

## CONTROLLORE CENTRALE DI IMPIANTO

### Guida all'acquisto



#### CHECKLIST :

- Certificazioni
- Componenti Hardware
- Componenti Software
- Cyber Security

## CERTIFICAZIONI

La tabella sottostante contiene tutti i documenti con i rispettivi riferimenti alla norma e, dove necessario, fornisce dei link esterni per la verifica dei certificati. Gli allegati di riferimento normativo per il CCI sono l'allegato O e il T all'interno della più corposa CEI 0-16.

Descrizione	Norma di riferimento	Riferimento norma CEI 0-16, allegati O e T	Note
<input type="checkbox"/> Conformità generale	CEI/EN 61557-12	O.7.4 e O.15.2	
<input type="checkbox"/> Cybersecurity Software	ISASecure SDLA per IEC 62443-4-1	0.15.4	<p><b>ATTENZIONE:</b> alcuni costruttori di CCI hanno volontariamente deciso di non ottemperare alla norma scegliendo di non adottare lo schema ISASecure nel loro prodotto. Per tale motivo questi CCI non sono conformi alla CEI 0-16.</p> <p><b>VERIFICA</b> sempre la presenza del certificato ISASecure direttamente dal sito ufficiale.</p>
<input type="checkbox"/>	ISASecure SDLA per IEC 62443-4-2		
<input type="checkbox"/> Cybersecurity Hardware	FIPS 140-2 Livello 3	O.13.7 e O.15.3	<p><b>ATTENZIONE:</b> Il CCI dev'essere dotato di un chip certificato FIPS 140-2 Livello 3 per lo stoccaggio dei certificati e delle chiavi crittografiche.</p> <p><b>VERIFICA</b> il certificato FIPS del chip utilizzato dal CCI direttamente sul sito ufficiale FIPS.</p>
<input type="checkbox"/> IEC 61850	Prove di conformità IEC 61850 in un laboratorio accreditato UCA User Group	O.3 e allegato T	<p><b>ATTENZIONE:</b> alcuni costruttori di CCI hanno volontariamente deciso di non testare il server IEC 61850 del CCI in un laboratorio UCA User Group. Per tale motivo questi CCI potrebbero avere problemi di interoperabilità con i clients dei DSO e non sono conformi alla CEI 0-16.</p>
<input type="checkbox"/> Profilo trasporto sicuro IEC 62351-3	Certificato test di conformità IEC 62351-3	O.15.4, T.3.3.4.1 e T.3.3.4.3.4	
<input type="checkbox"/> Produzione in regime di Qualità	ISO 9001	O.15.4	
<input type="checkbox"/> Prove climatiche	CEI 0-16 Tabella 20 (CEI EN 600068)	O.15.4	<p><b>ATTENZIONE:</b> sul mercato sono acquistabili dei dispositivi <b>abilitanti</b> il CCI, come PLC, RTU o PC industriali, che svolgono solo alcune delle funzioni richieste dalla norma CEI 0-16, ma non tutte. Questi dispositivi devono essere integrati in un quadro, dotato degli apparati necessari a svolgere le funzioni mancanti. Per esempio, se la RTU fosse sprovvista di ingressi di misura integrati, sarebbe necessario aggiungere un Power Analyzer (Convertitore di Misura). In questo caso il CCI è il quadro intero, ed è quest'ultimo che deve superare le prove ambientali (climatiche, isolamento, emc ed immunità) in un laboratorio accreditato CEI UNI EN ISO/IEC 17025. Chi vende la RTU non può farsi carico di questa certificazione non potendo sapere a priori quali oggetti l'utente finale andrà ad integrare alla sua RTU.</p> <p><b>VERIFICA</b> sempre che il tuo fornitore di CCI che usa una RTU abbia certificato l'assieme di tutti i dispositivi in un laboratorio accreditato ISO 17025.</p>
<input type="checkbox"/> Prove di Isolamento elettrico	CEI 0-16 Tabella 21 (CEI EN 60225-5)	O.15.4	
<input type="checkbox"/> Prove EMC e Immunità	IEC 61000 ETSI EN 301 489 Radio ETSI EN 303 413 GPS	O.15.4	

## CERTIFICAZIONI

Descrizione	Norma di riferimento	Riferimento norma CEI 0-16, allegati O e T	Note
<input type="checkbox"/> Prove Funzionali	CEI 0-16 Allegato O e Allegato T	O.15.1	<b>ATTENZIONE:</b> alcuni costruttori di CCI non hanno ancora implementato la gestione dei ruoli (RBAC), come richiesto dal capitolo T.3.3.4.3. Per tale motivo questi CCI non sono conformi alla CEI 0-16. <b>VERIFICA</b> sempre che il tuo fornitore di CCI abbia implementato la gestione dei ruoli nella comunicazione 61850/MMS
<input type="checkbox"/> Marchio CE	Direttiva 2014/30/EU (EMC) Direttiva 2014/35/EU (LVD) Direttiva 2014/53/EU (RED)	O.15.4	

