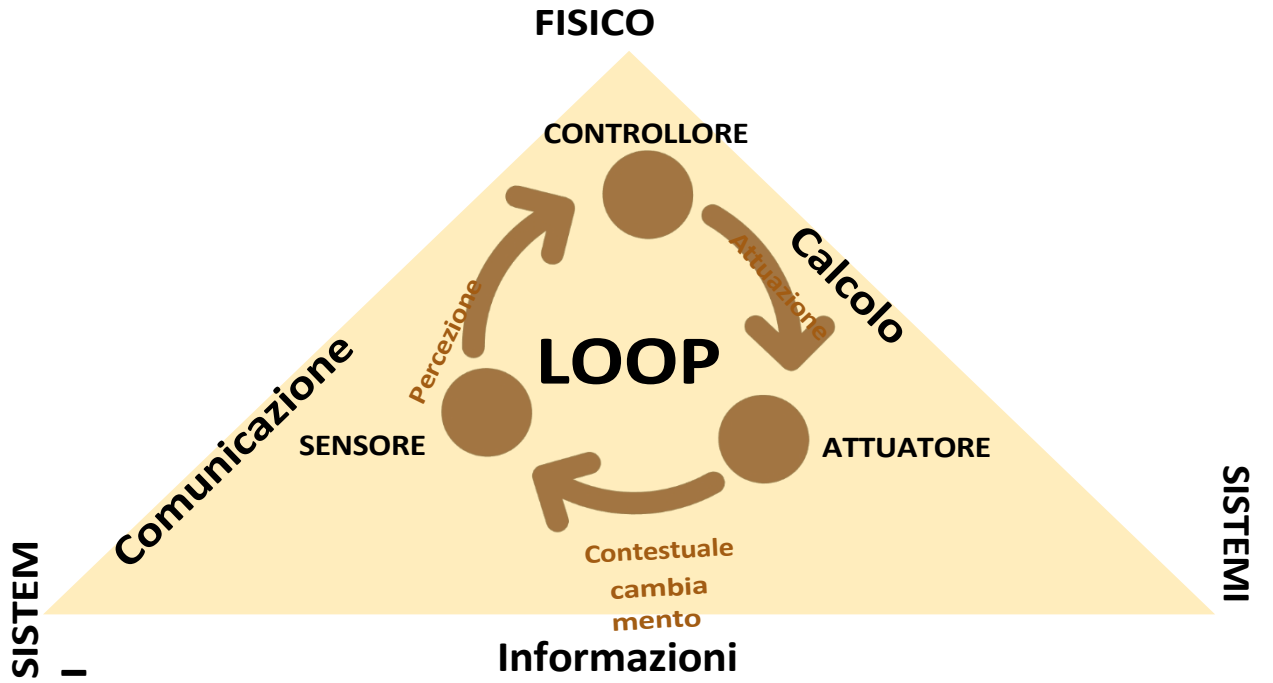


Il CPS può essere inteso come una **nuova disciplina in grado di catturare una serie di teorie, tecniche e componenti di controllo** quali: sistemi embedded, sistemi in tempo reale, sistemi ibridi (compresa l'IT), teoria del controllo, reti di sensori, metodi formali, tra gli altri.

Fonte: S. A. Seshia, "Explorations in cyber-physical systems education" (*Esplorazioni nell'educazione ai sistemi cyber-fisici*), *Communications of the ACM*, *65*(5), 60-69, 2022

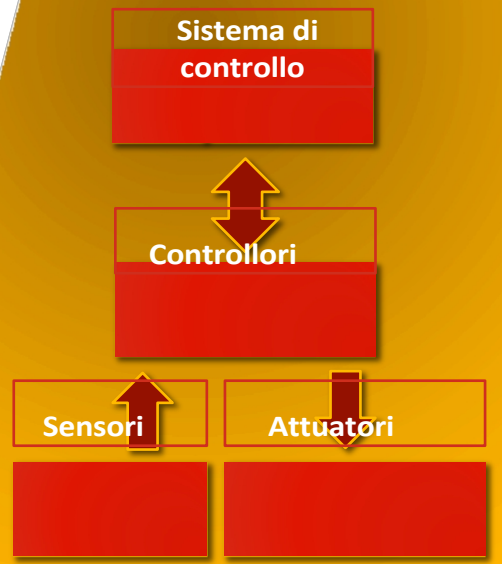
Nuova concettualizzazione del controllo nei sistemi di alimentazione elettrica

