Giovanna Dondossola

Impatto della Legislazione di Cybersecurity sulla Normativa per il controllo di risorse energetiche[*]

Abstract: L'utilizzo diversificato di energia rinnovabile e l'elettrificazione dei trasporti e del riscaldamento introducono una trasformazione digitale delle infrastrutture energetiche che richiede una gestione dei rischi derivanti dalle minacce alla cybersecurity. Lo sviluppo e l'adozione di misure di cybersecurity adeguate al livello di rischio dell'infrastruttura energetica cyber-fisica è una priorità riconosciuta dalle strategie di sviluppo e innovazione del sistema paese, finalizzate a garantire un livello di maturità tecnologica allineato ai target di cybersecurity europei e nazionali. Con l'obiettivo di esemplificare il percorso regolatorio che stabilisce misure di cybersecurity per infrastrutture energetiche, questo articolo illustra le caratteristiche principali del processo regolatorio per la cybersecurity degli impianti di generazione connessi alle reti elettriche, il quale prende avvio nel 2017 dalla regolazione elettrica a livello europeo, interseca la legislazione di cybersecurity e si concretizza con l'adozione nel 2023 di standard di cybersecurity internazionali da parte dei suddetti impianti.

Keywords: Cybersecurity; Direttiva NIS2; Perimetro nazionale di sicurezza Cibernetica; Electricity Regulation; Standard internazionali.

1. Processo regolatorio di settore elettrico

Il processo regolatorio del settore elettrico è tipicamente avviato da atti legislativi, denominati Codici di Rete, emanati dalla Unione Europea e successivamente recepiti dagli stati membri.

Il processo regolatorio illustrato in questo articolo, avviato nel 2017 e terminato nel 2023, fa riferimento al Codice di Rete Europeo 2017/1485 *System Operation Guideline* (SOGL)[1] il quale, ai fini della pianificazione e gestione operativa del

* Questo scritto è stato finanziato dal Fondo di Ricerca per il Sistema Elettrico nell'ambito del Piano Triennale 2022-2024 (DM MITE n. 337, 15.09.2022), in ottemperanza al DM 16 aprile 2018.

1 Regolamento EU 2017/1485, stabilisce orientamenti in materia di gestione del sistema di trasmissione dell'energia elettrica, 2017. Disponibile online: REGOLAMENTO (UE) 2017/

Teoria e Critica della Regolazione Sociale, n. 1, 2025 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320793 • DOI: 10.7413/197054760159

sistema elettrico in tempo reale, stabilisce la necessità di scambio dati tra operatori delle reti di trasmissione e distribuzione dell'energia elettrica e utenti di rete significativi. Il regolamento SOGL è stato recepito dall'Operatore italiano della rete elettrica di trasmissione, Terna, all'interno del Codice di Rete Nazionale, il cui Allegato 6[2] specifica le modalità, i contenuti e i requisiti dello scambio dati relativo ad impianti di generazione connessi alle reti in media tensione, di capacità uguale o superiore ad un megawatt. Il perimetro di applicazione del Codice di Rete contribuisce al raggiungimento degli obiettivi della transizione energetica del Paese stabiliti dal Piano Nazionale Integrato per l'Energia e il Clima (PNIEC), pubblicato nel 2019 e successivamente aggiornato (a giugno 2023) dal Ministero dell'Ambiente e della Sicurezza Energetica[3]. Secondo il PNIEC, nel 2030 l'Italia intende perseguire un obiettivo di copertura del 40,5% del consumo finale lordo di energia da fonti rinnovabili, delineando un percorso di crescita ambizioso di queste fonti con una piena integrazione nel sistema energetico nazionale.

Nel febbraio 2020 l'Autorità italiana per la Regolazione dell'Energia (ARERA) ha approvato le proposte di modifica del Codice di Rete di Terna ed incaricato contestualmente il Comitato Elettrotecnico Italiano (CEI) degli sviluppi normativi per la specifica delle regole di connessione alle reti e delle tecnologie digitali da utilizzare per l'implementazione dello scambio dati tra gli impianti di generazione nel perimetro di applicazione e gli Operatori delle reti di distribuzione (DSO) di competenza.

