Cybersecurity of DER-DSO data exchanges

From European Regulations to Italian Norms

Co-funded by
the European Union

Speaker's presentation

- Giovanna Dondossola, Leading Scientist and Project Manager at the Department *Transmission and Distribution Technologies* of RSE S.p.A, responsible of the *Integrated* ***Project Cybersecurity of Energy Systems*** within the **RdS** Italian Research Program 2022-2024, with focus on OT cybersecurity, cyber-physical system resilience, AI and ML for cyber anomaly detection
- Since 2000, responsible of the **RSE Lab** *Power Control Systems Resilience Testing*, carrying out evaluations of cybersecurity standards and innovative solutions
- Since 2004, *active member* of WGs on cybersecurity within **CIGRE SC D2**, CEN/CENELEC/ETSI, **IEC TC 57**
- Since 2016, *Secretary* of **CEI CT 57**, *active member* of a TF co-editing the **Annex T** of the **Norm CEI 0-16** on the *DER Plant Controller*, *convenor* of the JWG editing the **CEI PAS 57-127** on the *Charging Infrastructure Controller for Electric Vehicles* in **Annex X** of **CEI 0-21 Norm**

Giovanna Dondossola
Leading Scientist
Project Manager
RSE T&D Technologies

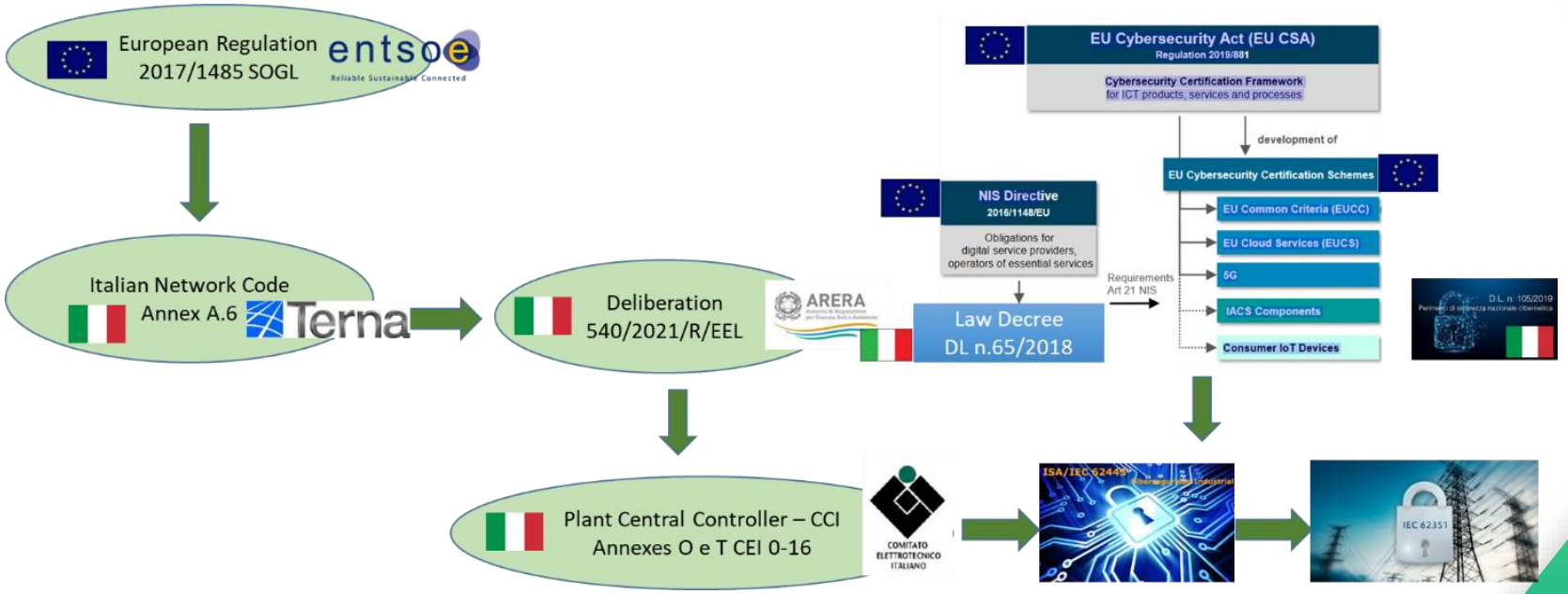
Co-funded by the European Union

Regulatory context

- **EU Regulation 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*
- implemented by the **Italian TSO** within the National Grid Code and approved by the **Italian Energy Regulatory Authority (ARERA)** in February 2020
- ARERA commissioned the norm development to the **Italian Electrotechnical Committee (CEI)**
- normative project ***Plant Central Controller*** **(CCI)** within the **Norm CEI 0-16**, a set of monitoring and control functions of DER plants to comply with grid **observability obligations**, **network operation** needs and **significant grid users' capabilities** to access **flexibility markets**
- ARERA Deliberation 540/2021/R/EEL, the CCI observability functions in CEI 0-16 are mandatory *in a first phase to the production plants connected to the medium voltage grids with a power equal to or greater than* ***1 MW***