- Se espandiamo gli elementi di controllo principali nei sistemi SCADA, otteniamo la seguente struttura:



Inoltre, ogni sottostazione può essere considerata come un CPS per sua natura

Pertanto, un CPS è un sistema in grado di **integrare e orchestrare una serie di** componenti **di calcolo e comunicazione** per elaborare dinamiche/processi fisici del "mondo reale"
(e seguendo un ciclo chiuso).

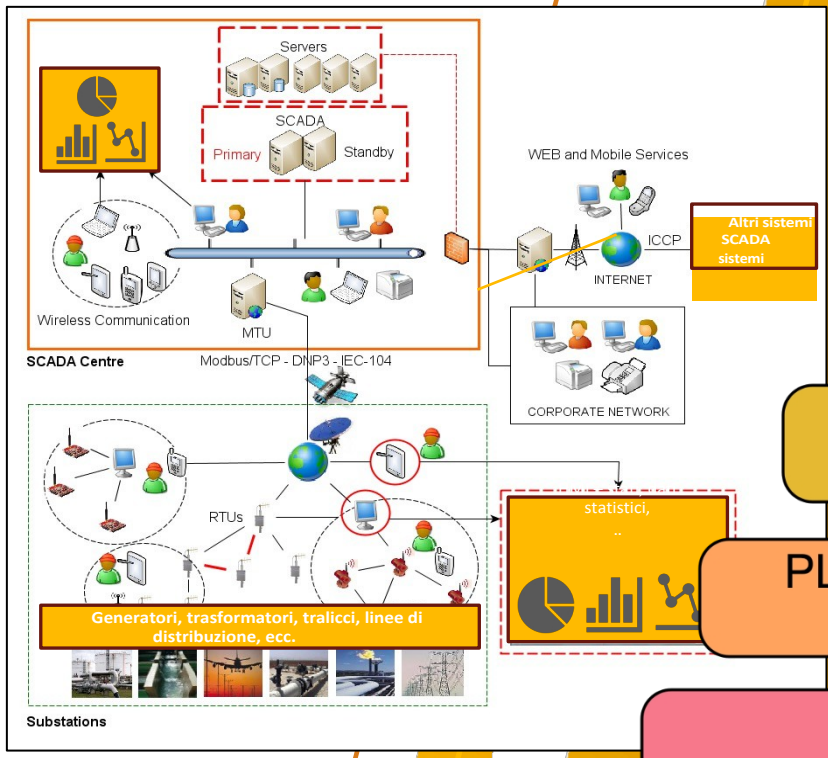


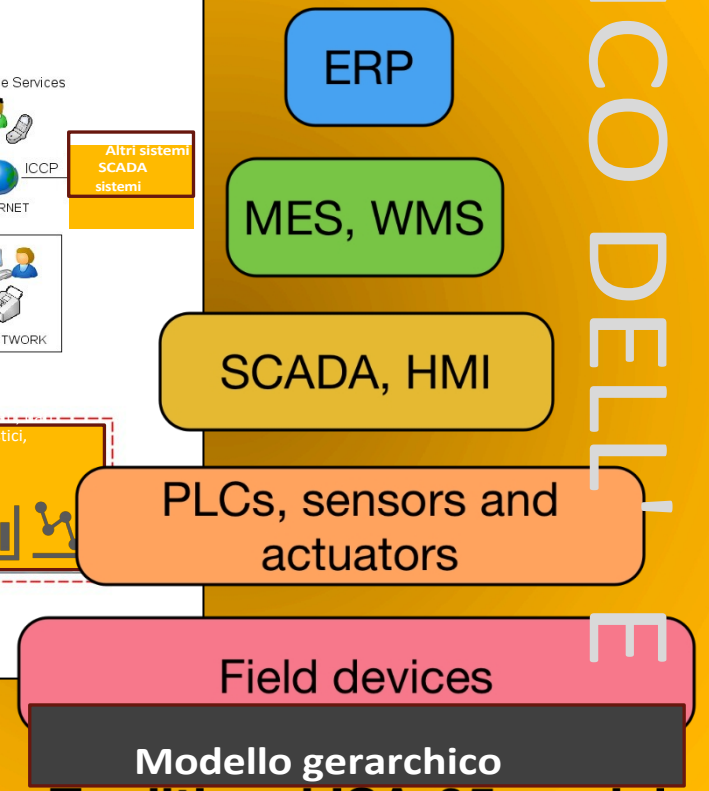
CLASSICO O OPERATIVO

Fonte: S. A. Seshia, "Explorations in cyber-physical systems education" (*Esplorazioni nell'educazione ai sistemi cyber-fisici*), *Communications of the ACM*, *65*(5), 60-69, 2022

Architetture di controllo tipiche

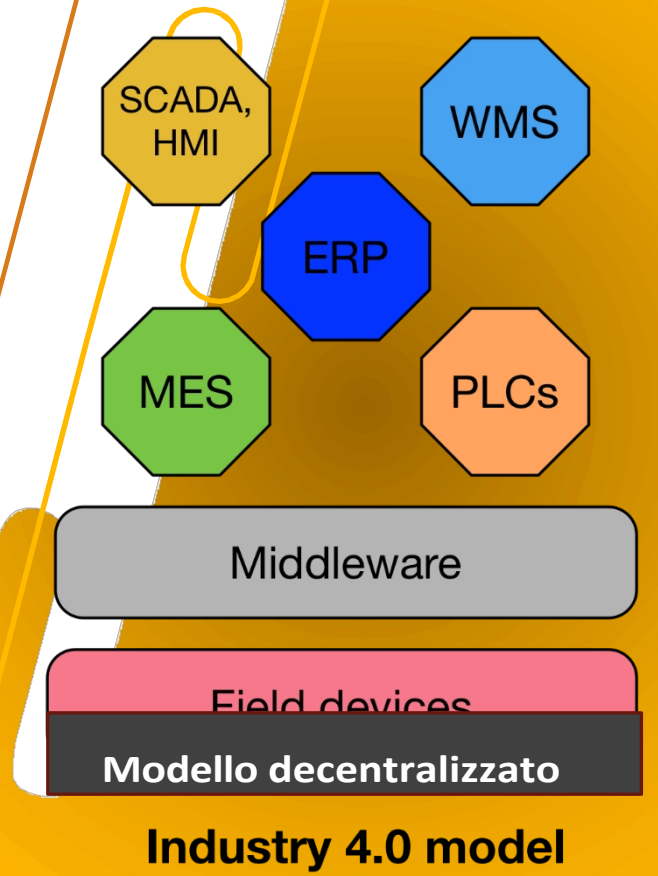
- Per introdurre le attuali architetture di controllo, è necessario innanzitutto tornare ai sistemi di controllo tradizionali
- Osservando la figura, possiamo notare che i sistemi SCADA sono composti principalmente da tre reti principali, che seguono una rigorosa **architettura gerarchica**:
  - Reti aziendali
  - La rete di controllo
  - Sottostazioni
- L'architettura segue il tradizionale modello ISA-95



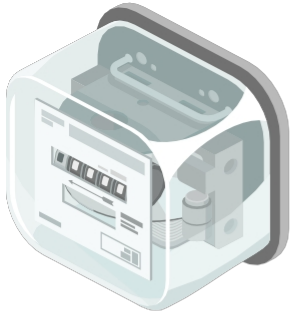


Architetture di controllo moderne

- Tuttavia, questa concettualizzazione gerarchica è attenuata dall'attuale necessità di
  - Modernizzare i processi operativi
  - Digitalizzare, decentralizzare e personalizzare processi e servizi
  - Controllare operazioni, processi e servizi da qualsiasi luogo, in qualsiasi momento e in qualsiasi modo
- L'idea è quella di creare un nuovo modo di controllare in modo intelligente la produzione di energia e la sua distribuzione senza sprechi energetici
  - in modo che le sottostazioni siano in grado di "*produrre energia in base alla domanda effettiva*"
- Questa evoluzione verso una nuova concettualizzazione di *"ecosistema intelligente*" è ciò che porta il settore energetico a diventare: **Sistema Smart Grid**