Prende quindi avvio a cura dei Comitati Tecnici CT 316 "Connessione alle reti elettriche di distribuzione Alta, Media e Bassa Tensione" e CT 57 "Scambio informativo associato alla gestione dei sistemi elettrici di potenza" del CEI il progetto normativo Controllore Centrale di Impianto (CCI), un insieme di funzioni di monitoraggio e controllo degli impianti energetici distribuiti (DER) la cui specifica funzionale e tecnologica è contenuta, rispettivamente negli Allegati O[4] e T[5] della Norma CEI 0-16.

Tenuto conto del quadro legislativo di riferimento per la cybersecurity delle reti informatiche degli operatori energetici illustrato in seguito, la specifica del CCI

1485 DELLA COMMISSIONE – del 2 agosto 2017 – che stabilisce orientamenti in materia di gestione del sistema di trasmissione dell'energia elettrica (europa.eu) (accesso 14 Agosto 2024).

2 Terna, Allegato A.6 del codice di rete Rev. 04, Criteri di acquisizione dati per il telecontrollo, luglio 2022. Disponibile online: https://download.terna.it/terna/20220701_Allegato_A.6_8da5b792cadec35.pdf (accesso 14 Agosto 2024).

3 Piano Nazionale Integrato per l'Energia e il Clima, Ministero dell'Ambiente e della Sicurezza Energetica, Giugno 2023. Disponibile online: https://www.mase.gov.it/sites/default/files/PNIEC_2023.pdf (accesso 14 Agosto 2022).

4 CEI 0-16:2022-03, Regola Tecnica di Riferimento per la Connessione di Utenti Attivi e Passivi alle reti AT e MT delle Imprese Distributrici di Energia Elettrica. CEI, Milano, Italy. 2022. Disponibile online: https://static.ceinorme.it/strumentionline/doc/18308.pdf (accesso 14 Agosto 2024).

5 Variante V2 della Norma CEI 0-16:2022-03, Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT e MT delle imprese distributrici di energia elettrica, 2023. Disponibile online: https://static.ceinorme.it/strumenti-online/doc/20402.pdf (accesso 14 Agosto 2024).

ha indirizzato i requisiti di cybersecurity attraverso l'applicazione degli standard internazionali ISA/IEC 62443[6,7] e IEC 62351[8].

Nel 2021 ARERA emette la Delibera 540/2021/R/EEL[9] la quale impone l'obbligatorietà delle funzioni di osservabilità del CCI conformi alla Norma CEI 0-16 per gli impianti di produzione connessi alle reti di media tensione con potenza pari o superiore a un megawatt.

Lo schema complessivo del processo regolatorio appena descritto (dal Codice di Rete SOGL all'implementazione obbligatoria degli standard di comunicazione e sicurezza informatica per le comunicazioni DSO-DER a livello nazionale) è schematizzato in Figura 1, insieme agli attori, agli atti legislativi, agli standard internazionali e alle norme nazionali che sono intervenuti nelle diverse fasi del processo.

