CRITERI DI CONNESSIONE AL SISTEMA DI CONTROLLO DI TERNA

Storia delle revisioni		
Rev 00	27/12/04	Prima edizione
Rev 01	18/19/05	Seconda edizione - Revisione paragrafi 5,6 e 7
Rev 02	27/09/06	Terza edizione - Inserimento prescrizioni finalizzate al disaster recovery dei siti di Terna e dei Titolari, caratteristiche RTU
Rev 03	Luglio 2010	Quarta edizione - Aggiornamento modalità di connessione per impianti eolici
Rev 04	09/04/2018	Quinta edizione - Aggiornamento modalità di connessione e requisiti dei collegamenti Inserite prescrizioni di connessione per impianti di Sardegna e Sicilia. Inseriti dettagli degli apparati acquisizione RTU e dei protocolli di comunicazione. Ampliati requisiti relativi alla sicurezza informatica
Rev 05	19/02/2020	Sesta edizione approvata con delibera ARERA 36/2020/R/eel - Inserimento varianti per gli apparati di acquisizione dei dati dagli impianti di produzione su rete di distribuzione per Osservabilità GD e attuazione del Regolamento europeo 2017/1485 ("*System Operation Guideline*")
Rev. 6	luglio 2022	Settima edizione – Recepimento della delibera 540/2021/R/eel
Rev. 7	ottobre 2025	Criteri di connessione alla rete dati per impianti connessi alla RTN su sezioni 36 kV di stazioni Terna e aggiornamento tecnologico

INDICE

1 Scopo

L'obiettivo del documento è quello di definire i criteri di connessione al sistema di telecontrollo TERNA, di apparati e sistemi di acquisizione dati ~~relativi ad impianti soggetti all'applicazione dell'Allegato A.6 finalizzata~~funzionali a consentire lo svolgimento delle funzioni di supervisione e controllo del SEN.

2 ~~2~~ Campo di applicazione

Le prescrizioni contenute nel presente documento riguardano ~~tutti gli~~tutte le seguenti tipologie di impianti ~~soggetti all'applicazione dell'allegato A.6~~, vale a dire:

a) impianti RTN o funzionali alla RTN a tensione maggiore o uguale a ~~50~~36 kV;

b) impianti di produzione connessi direttamente alla RTN o indirettamente alla RTN per il tramite di una porzione di rete con tensione nominale pari o superiore a ~~50kV~~36 kV;

c) impianti di consumo e autoconsumo connessi direttamente alla RTN o indirettamente alla RTN per il tramite di una porzione di rete con tensione nominale pari o superiore a 36 kV;

~~50kV;~~

d) impianti delle reti di distribuzione connessi direttamente alla RTN o indirettamente alla RTN per il tramite di una porzione di rete con tensione nominale pari o superiore a 50kV;

e) impianti HVDC e Interconnector AC connessi direttamente alla RTN;

f) impianti di produzione connessi a reti di distribuzione (ivi inclusi i sistemi di distribuzione chiusi) come specificato di seguito.

La connessione di un componente deve essere effettuata per realizzare le funzioni di:

- supervisione e controllo;

- tele-regolazione;
- monitoraggio da remoto delle grandezze elettriche.

~~3~~ Il presente documento si applica sia ai sistemi di connessione dati nuovi che ai sistemi di connessione esistenti (vale a dire già installati e certificati alla data di entrata in vigore del presente documento). Con riferimento ai sistemi esistenti, si precisa, inoltre, che tali sistemi devono essere adeguati a tutte le prescrizioni entro 12 mesi dalla data di entrata in vigore della Rev. 07 del presente documento. Per gli impianti soggetti all'obbligo di istallazione dell'UPDM, l'adeguamento alle prescrizioni del presente Allegato (Rev.07) deve essere effettuato entro la data più lontana tra il termine previsto per l'istallazione dell'UPDM e 12 mesi dalla data di entrata in vigore della Rev. 07 del presente documento.

L'adeguamento dell'infrastruttura TLC e relativi apparati asserviti dovrà avvenire garantendo la continuità dei flussi informativi già scambiati con il Sistema di Difesa e il Sistema di Controllo e Conduzione di Terna. In particolare dovrà essere gestito con un processo di migrazione opportunamente condiviso con le strutture operative di Terna.

~~.~~

L'allegato A.6 (Criteri di acquisizione dati per il telecontrollo) sarà oggetto di successiva consultazione al fine di rivedere coerentemente il perimetro delle telemisure e dei telesegnali.

3 Documenti di riferimento

[1] Criteri di telecontrollo e acquisizione dati (Allegato 6 al Codice di Rete)

[2] Profili protocolli IEC 60870-5-104/101

[3] Codice di Rete

[4] Elenco Referenti TERNA

I documenti [1] e [3] sono pubblicati sul sito internet di TERNA, mentre i restanti documenti saranno forniti da TERNA all'atto del primo contatto con le strutture tecniche.