Architetture di controllo moderne

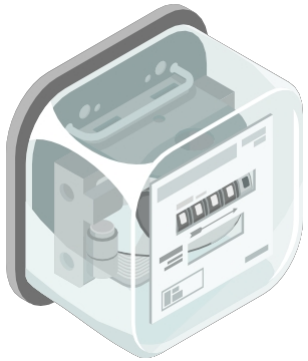


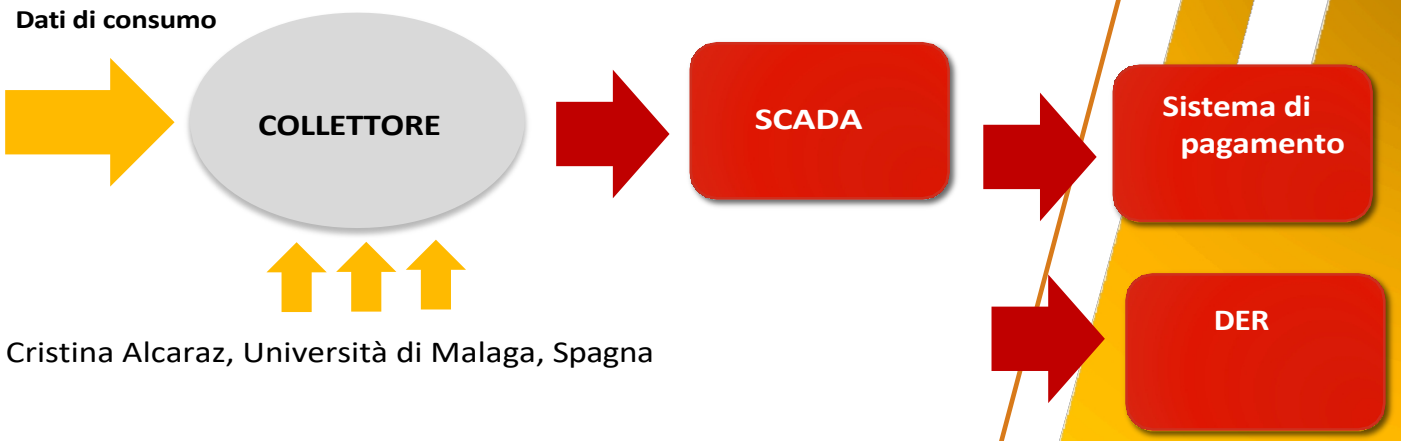
- Per creare un ecosistema "intelligente" in grado di produrre energia in base alla domanda effettiva, è necessario:
  - Collegare i sistemi di controllo con il mondo reale (le città) attraverso **contatori intelligenti**, che rilevano dinamicamente il consumo effettivo
  - Intensificare la cooperazione tra le parti interessate, nonché la catena di approvvigionamento energetico nell'ambito dei quadri normativi
- Tra le **parti interessate**, segnaliamo:
  - Operatori di rete quali:
    - Gestori dei sistemi di trasmissione (TSO)
    - Gestori di sistemi di distribuzione (DSO)
  - Fornitori o prestatori di servizi per facilitare l'uso dell'energia
  - Autorità o regolatori per stabilire le regole di funzionamento
  - Consumatori/prosumatori

Fonte dell'immagine: Vecteezy URL:https://www.vecteezy.com

Architetture di controllo moderne

- Come accennato in precedenza, **i contatori intelligenti** sono componenti operativi essenziali per rilevare in modo dinamico il consumo energetico effettivo in una o più aree.
- I contatori intelligenti sono normalmente collegati a collettori per trasferire i valori di consumo e consentono di
  - Il sistema di controllo di produrre e distribuire dinamicamente l'energia per area
  - Il sistema di pagamento di calcolare il valore finale dei consumi