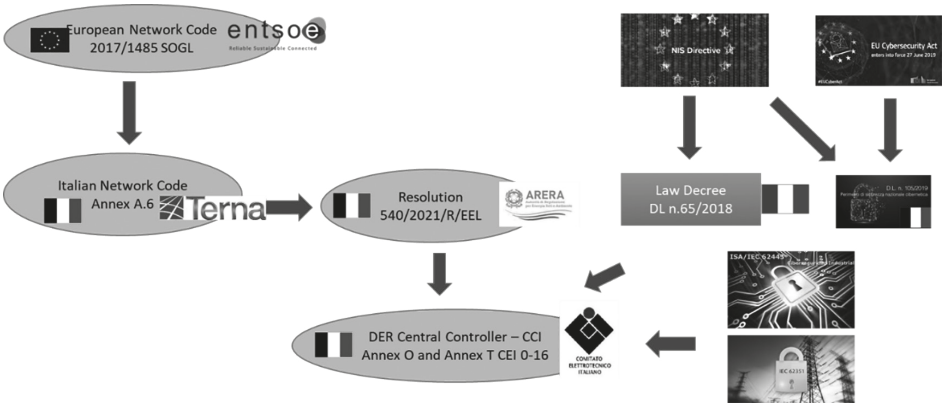


Figura 1 – Schema e attori del processo regolatorio

Nelle sezioni che seguono vengono illustrati gli aspetti salienti della legislazione sulla cybersecurity, a livello Europeo e Nazionale, e il loro recepimento nei requisiti e nelle tecnologie del Controllore Centrale di Impianto.

6 ISA/IEC 62443-4-1, Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. Available online: https://webstore.iec.ch/en/publication/33615 (access on 14 August 2024).

7 IEC 62443-4-2:2019, Security for Industrial Automation and Control Systems-Part 4-2: Technical Security Requirements for IACS Components IEC, Geneva, Switzerland, 2019. Available online: https://webstore.iec.ch/en/publication/34421 (access on 14 August 2024).

8 IEC 62351:2024, Power systems management and associated information exchange – Data and communications security – ALL PARTS", 2024. Available online: https://webstore.iec.ch/en/publication/6912 (access on 14 August 2024).

9 ARERA, Regolazione dello scambio dati tra TERNA S.P.A., Imprese Distributrici e Significant Grid Users ai fini dell'esercizio in sicurezza del sistema elettrico nazionale, Deliberazione 540/2021/R/EEL, 30 Novembre 2021. Disponibile online: https://www.arera.it/fileadmin/allegati/docs/21/540-21.pdf (accesso 14 Agosto 2022).

2. La Direttiva europea NIS2 2022/2555

I settori dell'energia rientrano nel perimetro di applicazione della Direttiva Europea NIS2 2022/2555[10] relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, entrata in vigore il 16 gennaio 2023 in sostituzione della precedente Direttiva NIS 2016/1148[11] sulla sicurezza delle reti e dei sistemi informativi.

La NIS2 rinforza lo stato di sicurezza informatica richiesto a tutta l'Europa coprendo una quota più ampia dell'economia e della società. Il campo di applicazione del settore Energia, considerato ad alta criticità, include i sottosettori energia elettrica, teleriscaldamento e teleraffrescamento, petrolio, gas e idrogeno. Per il sottosettore energia elettrica, la direttiva esplicita i seguenti tipi di soggetti interessati (Allegato I):

- le imprese elettriche;
- i gestori dei sistemi di distribuzione e di trasmissione;
- i produttori, quali sono i proprietari degli impianti di generazione interessati dal processo regolatorio descritto in questo articolo;
- i gestori del mercato elettrico;
- i partecipanti al mercato dell'energia elettrica che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia;
- i gestori di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità.

I soggetti, che rientrano nell'ambito di applicazione della NIS2, ai fini del rispetto delle misure di gestione dei rischi di cybersecurity e degli obblighi di segnalazione, vengono classificati in soggetti essenziali e soggetti importanti (Articolo 3) in funzione della loro rilevanza per il settore o il tipo di servizi che forniscono, nonché delle loro dimensioni.

In tema di misure di gestione dei rischi di cibersicurezza, il paragrafo 1 dell'Articolo 21 stabilisce che "Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi".

Le misure di sicurezza tengono conto delle soluzioni più aggiornate e mature e degli standard europei ed internazionali pertinenti per il settore al fine di assicurare un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. La proporzionalità delle misure dipende dal grado di esposizione del soggetto a

10 Direttiva EU 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, 2022. Disponibile online: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555 (accesso 14 Agosto 2024).

11 Direttiva EU 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione 2016. Disponibile online: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148 (accesso 14 Agosto 2024).

rischi, dalle dimensioni del soggetto, dalla probabilità che si verifichino incidenti, dalla loro gravità e dal loro impatto sociale ed economico.

