

Cybersecurity priorities and challenges in the digital-energy transition

Giovanna Dondossola

Digital and Cybersecurity Knowledge Exchange
World Bank Study Tour Italy

May 27, 2026
Milan, Ramada Plaza Hotel, Via Stamira d'Ancona 27



PNIEC 2030



Integrated National Plan for Energy and Climate

- "To achieve the necessary developments in energy security... we cannot ignore the strengthening and **digitalization** of infrastructure."
- "The spread of **self-consumption** will naturally be favored by the diffusion of **digital technologies**, along with the **Internet of Things** and **greater accessibility to small- and medium-sized generation and storage systems.**"
- "Digitalization will play a **cross-sectoral enabling role**, offering opportunities for acceleration across **the entire battery sector**. **Digital twins and big data analytics** will be crucial for the advancement of **battery management systems (BMS).**"
- "Achieving ambitious **decarbonization goals** requires, in addition to a **high degree of reliability, security, and flexibility** of the national energy system, its **substantial integration with digital technologies**, ensuring both **optimized management of renewable energy production** and the enabling of **greater electrification of consumption.**"

Regulatory process

Energy

Cybersecurity





- **EU Network Codes 2017/1485** System Operation Guideline (SOGL), responsibilities of data exchanges between transmission and distribution operators and **significant grid users**, for the purpose of **system operational planning and management close to real time**
- Data exchange requirements defined by Terna within the **National Grid Code A.6**, approved by the Italian Energy Regulatory Authority (ARERA) in February 2020
- ARERA commissioned the standard development to the Italian Electrotechnical Committee (CEI)
- CEI developed the normative project **DER Plant Central Controller** (CCI) of CEI 0-16, a set of monitoring and control functions of DER plants to comply with grid observability obligations, network operation control needs and significant grid users' capabilities to access flexibility markets
- ARERA Resolution 540/2021/R/EEL, the CCI observability functions of CEI 0-16 become mandatory for **production plants with a power capacity ≥ 1 MW connected to medium voltage grids**



- work in progress
- In 2025 Terna updated the network code A.72 on the **national defence plan**
- ARERA resolution 385/2025/R/EEL requires that the **DER Plant Central Controller control function “active power limitation upon DSO command”** in CEI 0-16 standard becomes mandatory for **wind and photovoltaic production plants connected to the medium voltage grids with a power capacity ≥ 100 kW**
- CEI is updating the normative project DER Plant Central Controller (CCI)
 - Communication interface CCI-SPI (Interface Protection System) based on IEC 61850/GOOSE



Standard CEI 0-16 – DER Plant Controller

CEI 0-16 «Reference technical rule for the connection of active and passive Users to the AT and MT networks of electricity distribution companies»

– Annex O – DER Central Controller – CCI

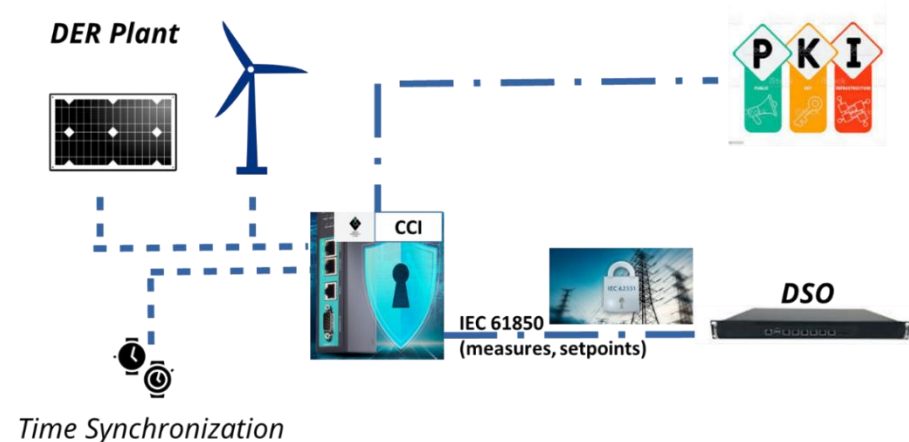
<https://static.ceinorme.it/strumenti-online/doc/EstrattoAllegatoO.pdf>

