UNIVERSITÀ DI TRENTO

Dipartimento di
Ingegneria e Scienza dell'Informazione

Corso di Laurea in
Ingegneria Informatica, delle Comunicazioni ed Elettronica

Presentazione elaborato finale

Modellazione di Minacce Informatiche in Ambiente Smart Grid Cloud-Native

Supervisore
Prof. Domenico Siracusa

Laureando
Cristiano Berardo - 234428

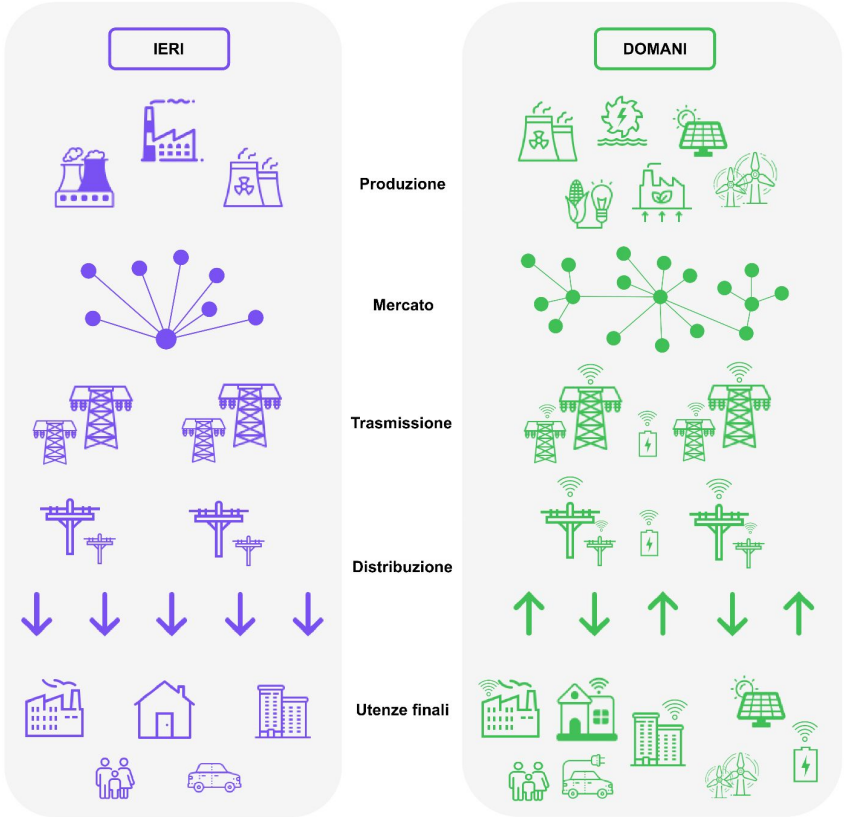
Smart Grid: Introduzione e Architettura

Generazione di energia distribuita

Prosumer