Tra gli aspetti delle misure di sicurezza elencati nel paragrafo 2 dell'Articolo 21, le misure indirizzate dalla Norma CEI 0-16 riguardano:

- sicurezza dell'approvvigionamento dei dispositivi CCI e dei servizi di gestione dei certificati elettronici;
- la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei dispositivi CCI;
- le politiche, le procedure e gli algoritmi di crittografia e di cifratura;
- le soluzioni di controllo degli accessi, delle autorizzazioni e di autenticazione.
- In allineamento con il Regolamento Europeo *Cyber Security Act*[12] e con la proposta di Regolamento Europeo *Cyber Resilience Act* (CRA)[13], la NIS2 fa esplicito riferimento alla conformità a schemi Europei di certificazione della cybersecurity (Articolo 24). Il CRA si applica ai prodotti con elementi digitali il cui uso prevede una connessione dati, diretta o indiretta, logica o fisica, a un dispositivo o a una rete, stabilendo obblighi per i costruttori, i distributori e gli operatori dei prodotti per garantire:
- miglioramenti nella sicurezza di prodotti con elementi digitali durante l'intero ciclo di vita;
- un framework di sicurezza informatica, che facilita la conformità per produttori di hardware e software, favorendone la valutazione della conformità;
- trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali, consentendo alle aziende e ai consumatori di utilizzare prodotti con elementi digitali in modo sicuro.

Il sistema sanzionatorio introdotto dalla NIS2, la cui responsabilità ricade sugli Stati membri, dovrà essere adottato in funzione della tipologia di soggetti (Articolo 34).

3. La legge italiana 2019/105

Il Decreto-Legge 2018/65[14], entrato in vigore il 24 Giugno 2018, costituisce l'attuazione italiana della Direttiva europea NIS[15]. Un primo fondamentale provvedi-

12 Regolamento EU 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, 2019. Disponibile online: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881 (accesso 14 Agosto 2024).

13 Proposta di Regolamento EU relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, 2022. Disponibile online: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0010.02/DOC_1&format=PDF (accesso 14 Agosto 2024).

14 Decreto-Legge 2018/65, attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, Gazzetta Ufficiale n.132 del 9-6-2018, 2018. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg (accesso 14 Agosto 2024).

15 Cfr. nota 11.

mento stabilito dal Decreto 2018/65 è relativo all'identificazione degli operatori classificati come fornitori di servizi essenziali, quali quelli energetici, soggetti agli obblighi in materia di sicurezza e notifica degli incidenti indicati dall'Articolo 14, e alle relative sanzioni amministrative in caso di inadempienza di cui all'Articolo 21.

Il successivo Decreto-Legge 2019/105[16] introduce disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

Il perimetro di sicurezza cibernetica riguarda tutte le infrastrutture critiche private e pubbliche, aventi una sede nel territorio nazionale, che assicurano un servizio essenziale per le attività civili, sociali o economiche fondamentali per la nazione, e che per la fornitura di tale servizio si avvalgono di reti, sistemi informativi e servizi informatici dal cui malfunzionamento o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale. Nella legge Perimetro vengono stabilite le misure (legali, organizzative e tecnologiche) di gestione del rischio e di mitigazione e gestione degli incidenti che garantiscono elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici tenendo conto degli standard definiti a livello internazionale ed europeo.

L'attuazione della Legge Perimetro è a carico dell'Agenzia per la Cybersicurezza Nazionale (ACN) istituita dal Decreto-Legge 2021/82[17] del 14/06/2021. ACN è l'Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. L'ACN predispone la strategia nazionale di cybersicurezza ed è Autorità nazionale di certificazione della cybersicurezza**,** secondo quanto specificato dal Parlamento europeo e del Consiglio, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni.