Co-funded by the European Union

The normative process



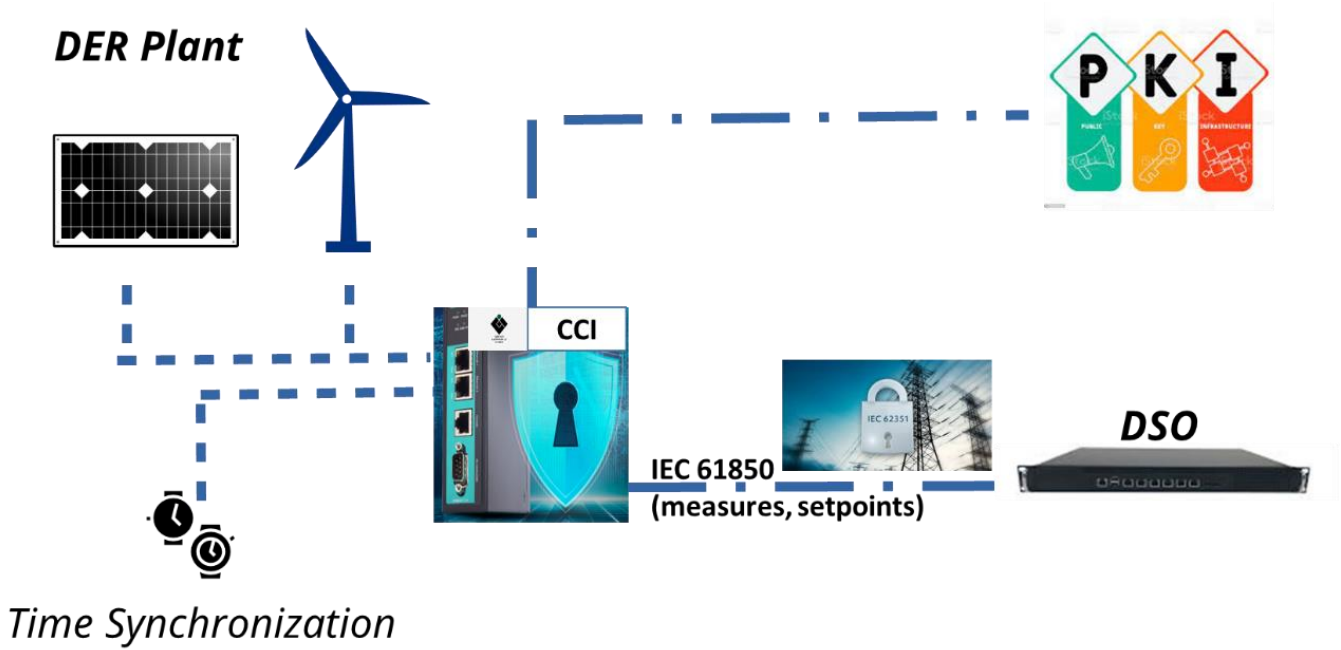
Co-funded by the European Union

Cybersecurity in Norm CEI 0-16

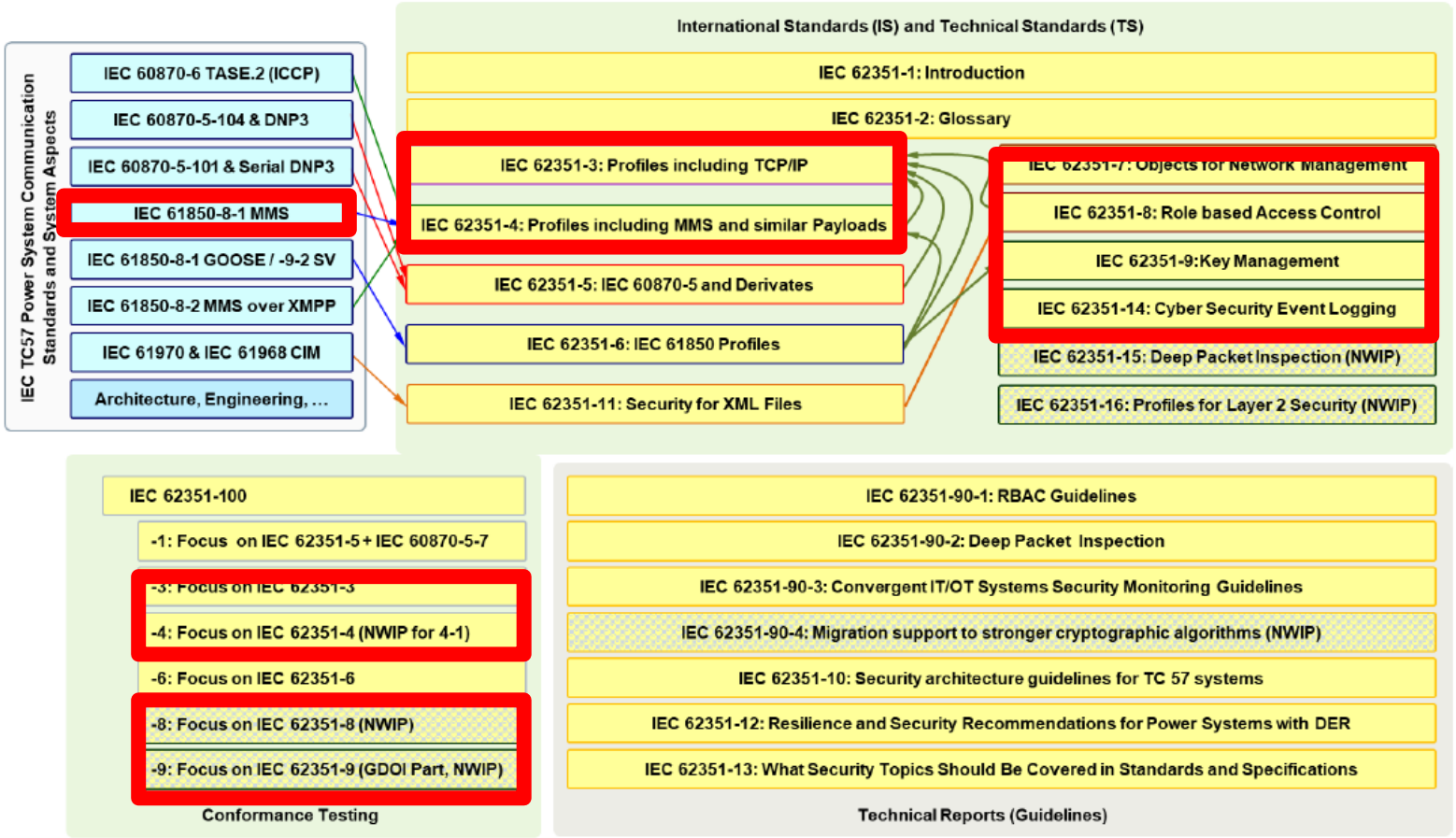
- CEI 0-16 «Reference technical rule for the connection of active and passive Users to the AT and MT networks of electricity distribution companies»
  - Annex O – Plant Central Controller (CCI)
    - Cybersecurity of firmware/software upgrades
    - Physical security of the Hardware Security Module
    - Compliance certifications
  - Annex T – CCI Data Model, communication interfaces and cybersecurity