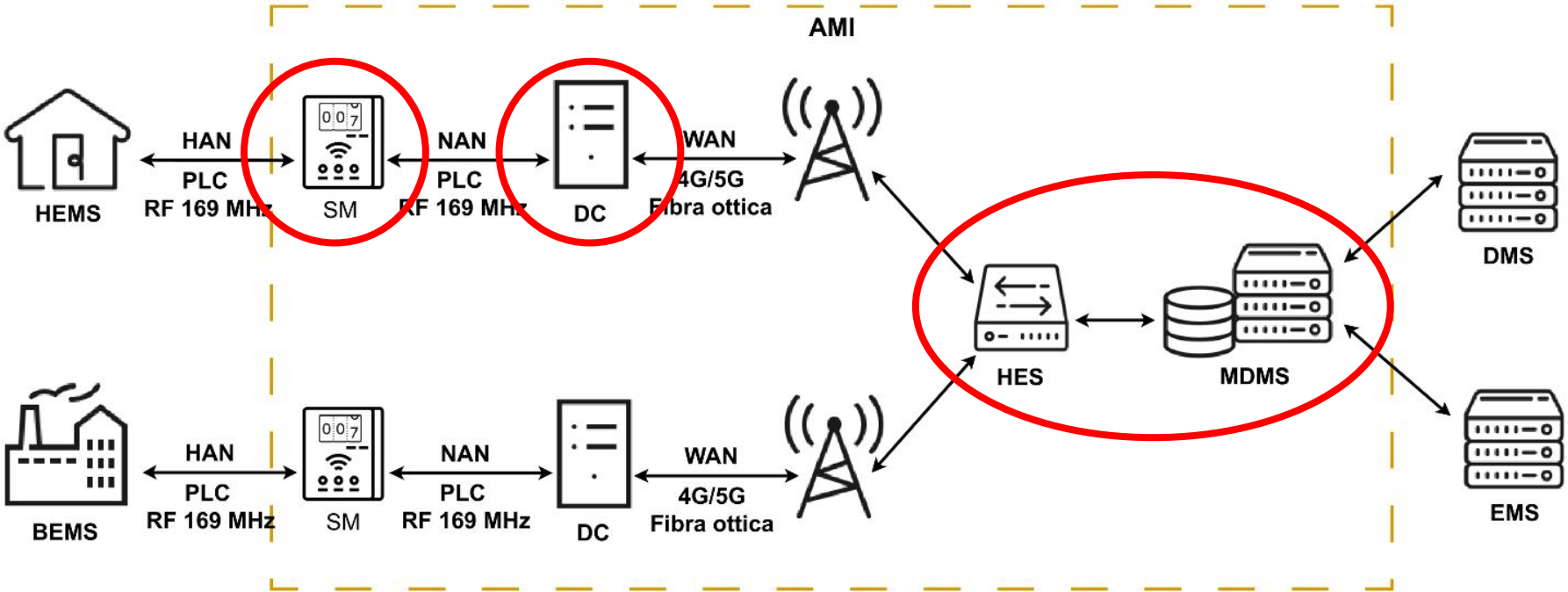
Flussi bidirezionali

Smart Grid è l'evoluzione dell'infrastruttura energetica tradizionale: sensoristica, comunicazione e controllo



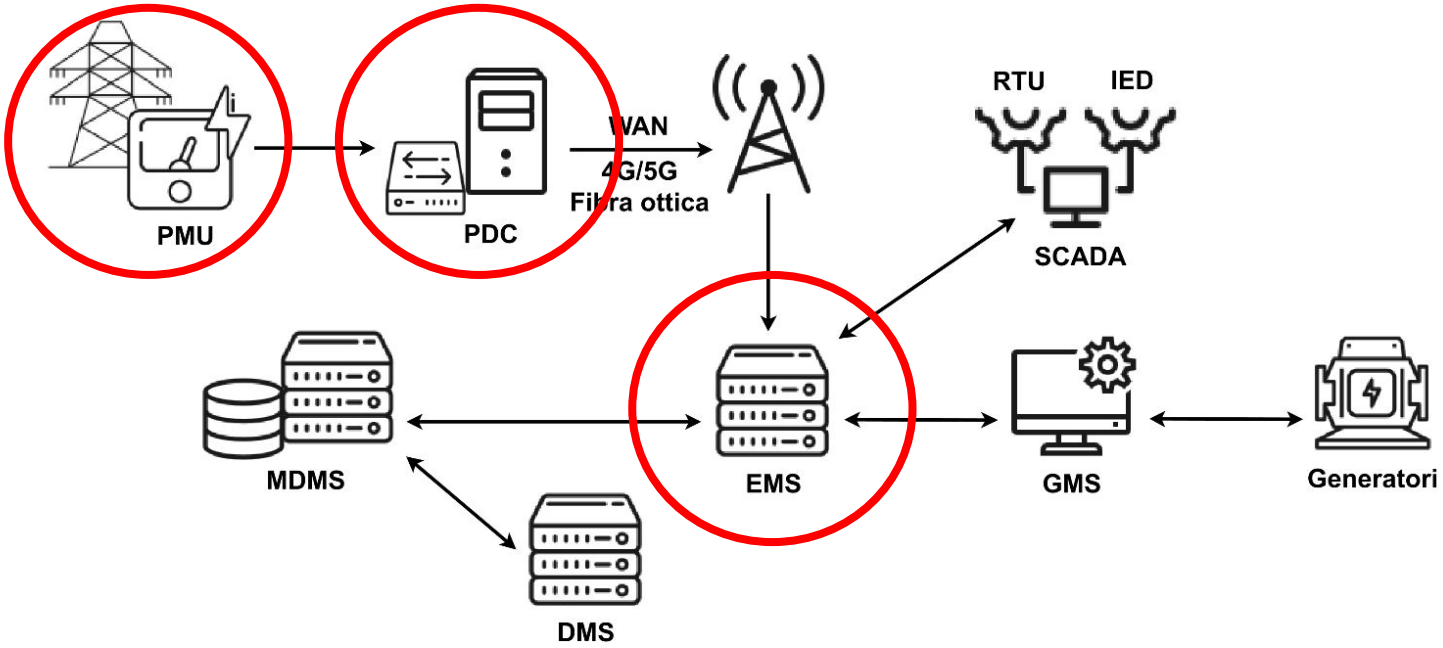
Smart Grid: Dominio del Consumatore

Rappresenta l'interfaccia diretta tra la rete e il consumatore



Smart Grid: Dominio Operazionale

Qui operano sistemi di controllo critici utilizzati degli operatori per regolare in tempo reale domanda e offerta di elettricità