Il Decreto del Presidente della Repubblica (DPR) 2021/54[18] del 5/02/2021, include:

16 Decreto-Legge 2019/105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (e di disciplina dei poteri speciali nei settori di rilevanza strategica), Gazzetta Ufficiale Serie Generale n.222 del 21-09-2019, 2019. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg (accesso 14 Agosto 2024).

17 Decreto-Legge 2021/82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, Gazzetta Ufficiale Serie Generale n.140 del 14-06-2021, 2021. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg (accesso 14 Agosto 2024).

18 Decreto del Presidente della Repubblica 2021/54, Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, Gazzetta Ufficiale Serie Generale n.97 del 23-04-2021, 2021. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/SG (accesso 14 Agosto 2024).

- procedure, modalità e termini di funzionamento del Centro di Valutazione e Certificazione Nazionale (CVCN) trasferito presso ACN;
- criteri tecnici per l'individuazione delle categorie e dell'elenco dei beni, dei sistemi e dei servizi a cui si applica la procedura di valutazione;
- procedure, modalità e termini con cui le autorità competenti effettuano le verifiche.

Il Procedimento di verifica e valutazione dettagliato nell'Articolo 4 del DPR si articola in verifiche preliminari (Articolo 5), fase di preparazione all'esecuzione dei test (Articolo 6); esecuzione dei test di hardware e software (Articolo 7).

All'esito delle verifiche e dei test, il CVCN o i Centri di Valutazione accreditati definiscono eventuali condizioni e test di hardware e di software da inserire nelle clausole del bando di gara o del contratto, nonché eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro.

Il Decreto del Presidente del Consiglio dei Ministri (DPCM) 2021/81[19] del 14/04/2021 introduce il regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici. Il DPCM riporta tre allegati:

1. nell'allegato A sono presenti tabelle che rappresentano, divisi per categoria, gli incidenti aventi impatto sui beni ICT;
2. nell'allegato B sono presenti le misure di sicurezza, articolate in funzioni, categorie, sottocategorie, punti e lettere;
3. nell'allegato C sono presenti le misure minime di sicurezza per la tutela delle informazioni.

Dal 1° gennaio 2022, i soggetti inclusi nel perimetro, al verificarsi di uno degli incidenti avente impatto su un bene ICT di rispettiva pertinenza individuati nelle tabelle di cui all'allegato A, procedono alla notifica al CSIRT italiano secondo le modalità descritte nel decreto.

I soggetti inclusi nel perimetro procedono alla notifica anche nei casi in cui uno degli incidenti individuati nelle tabelle dell'allegato A si verifichi a carico di un sistema informativo o un servizio informatico, o parti di essi, che condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione.

Nella prossima sezione vengono sommariamente descritte le misure di sicurezza dei controllori di impianti di generazione specificate dalla Norma CEI 0-16[20], che ricadono nelle funzioni di sicurezza Protezione (PR) e Rilevamento (DE) indicate nell'Allegato B. In ottemperanza ai requisiti della Legge Perimetro, la Norma prevede il rilascio, da parte di enti di certificazione, di attestati di conformità allo standard dei profili di cybersecurity e di certificazioni di cybersecurity del prodotto CCI.

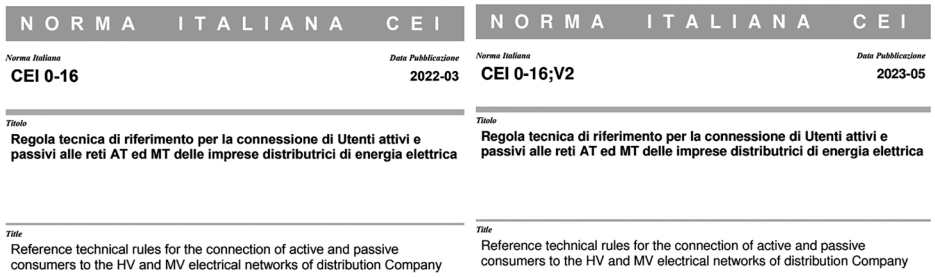
19 Decreto del Presidente del Consiglio dei Ministri 2021/81, Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, Gazzetta Ufficiale Serie Generale n.138 del 11-06-2021, 2021. Disponibile online: https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/SG (accesso 14 Agosto 2024).