4 Premessa

TERNA realizza la supervisione ed il controllo della rete rilevante mediante l'acquisizione di tutte le informazioni necessarie allo svolgimento di tale funzione e la loro integrazione nel proprio sistema di controllo e conduzione, articolato su più centri tra loro interconnessi attraverso una rete dati dedicata.

Per perseguire tale obiettivo TERNA ha realizzato, nel rispetto dei vincoli tecnologici dei propri sistemi, una soluzione razionale, standardizzata e diffondibile a tutti i Titolari che abbiano impianti il cui esercizio ha influenza sul funzionamento della rete rilevante, affinché gli stessi possano fornire i flussi informativi necessari alla gestione unitaria del sistema elettrico.

5 Prescrizioni per la Rete elettrica Rilevante (RR)

Le prescrizioni contenute nel presente paragrafo si applicano agli impianti elencati alle lettere da a) a e) del precedente paragrafo 2 (fatta eccezione per gli impianti di produzione o consumo connessi direttamente alla RTN sul livello di tensione 36 kV per i quali si applica il successivo paragrafo 7) e devono essere adempiute dai relativi

Titolari/gestori.

5.1 Descrizione del Sistema di acquisizione dati

Il sistema di acquisizione dati si basa su una rete di comunicazione dedicata sulla quale insistono i centri di controllo della rete di trasmissione nazionale.

Tale rete è distribuita per coprire l'intero territorio nazionale e comprende diversi *Punti di Accesso* (PA) localizzati nelle seguenti Sedi Territoriali: Pero (MI), Torino, Venezia, Napoli, Roma, Palermo e Cagliari.

Figura 1 - Punti di Accesso alla rete di comunicazione di TERNA

La Figura 1 descrive la rappresentazione schematica dei Punti di Accesso alla rete di comunicazione di TERNA, ognuno dei quali è:

- predisposto per la connessione con altre reti;
- dotato di opportuni sistemi di sicurezza per il controllo degli accessi; ~~• protetto da sistemi firewall.~~
- fornito di un sistema di controllo centralizzato;
- protetto da sistemi di Cyber Security (Perimeter Defence, etc).

5.2 Regole di connessione alla Rete di comunicazione

Al fine di assicurare la necessaria ridondanza di sistemi, canali e punti di accesso (in ottica Disaster Recovery), i Titolari devono connettersi alla rete di comunicazione di TERNA in almeno due Punti differenziati di Accesso (PA).

Le indicazioni circa i punti PA di interconnessione verranno definite in apposito accordo tecnico tra il Titolare e Terna.

Nel caso di Titolare~~-~~ che invia informazioni di particolare rilevanza per la gestione della rete nazionale o che invia informazioni relative ad un elevato numero di impianti, Terna si riserva la possibilità di richiedere la predisposizione di ulteriori collegamenti e relative attestazioni ai propri punti di accesso, oltre ai due prescritti, preventivamente alla realizzazione del sistema di connessione.

Le prescrizioni relative al numero e alla tipologia delle informazioni ed il tempo di aggiornamento richiesto per ogni singolo dato/misura, sono riportati nell'Allegato A.6, relativo ai Criteri di Telecontrollo.

L'architettura e le prestazioni del sistema di interconnessione devono garantire quanto previsto in termini di tempi di trasferimento di misure, eventi spontanei e set point di regolazione.

In ogni caso, il collegamento deve essere conforme ai requisiti minimi di seguito riportati al fine di garantire l'inter-operabilità con i sistemi per la gestione del sistema elettrico e gli standard prestazionali e di sicurezza adottati per il sistema di acquisizione dati.

Il Titolare deve comunicare a Terna i riferimenti del proprio punto di contatto per la risoluzione di anomalie o irregolarità relative al sistema di acquisizione dati~~.~~ garantendone assistenza H24. Nel caso di affidamento a terzi, in qualità di fornitori di servizi tecnici (O&M), delle attività di predisposizione e di gestione tecnica e operativa dell'architettura e delle prestazioni del sistema di interconnessione al Sistema di Controllo Terna, fermo restando la responsabilità del Titolare nei confronti di Terna, il Titolare deve comunicare a Terna i riferimenti operativi della Società a cui sono eventualmente affidate tali attività (e tenere aggiornati gli stessi in caso di modifiche) e garantire in ogni caso il rispetto di tutte le prescrizioni previste nel presente Allegato ivi incluse quelle in materia di cyber security (compresa la garanzia che la Società affidataria che gestisca più Titolari garantisca una efficace segregazione tra gli stessi).

~~*5.2.1*~~ Si specifica, inoltre,che l'intera infrastruttura di connessione al sistema di Controllo (sistemi e telecomunicazioni) deve essere localizzata sul territorio nazionale italiano.