- CCI functional specification
- **Compliance certifications**

– Annex T – Information exchange based on IEC 61850

<https://static.ceinorme.it/strumenti-online/doc/EstrattoAllegatoT.pdf>

- CCI IEC 61850 data model
- CCI communication interfaces
- CCI IEC 62351 cybersecurity





- Identification, authorization and authentication of remote entities
 - Validation of the CA certificate pre-configured on the CCI
- Authorizations based on entity roles
 - RBAC specification based on IEC 62351-8
 - standard and custom roles
- Secure transport layer
 - Mutual authentication based on digital certificates signed by trusted Authorities
 - Data integrity and confidentiality through cryptographic algorithms: key exchange with asymmetric keys, data encryption with symmetric keys, hashing, digital signatures
- Key and certificate management through PKI
 - Certificate issuing, renewal, revocation, status validation



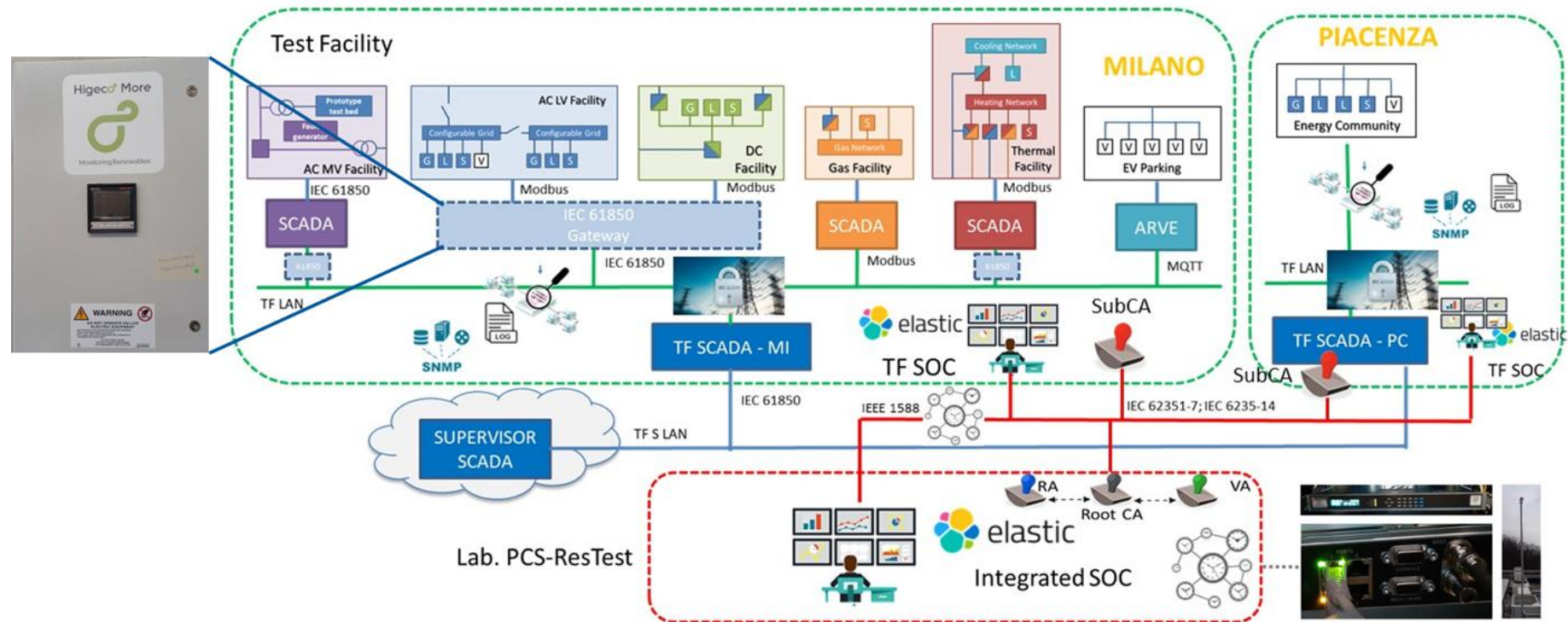
CEI 0-16 – Cybersecurity Certifications

- CEI 0-16 requires certificates of conformity to cybersecurity standards issued by accredited certification bodies
- CCI cryptographic keys and digital certificates shall be appropriately stored in a dedicated Hardware Secure Module (HSM) compliant to FIPS 140-2 L3 for resistance to physical tampering
- IEC 61850 certification
- CEI 0-16 prescribes CCI compliance to IEC 62351-3
 - Checks of key and certificate sizes, time limits
 - Tests for both expected and abnormal behaviours
- Compliance with ISA/IEC 62443-4-1
 - Security of the CCI Development process
- Compliance with ISA/IEC 62443-4-2