20 Cfr. nota 5.

4. La norma CEI 0-16 e la sicurezza delle comunicazioni dei controllori di impianti di generazione connessi alle reti in media tensione

Per il funzionamento in sicurezza del sistema elettrico, il CCI deve mettere a disposizione una serie di misure e stati di impianto assicurando il dettaglio, la precisione e la periodicità di aggiornamento prescritti dall'Allegato 6 del Codice di Rete Nazionale[21].

Come evidenziato in Figura 1, la specifica del dispositivo CCI e delle sue interfacce di comunicazione è contenuta negli Allegati O[22] e T[23]della Norma CEI 0-16 redatta a cura di esperti dei Comitati Tecnici 316 e 57 del CEI (Figura 2).


NORMA ITALIANA CEI

Norma Italiana **CEI 0-16** *Data Pubblicazione* **2022-03**

Titolo
Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT ed MT delle imprese distributrici di energia elettrica

Title
Reference technical rules for the connection of active and passive consumers to the HV and MV electrical networks of distribution Company

NORMA ITALIANA CEI

Norma Italiana **CEI 0-16;V2** *Data Pubblicazione* **2023-05**

Titolo
Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT ed MT delle imprese distributrici di energia elettrica

Title
Reference technical rules for the connection of active and passive consumers to the HV and MV electrical networks of distribution Company

Figura 2 – Norma CEI 0-16:2022-03 e variante CEI 0-16;V2:2023-05

L'interfaccia di comunicazione DER-DSO definisce un modello dati e protocolli di comunicazione e di cybersecurity conformi agli standard internazionali IEC 61850[24] e IEC 62351[25].

Le funzioni di sicurezza dell'interfaccia DER-DSO, raggruppate secondo la classificazione della Legge Perimetro, sono elencate nel seguito:

- Gestione delle identità, autenticazione e controllo degli accessi (PR.AC): identificazione e autorizzazione delle entità remote basate sulla verifica del certificato elettronico della Autorità di Certificazione, preconfigurato nel CCI, e sul controllo delle autorizzazioni di accesso basato sui ruoli (Figura 3) in conformità allo standard IEC 62351-8[26];

21 Cfr. nota 2.
22 Cfr. nota 4.
23 Cfr. nota 5.
24 IEC 61850:2024, Communication networks and systems for power utility automation – ALL PARTS, 2024. Available online: https://webstore.iec.ch/en/publication/6028 (access on 14 August 2024).
25 Cfr. nota 8.
26 IEC 62351-8, Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management. Available online: https://webstore.iec.ch/en/publication/61822 (access on 14 August 2024).