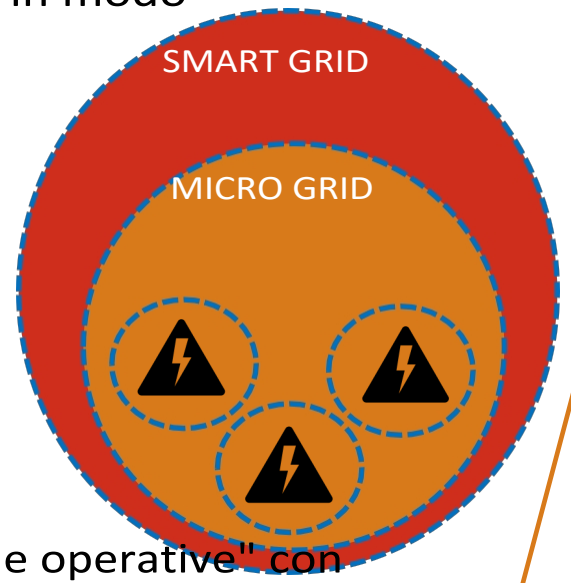




Fonte dell'immagine: Vecteezy URL:https://www.vecteezy.com

Dalle reti intelligenti alle micro-reti e alle risorse energetiche distribuite

- Nell'ambito delle reti intelligenti, stanno emergendo **sistemi basati su microgrid** per produrre energia in modo modo "sicuro"
- Le microgrid corrispondono a mini-sottostazioni distribuite vicino all'utente finale, il cui scopo principale è quello di:
  - Fornire energia a livello locale
  - Collegarsi alla rete principale per trasferire/ricevere energia
- Questo tipo di implementazione crea "isole operative" con l'obiettivo di aumentare:
  - la "resilienza" riducendo l'impatto di potenziali interruzioni

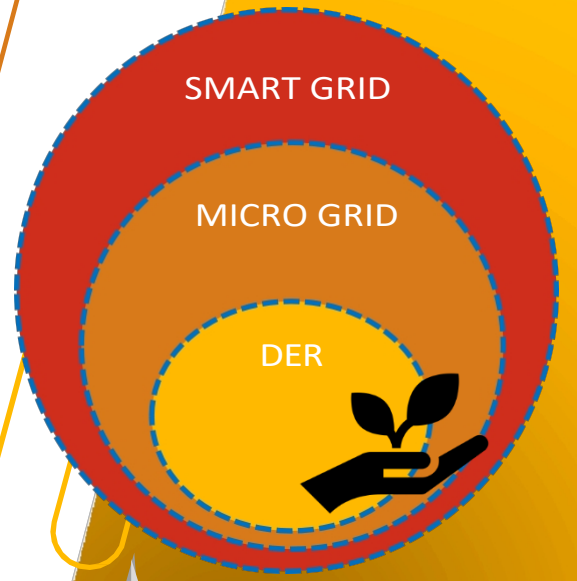


CLASSICO DELL'

Dalle reti intelligenti alle micro-reti e alle risorse energetiche distribuite

- Nel contesto delle microgrid, possiamo anche trovare
  - **Risorse energetiche distribuite** (DER)
    - Sistemi rinnovabili come pannelli solari o parchi eolici
    - Sistemi di accumulo
    - Veicoli elettrici (EV) - Le batterie degli EV possono restituire energia alla rete se esiste il V2G
  - **Sistemi di controllo**
  - **Contatori intelligenti**

Il Vehicle-to-Grid (V2G) si basa su tecnologie che consentono di reimmettere energia nella rete dalle batterie dei veicoli elettrici