## PRINCIPALI COMPONENTI HARDWARE

Componente	Riferimento norma CEI 0-16, allegati O e T	Breve descrizione
<input type="checkbox"/> RTU (Remote Terminal Unit)		Una RTU (Remote Terminal Unit) raccoglie ed espone i dati di monitoraggio ed implementa le funzioni di controllo. Agisce come interfaccia tra l'impianto ed il DSO (Distributor System Operators), comunicando in IEC61850 con TLS.
<input type="checkbox"/> PMD (Power Metering Device)	Norma CEI 0-16 O.8.3 e O.15.2	Insieme alla RTU, è uno dei dispositivi cuore del sistema, deve essere certificato secondo lo standard IEC 61557-2 e serve per acquisire le misure elettriche al punto di connessione con la rete. Può essere integrato nella RTU o separato.
<input type="checkbox"/> Sistema di alimentazione ausiliaria	Norma CEI 0-16 allegato O.13.3	Per garantire il funzionamento del CCI anche in caso di perdita di alimentazione principale è necessario prevedere un sistema di backup realizzato da apposito UPS o da batteria tampone per un tempo di almeno 1 ora. Il CCI di Higecco More è dotato di batteria tampone.
<input type="checkbox"/> Interfacce di comunicazione	Norma CEI 0-16 allegato O.13.1	Ogni CCI deve disporre di almeno tre interfacce distinte, di cui una dedicata al DSO, una alla comunicazione verso l'impianto ed una per soggetti terzi abilitati alla connessione remota. L'interfaccia dedicata al DSO deve essere di tipo Ethernet 100Base-FX, su fibra multimodale a 1310 nm con connettore doppio LC.
<input type="checkbox"/> GPS (Global Positioning System)	Norma CEI 0-16 allegato O.7.1	Componente necessario per la sincronizzazione dell'orologio tramite segnale da satellite.

## COMPONENTI SOFTWARE

Funzionalità	Note
<input type="checkbox"/> PF1: Monitoraggio	Funzionalità obbligatorie
<input type="checkbox"/> PF2: Regolazione e Controllo	Funzionalità opzionali dal punto di vista del DSO: Il DSO potrà richiedere in qualunque momento (anche dopo l'installazione del tuo CCI) le funzioni di regolazione (PF2)
<input type="checkbox"/> PF3: Partecipazione Mercati di Flessibilità ed Ottimizzazione di impianto	Funzionalità facoltative dal punto di vista del produttore: come Produttore, potrai indicare se vuoi attivare le funzioni facoltative PF3 per poter partecipare al mercato di dispacciamento.

*Al momento le PF2 e le PF3 non sono obbligatorie, ma la norma CEI 0-16 in O.1 indica che "le tempistiche secondo cui anche le funzioni attualmente opzionali e facoltative diventeranno obbligatorie saranno stabilite successivamente da Arera con appropriate Delibere". Inoltre la crescente diffusione della generazione distribuita, soprattutto da fonte rinnovabile, rende imprescindibile che questi impianti siano regolabili e controllabili da remoto, per il bilanciamento di rete: non è questione di "se", ma solo di "quando".*

## CYBER SECURITY

*La norma dedica l'intero Allegato T a descrivere in dettaglio come proteggere la comunicazione in IEC 61850 tra il CCI ed il mondo esterno. Per quanto sia un allegato complicato da leggere, è necessario prendere seriamente ogni singolo requisito e non sottovalutarne o minimizzarne l'importanza.*

Componente	Funzionalità
<input type="checkbox"/> Certificazioni IEC 62443-4-1 e -4-1	Garanzia che il CCI sia stato sviluppato considerando la sicurezza il requisito principale e che sia dotato delle migliori tecnologie possibili per garantire la Confidenzialità e l'Integrità dei dati, assicurandone la massima Disponibilità.
<input type="checkbox"/> Profilo di trasporto sicuro (TLS)	Protezione delle comunicazioni IEC 61850: come tutti i protocolli di comunicazioni non è stato progettato per essere sicuro e l'utilizzo di TLS è quindi imprescindibile per proteggerlo.
<input type="checkbox"/> Gestione dei ruoli (RBAC)	Definizione di diverse autorizzazioni per i diversi attori remoti che interagiscono con il CCI. Non averla significherebbe dare gli stessi permessi a tutti gli attori, per esempio permettere ad un Produttore di limitare inavvertitamente la potenza attiva dell'impianto, o di spegnerlo. Oppure permettere all'aggregatore di usare le funzioni di controllo destinate, invece al DSO.
<input type="checkbox"/> Secure Boot	Tecnologia che impedisce che un dispositivo, come il CCI, esegua all'avvio software non attendibile, in particolare non approvato dal costruttore.
<input type="checkbox"/> Public Key Infrastructure (PKI)	Sistema di regole, hardware e software, pensato per gestire certificati e chiavi. Il suo utilizzo aumenta significativamente la sicurezza di una rete e fornisce le fondamenta per rendere sicuri gli scambi informatici di dati.