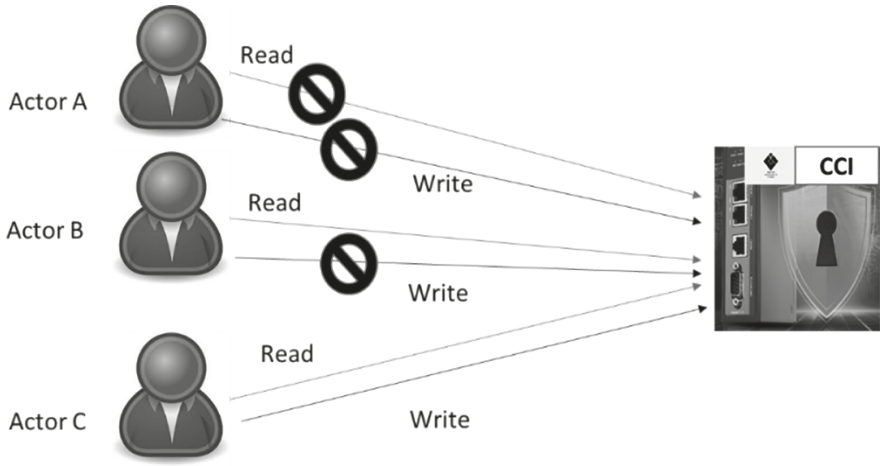


Figura 3 – Controllo delle autorizzazioni di accesso basato sui ruoli

- Sicurezza dei dati (PR.DS): sicurezza delle comunicazioni IEC 61850[27], in conformità agli standard IEC 62351-3[28] e IEC 62351-4[29]. In particolare:
  - mutua autenticazione dei nodi comunicanti mediante certificati elettronici firmati da autorità riconosciute;
  - integrità e confidenzialità dei dati scambiati attraverso algoritmi crittografici;
  - scambio delle chiavi con algoritmi a chiavi asimmetriche;
  - cifratura dei dati applicativi con algoritmi a chiave simmetrica;
  - algoritmi di hashing e firma digitale;
- Procedure e processi per la protezione delle informazioni (PR.IP): gestione dei certificati e delle chiavi, in conformità allo standard IEC 62351-9[30], per mezzo di una infrastruttura di gestione delle chiavi pubbliche per le funzioni di registrazione dei dispositivi, emissione, rinnovo e revoca dei certificati e validazione del loro stato di validità;

27 Cfr. nota 19.

28 IEC 62351-3, Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP. Available online: https://webstore.iec.ch/en/publication/68410 (access on 14 August 2024).

29 IEC 62351-4, Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives. Available online: https://webstore.iec.ch/en/publication/67350 (access on 14 August 2024).

30 IEC 62351-9, Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment. Available online: https://webstore.iec.ch/en/publication/66864 (access on 14 August 2024).

- Anomalie e eventi (DE.AE): monitoraggio della sicurezza a supporto di attività di diagnostica e audit.

A supporto dei requisiti di conformità e certificazione introdotti dalla Legge Perimetro, la Norma CEI-016[31] richiede che il CCI sia dotato delle seguenti certificazioni rilasciate da terze parti:

- UCA IEC 61850 che attesti la conformità del profilo CCI allo standard IEC 61850;
- IEC 62351-100-3[32] che attesti la conformità del profilo di sicurezza di livello trasporto allo standard IEC 62351-3[33]. I test specificati includono verifiche sulla dimensione di chiavi e certificati, sui limiti temporali delle procedure di rinnovo e validità, test di comportamenti attesi e anomali (Figura 4);

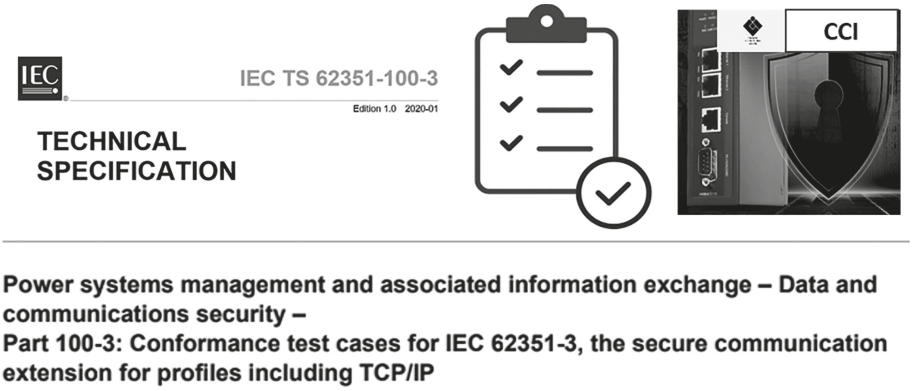


Figura 4 – Casi di Test per la conformità allo standard IEC 62351-3

- ISA/IEC 62443-4-1[34] che attesti la conformità del processo di sviluppo del CCI con livello di maturità 3;
- ISA/IEC 62443-4-2[35] che attesti i requisiti di sicurezza del dispositivo CCI con i livelli di sicurezza specificati in Figura 5;

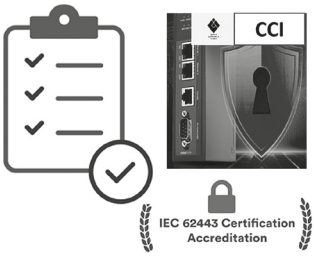
31 Cfr. nota 4.