Co-funded by
the European Union

CCI communication interfaces



IEC 62351



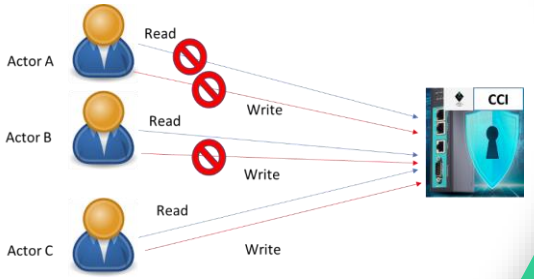
Co-funded by the European Union

CCI security and IEC 62351 profiles

- Identification and authorization of communicating entities
  - IEC 62351-9 and IEC 62351-8
  - Role-based access control
- IEC 61850 communication security
  - IEC 62351-3 and IEC 62351-4
- Key and certificate management
  - IEC 62351-9 profiles
- Security monitoring
  - Security events - IEC 62351-14
- Conformance tests
  - IEC 62351-100-3

CEI 0-16 – Remote access control

- 3 mechanisms
  - Identification of the remote entity
    - Check of the CA certificate pre-configured on the CCI
  - Authorizations based on entity roles
    - role specification based on IEC 62351-8
    - standard and custom roles
    - Profile A – Roles in extended ID certificates
    - Profile B - Roles in attribute certificates
  - Authentication of communicating nodes
    - protocol level



Co-funded by
the European Union

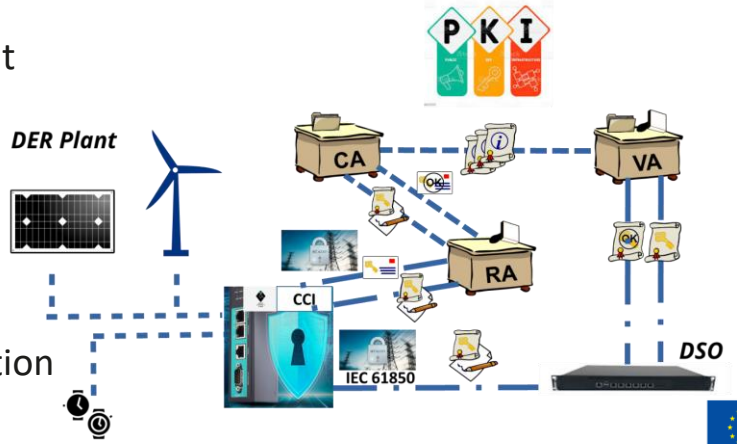
CEI 0-16 - IEC 61850 security

- **IEC 62351-3 profiles**
  - Transport layer, TLS based
  - Mutual authentication based on digital certificates signed by recognized authorities
  - Data integrity and confidentiality
  - Cryptographic algorithms
    - Key exchange with asymmetric keys
    - Data encryption with symmetric keys
    - Hashing, digital signatures
  - Performance tests of CEI 0-16 TLS profiles at RSE PCS-ResTest Lab

- **IEC 62351-4 profiles**
  - Application layer
  - Authentication, data encryption and integrity check of application messages
  - End-to-End security for segmented communication architectures