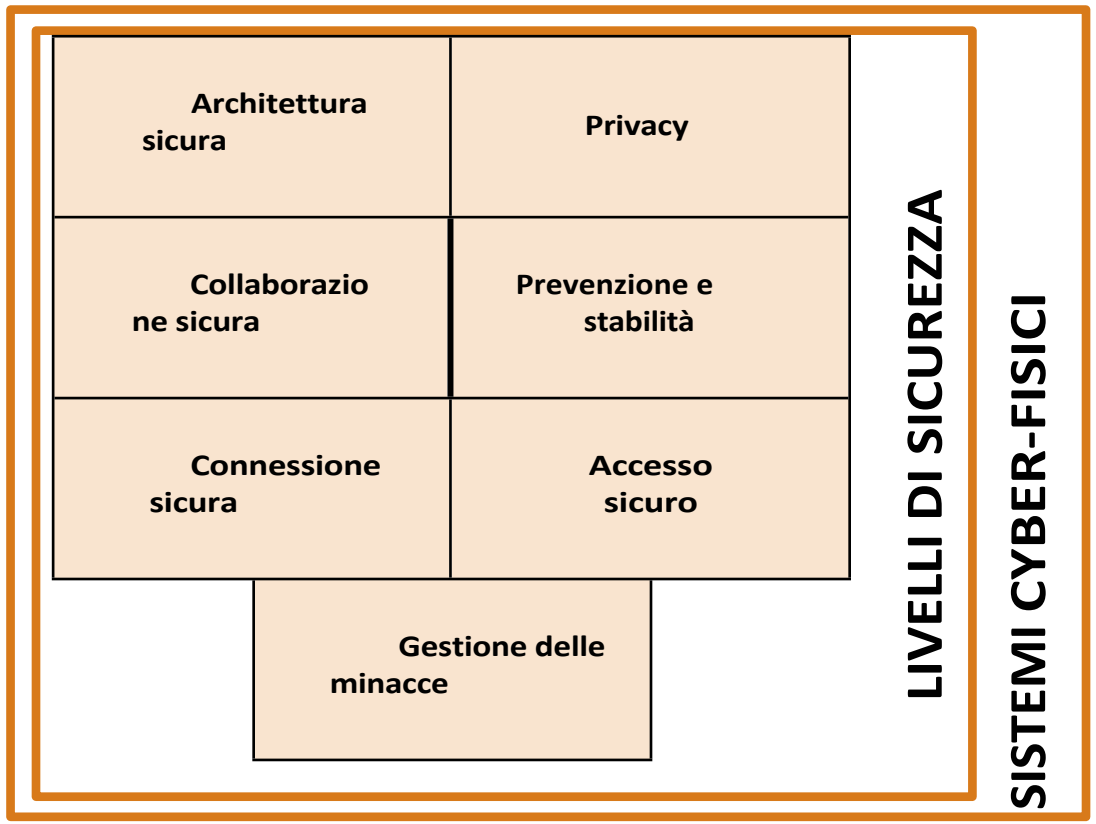


CLASSICO DELL'