Smart Grid: l'evoluzione e lo stato dell'arte attuale

Hardware specifico

Funzioni logiche su hardware generico: il cloud

Approccio a logica di microservizi

Aumenta esponenzialmente la superficie di attacco

Smart Grid: introduzione all’architettura cloud proposta

Microservizi per software complesso

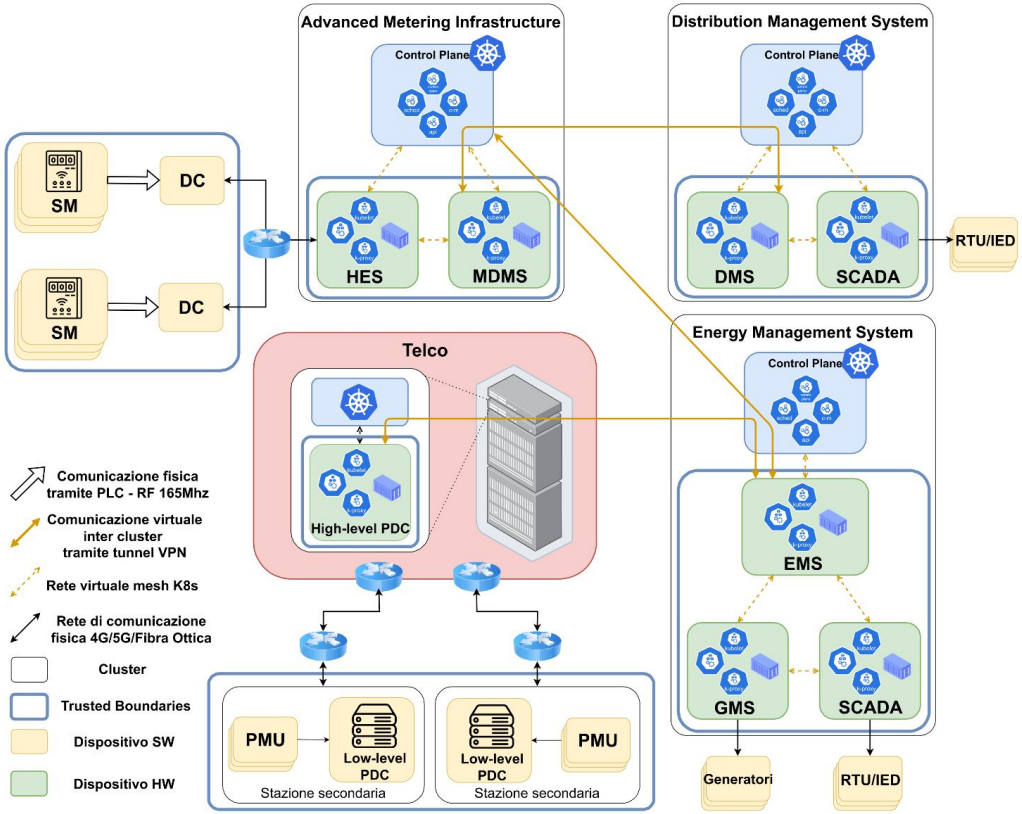
Gestione attraverso Docker container e orchestratore Kubernetes

Smart Grid: L'architettura Cloud-Native proposta

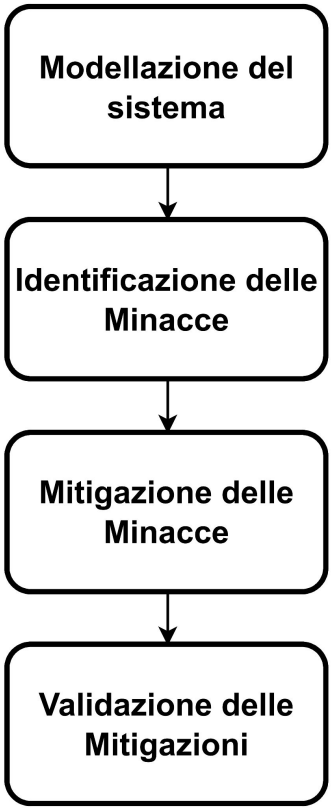
Federazione di cluster Kubernetes indipendenti