Keys and certificates management

- **IEC 61351-9**, standard ITU-T X.509
  - Private/public keys, associated digital certificates
  - Public Key Infrastructure (PKI)
    - RA, CA, VA
    - CA issues certicates or authorise other entities
    - DSO and CCI Owners shall exchange their CA certificates (PKI federation)
  - Digital certificate management
    - CCI enrollment
    - Certificate renewal
    - Certificate revocation
    - Certificate status validation



CCI communications - conformance tests

- accredited certification bodies, certificate of conformity to reference standards
- For IEC 62351-3, CEI 0-16 prescribes CCI compliance with IEC TS 62351-100-3
  - Checks of key and certificate sizes, time limits
  - Tests for both expected and unusual cases

Conformance Testing IEC 62351

Cybersecurity of the CCI product

- ✓ Compliance with ISA/IEC 62443-4-1
  - ➢ Security of the CCI Development process
  - ➢ Maturity Level 3
- ✓ Compliance with ISA/IEC 62443-4-2

Foundational Requirement	Description	Security Level
FR1	Identification and authentication control(IAC)	2
FR2	Use control (UC)	2
FR3	System integrity (SI)	2
FR4	Data confidentiality (DC)	1
FR5	Restricted data flow (RDF)	1
FR6	Timely response to events (TRE)	1
FR7	Resource availability (RA)	3

Hardware Security Module

- cryptographic keys and digital certificates appropriately stored in a dedicated Hardware Secure Module (HSM)
- Compliance with FIPS 140-2 L3
  - ✓ degree of HSM resistance to physical tampering

Lessons learned – development process

- The normative process requires several *interaction* cycles with *standardization committees and device manufacturers*
- The *technology readiness* of solutions specified by cybersecurity standards accelerates the *time to market* of commercial devices supporting such cybersecurity standards
- The *developers* of software libraries are recommended to keep aligned with the *evolution of standards*
- CCI simulators based on *open libraries* were created in lab environments to undergo preliminary testing with DSO clients. This enabled the decoupling of the development time between DSOs and CCI manufactures
- CEI TR 57-126, with the CCI data model in xml format, allows to minimize possible errors in the interpretation of the CEI 0-16 Norm and facilitate the implementation work by manufacturers. The report contains the logical nodes of IEC 61850-7-420, thus anticipating the publication of the new edition of IEC 61850-7-4
- The preliminary functional testing of DER-DSO communications revealed limited interoperability issue, confirming the advantage of adopting a standard specification

Co-funded by the European Union

Lessons learned – PKI services

- *Energy Producers* must interact with third party *Digital Certificate* (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*. Nonetheless, once the systems are in place the advantages of the automation behind certificates management are expected to balance the provisioning costs
- *Federation among third party/private PKI* will ensure both reasonable security and interoperability according to certifiable standards and protocols. A possible evolution would be the **election of a single Authority** having the role of *Trust Issuer* for recognized energy sector PKIs, which will provide a single Trust Anchor thus removing the need to preconfigure entities' Certificate Authorities (both DSO and Producer) on the device before each installation
- 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

Co-funded by the European Union

Lessons learned – software upgrades

- *Software and firmware upgrades* deserve a special attention for cybersecurity of energy systems
  - Upgrade steps allow to follow *a graded approach in the implementation of the normative obligations*, necessary to meet the manufacturers' development timeline
  - Cybersecurity software upgrades *may also be required for strengthening the robustness to an evolving threat landscape,* where the upgrade process involve manufacturers, plant owners and system operators
  - Cybersecurity upgrades may require reviewing the content of the Norm, therefore agile processes for Norm reviewing and device updating are required

Co-funded by the European Union

A constructive dialogue among

regulators, standard experts, operators and manufacturers

is a win factor to achieve the *shared objective* of

energy infrastructures cybersecurity.

This dialogue plays *a key role* in reducing the timeline of entering in operation of secure communications and in accommodating the market response speed

Thank you

Giovanna.Dondossola@rse-web.it

Co-funded by the European Union