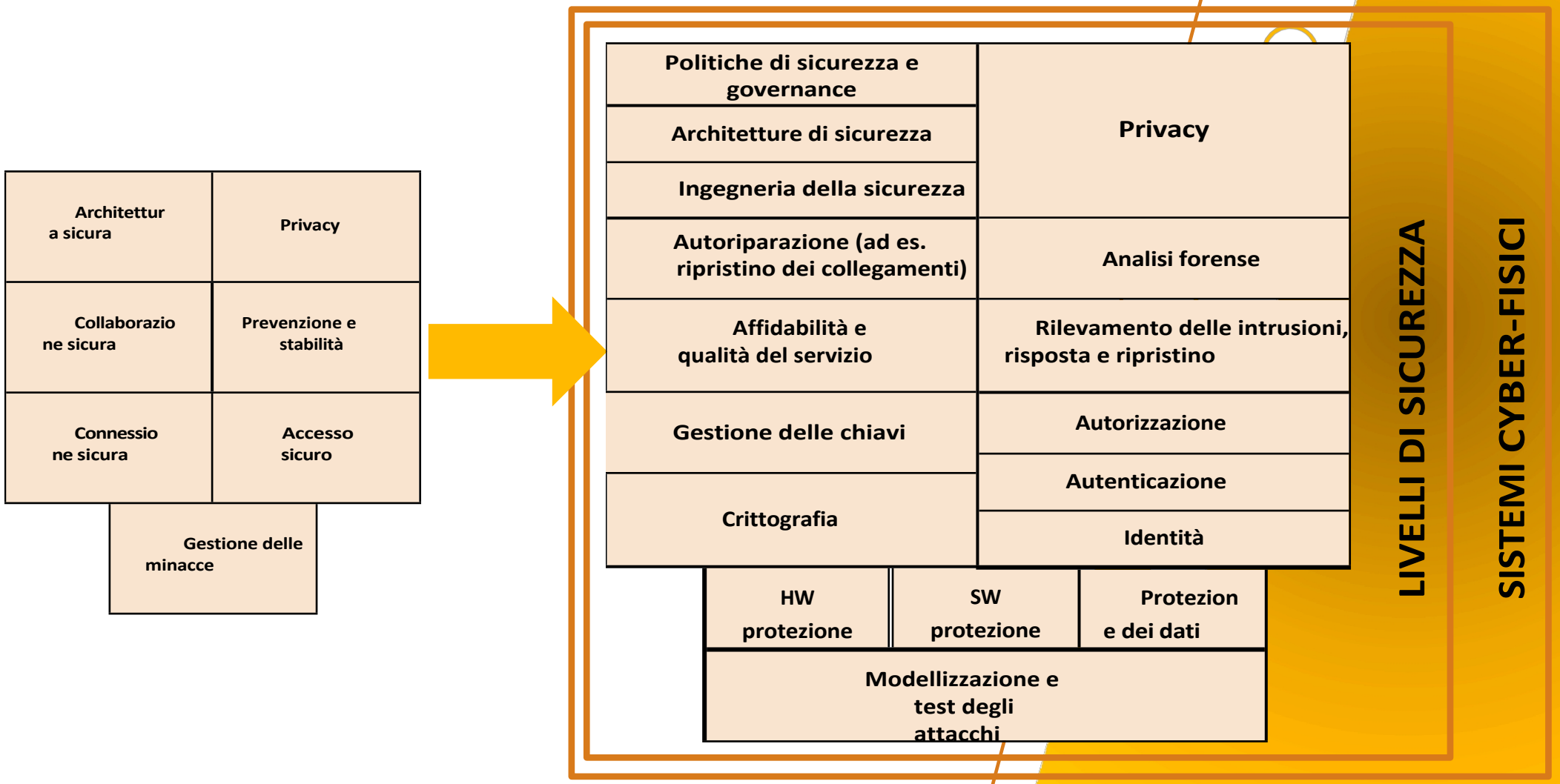
Fonte dell'immagine: Vecteezy URL:https://www.vecteezy.com

Altri componenti rilevanti in ecosistema di sicurezza informatica energetica

- Oltre ai componenti operativi tipici e moderni, è anche essenziale considerare altri elementi rilevanti relativi alla sicurezza informatica e ai relativi livelli di protezione



Altri componenti rilevanti in ecosistema di sicurezza informatica energetica



COOPERRAATTIOONN

CSP001_C_E – ARGOMENTO 2: Cristina Alcaraz, Università di Malaga, Spagna

Considerazioni finali

- Abbiamo esaminato la funzionalità dei sistemi energetici convenzionali e moderni e abbiamo esplorato i componenti principali di un ecosistema di sicurezza informatica energetica, quali:
  - Sottostazioni di controllo e loro principali componenti cyber-fisici, che includono ICT e protocolli
  - Sistemi SCADA
  - Sistemi Smart Grid e microgrid
  - DER
  - Contatori intelligenti
  - Parti interessate
- Abbiamo anche introdotto e collegato il concetto di CPS al settore energetico per gestire le nuove terminologie, nonché i componenti di sicurezza informatica.

Riferimenti e fonti

1. Alcune immagini sono state prese da Vecteezy, URL: https://www.vecteezy.com/ - grazie!
2. DeepL Translator per la revisione:
   URL: https://www.deepl.com/translator
3. S. A. Seshia, "Explorations in cyber-physical systems education", Communications of the ACM, 65(5), 60-69, 2022

Connettiti con CyberSecPro: Come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Per qualsiasi domanda, non esitate a contattare:

- Cristina Alcaraz
  Professore associato
  Università di Malaga
  alcaraz@uma.es