CCI in the RSE Test Facility and PCS-ResTest Lab



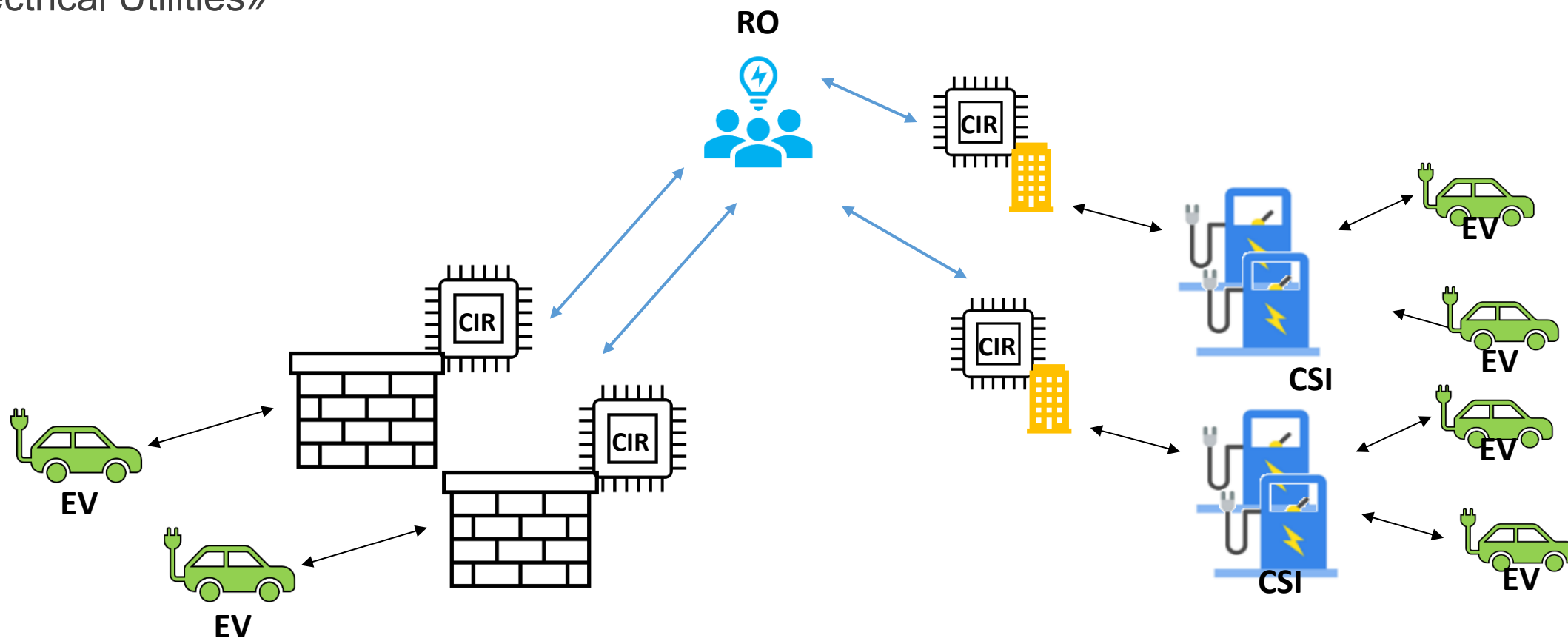


- Grid flexibility
 - Legislative Decree 5/2026 implementing **EU RED III Directive** states that starting from 1 January 2027, to guarantee **intelligent charging functionality** and **direct communication with intelligent measurement systems**, all **non–publicly accessible power recharging points** installed on the national territory, are certified to CEI 0-21 standard
 - CEI developed the normative project EV Charging Infrastructure Controller (CIR) of CEI 0-21 performing local and remote control of charging infrastructures to comply with network security and **flexibility** needs



Standard CEI 0-21 - Charging Infrastructure Controller

CEI 0-21 «Reference technical rules for the connection of active and passive users to the LV electrical Utilities»

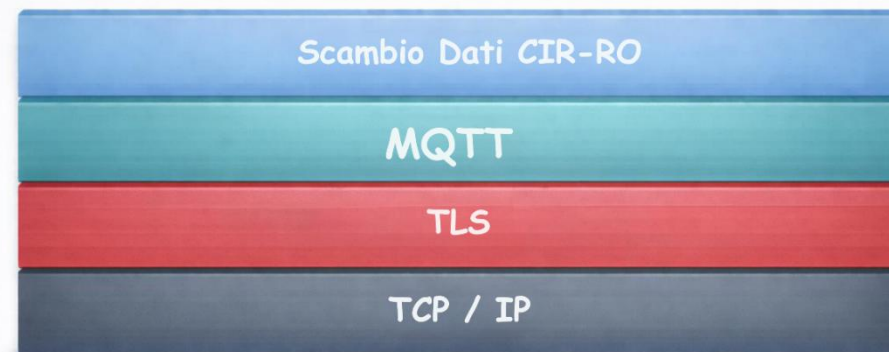




Stack protocollare XMPP con TLS e SASL



Stack protocollare MQTT con TLS





- RSE Research Program
- Project 2.7 Sustainable mobility and interaction with the energy system
- Project 2.1 Cyber Security of energy systems
- Collaboration agreements with stakeholders: CIR manufactures, CIR developers, CIR Remote Operators
- Activities
 - Communication server setup
 - Client integration , CIR and RO
 - Functional testing
 - PKI service
 - Cybersecurity conformance testing

Standard Functionality	Tested
SUC-00	✓
SUC-01	✓
SUC-02	✓
SUC-03	✓
SUC-04	✓
SUC-05	➡
SUC-06	✓
SUC-07	➡



Conformance Testing
CEI PAS 57-127



- The normative process required several interaction rounds with *standardization committees and device manufacturers*
- The *technology readiness* of standard cybersecurity solutions accelerated the *time to market* of commercial devices supporting such cybersecurity standards
- Energy Producers need to interact with third party *PKI Service Providers*
- The proper management of private/third party PKI infrastructures is *a source of complexity and increases the operational costs for both DSO and Producers*
- DER plants without internet connectivity shall have to manage manually most key and certificate operations. This would make more difficult the implementation of the cybersecurity management process by personnel with adequate cybersecurity awareness and competences
- *Software and firmware upgrades* deserve a special attention for cybersecurity of energy systems



Key message

- A constructive dialogue among **regulators**, **standard experts**, **operators** and **manufacturers** is a win⁴ factor to achieve the shared objective of energy infrastructures interoperability and cybersecurity
- This dialogue plays a key role in reducing the time to market and to operate secure communications



Thank you

Stay up to date with RSE because

#wemoversearch

Giovanna Dondossola



giovanna.dondossola@rse-web.it



www.rse-web.it



[@Ricerca sul Sistema Energetico - RSE SpA](#)



[@RSEnergetico](#)



[RSE SpA - Ricerca sul Sistema Energetico](#)