32 IEC TS 62351-100-3, Power systems management and associated information exchange – Data and communications security – Part 100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP. Available online: https://webstore.iec.ch/en/publication/61597 (access on 14 August 2024).

33 Cfr. nota 21.

34 Cfr. nota 6.

35 Cfr. nota 7.



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

Figura 5 – Certificazione ISA/IEC 62443

- FIPS 140-2 che attesti un grado di resistenza a manomissioni fisiche di livello 3 per il modulo di sicurezza hardware in cui sono memorizzate le chiavi crittografiche e i certificati elettronici.
- Nell'ambito del progetto 2.1 "Cybersecurity dei sistemi energetici" del Piano Triennale 22-24 della Ricerca di Sistema i profili di sicurezza della CEI 0-16 sono oggetto di test prestazionali[36] e di conformità[37]. Gli schemi di certificazione ISA/IEC 62443 vengono valutati in relazione ai test richiesti dal Centro di Valutazione e Certificazione Nazionale dell'ACN in ottemperanza alla Legge Perimetro.

5. Conclusioni

Il presente articolo ha illustrato, attraverso un ambito applicativo relativo alla digitalizzazione del settore energetico, il recepimento dei requisiti legislativi dei sistemi che ricadono nel perimetro di sicurezza nazionale cibernetica attraverso soluzioni di cybersecurity conformi a standard internazionali di settore.

Le esperienze pionieristiche riportate nell'articolo, oggetto di diverse azioni di divulgazione nazionale[38] ed internazionale[39], costituiscono una base di competenze utile per le numerose future applicazioni digitali in ambito energetico.

Affinché la transizione energetica delineata dal PNIEC[40] possa indirizzare l'autonomia tecnologica auspicata dalla strategia dell'Agenzia per la Cybersicurezza Nazionale risulta essenziale seguire il processo di recepimento nazionale della Direttiva NIS2 e l'evoluzione degli standard internazionali sviluppati dai comitati di riferimento.

36 Todeschini 2023.
37 Todeschini, Guagliardi 2023.
38 Dondossola, Terruggia, Todeschini, Bianco, Modica 2022.
39 Dondossola, Terruggia, Todeschini, Bianco, Delli Carpini, Modica 2024.
40 Cfr. nota 3.

Bibliografia

Dondossola G., Terruggia R., Todeschini M., Bianco G., Delli Carpini L., Modica M. 2024, "Cybersecurity-Enabling Technologies: Digital Applications" in *the Energy Transition, IEEE Power and Energy Magazine*, Volume: 22, Issue: 3, May-June, available online: https://ieeexplore.ieee.org/document/10522091?source=authoralert (access on 14 August 2024).

Dondossola G., Terruggia R., Todeschini M., Bianco G., Modica M. 2022, "L'implementazione della cybersecurity per lo scambio dati con utenti attivi MT", in *Rivista AEIT L'Energia Elettrica*, N. 2 Vol. 99, pagg 11-19, disponibile online: https://www.rse-web.it/pubblicazioni/limplementazione-della-cybersecurity-per-lo-scambio-dati-con-utenti-attivi-mt/ (accesso 14 Agosto 2024).

Todeschini M. 2023, "Progetto di un'architettura per la misurazione dell'impatto dell'autenticazione basata su PKI centralizzata nelle comunicazioni di telecontrollo", in *Ricerca di Sistema*, RSE n. 23006655.

Todeschini M. G., Guagliardi A. 2023, "Progettazione di una piattaforma automatizzata per test di conformità ai requisiti di cybersecurity delle comunicazioni nei dispositivi energetici", in *Ricerca di Sistema*, RSE n. 23006657.