Uno per ogni dominio funzionale per garantire:

- Robustezza
- Sicurezza
- Autonomia operativa

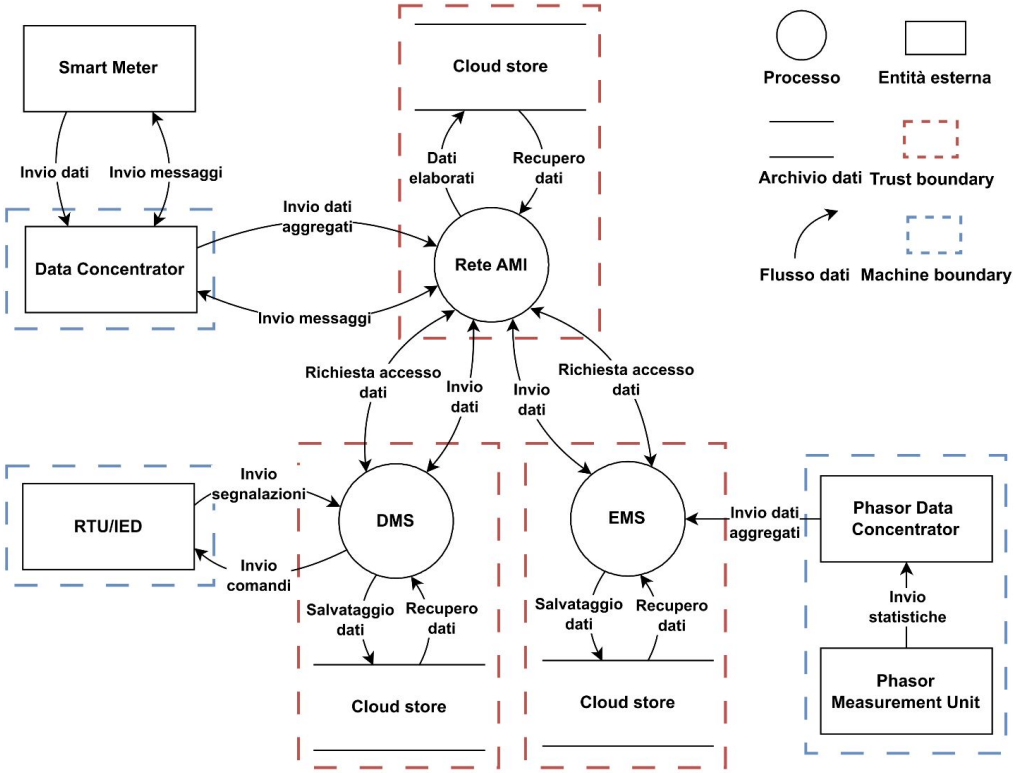


Threat Modeling: il framework STRIDE e le sue quattro fasi



Spoofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege[8]

Threat Modeling: Modellazione del sistema



Modellazione del sistema → Identificazione delle minacce → Mitigazione delle minacce

Threat Modeling: Identificazione delle minacce

Information Disclosure	Vulnerabilità presenti nei software open source come ad esempio OpenEMS o librerie.
Denial of Service	Accedendo alle cabine secondarie l'attaccante individua il servizio SCADA. Usando hping può lanciare un attacco DoS verso il canale causando latenza.

Modellazione del sistema → **Identificazione delle minacce** → Mitigazione delle minacce

Threat Modeling: Mitigazione delle minacce

Information Disclosure	Code review e utilizzo delle best practise di sicurezza e implementative
Denial of Service	Il router è il punto debole della comunicazione con il servizio SCADA. Utilizzando regole di firewall appropriate si impedisce di intaccare il servizio [1]

[1] Filip Holik, Lars Halvdan Flå, Martin Gilje Jaatun, Sule Yildirim Yayilgan, and Jørn Foros.
Threat modeling of a smart grid secondary substation. Electronics, 11(6), 2022.

Modellazione del sistema → Identificazione delle minacce → **Mitigazione delle minacce**

Conclusioni e sviluppi futuri

L’ecosistema Smart Grid presenta numerose sfide e complessità

La rete elettrica è essenziale per qualsiasi servizio dall’azienda al privato cittadino e bisogna garantire la sua resilienza

Sviluppi futuri: testare l’architettura presentata e validare le mitigazioni proposte