5.2.1 Requisiti dei collegamenti ai punti di accesso Terna - collegamenti esistenti (tecnologia non MPLS)

Le disposizioni di cui al presente paragrafo sono applicabili esclusivamente ai collegamenti già esistenti alla data di entrata in vigore della versione Rev.07 del presente Allegato realizzati con una tecnologia diversa da quella MPLS descritta nel successivo paragrafo 5.2.2 fino alla data di adeguamento prevista per i collegamenti esistenti riportata nel paragrafo 2 del presente Allegato.

Le due interconnessioni devono essere dedicate ad uso esclusivo della funzione in oggetto, devono essere realizzate da due provider distinti con diversificazione di percorso sull'intera tratta, nel rispetto delle prescrizioni di seguito indicate.

Prescrizioni di base valide per tutte le tipologie di circuito:

- Il Circuito deve garantire, con prove certificate prima, dopo e durante la durata del contratto, una latenza indicativamente di 50ms RTT (round trip time) con minimo

- 300 byte di Payload pena la mancata attivazione dello stesso;
- Il Provider deve garantire priorità dei pacchetti tramite meccanismi di QoS (quality of service);
- Il Circuito non deve essere in alcun modo esposto su Internet;
- Il Circuito deve afferire ad una rete privata tra PA Terna ed il Titolare;
- La velocità di connessione dovrà essere proposta dal Titolare sulla base del volume di dati da trasmettere al fine di garantire i tempi di aggiornamento richiesti nell'Allegato A.6.

Per motivi di sicurezza le politiche di routing ed il piano di indirizzi IP saranno definiti da TERNA.

Le tipologie di collegamento ammesse sono:

- Collegamento in tecnologia CDN (Circuito Diretto Numerico);
- Collegamento in tecnologia Frame Relay;
- Collegamento in tecnologia Ethernet - Layer 2 su architettura di rete MPLS o SDH; che dovrà seguire le indicazioni riportate sotto:
  - Circuito di tipo Punto-Punto Privato terminato in RJ45. Per motivi di sicurezza non potranno essere rilasciati nei CED Terna (PA) apparati quali Router (CPE) e Firewall;
  - I circuiti tra l'impianto e il primo PoP (Point of Presence) della rete dell'operatore telefonico potranno essere realizzati mediante le seguenti portanti trasmissive~~quali: Doppino rame, Link in~~ :
    - Rame;
    - Fibra Ottica~~,~~;
    - Ponti radio (su Frequenze licenziate).

I collegamenti con il Punto di Accesso scelto devono essere realizzati in modo da garantire, senza soluzione di continuità, i seguenti requisiti minimi di disponibilità e qualità del servizio conformi agli standard della rete:

- un livello di disponibilità annua del servizio atteso pari al 99.8%;
- un andamento costante di latenza della rete;
- un tempo massimo di ripristino per i disservizi che provocano la perdita di una delle due connessioni:
    - atteso: pari a 9 ore solari;
    - limite: non superiore comunque alle 18 ore solari;
- un tempo di ripristino massimo per i disservizi che degradano la qualità del servizio:
    - atteso: pari a 24 ore solari;
    - limite: non superiore comunque alle 36 ore solari.

Detti requisiti dovranno essere certificati dal Titolare all'atto della richiesta di connessione e comprovati dalla formalizzazione di uno specifico livello di servizio con il provider, al fine di garantire un livello di gestione proattiva del guasto.

Lo scambio dati deve essere realizzato utilizzando il protocollo standard *IEC60870-5-104* (di seguito IEC 104) conformemente al profilo descritto nei Profili protocolli IEC 60870-5-104/101.

L'onere relativo alla realizzazione della connessione, ed il canone dei canali di comunicazione, sono a carico del Titolare.

TERNA si riserva di accettare, a titolo provvisorio, soluzioni alternative in deroga alle suddette prescrizioni, in funzione di eventuali vincoli e particolarità esistenti. Tali soluzioni devono essere preventivamente accettate da Terna.

In particolare, nel caso di impianti ubicati in aree non servite dai canali di telecomunicazioni precedentemente descritti, a fronte di una dichiarazione inviata a Terna da parte del titolare in cui si attesti tale condizione e i tempi necessari per il suo

superamento, sarà possibile adottare soluzioni alternative. Tali soluzioni alternative comprendono, a titolo esemplificativo, il collegamento satellitare ovvero l'utilizzo del punto d'ingresso alla rete di Terna più idoneo (ad es. stazione di Terna), alle condizioni tecnico-economiche definite dalla stessa Terna. Resta ferma, in tali casi, la responsabilità in carico al Titolare della trasmissione dei dati sino ai PA di Terna.

5.2.2 Requisiti dei collegamenti ai punti di accesso - collegamenti nuovi (tecnologia MPLS)

Nel presente paragrafo vengono descritti i requisiti e le caratteristiche della soluzione tecnologica per la connessione alla rete dati che il Titolare d'Impianto deve rispettare per i collegamenti nuovi da realizzare successivamente all'entrata in vigore della versione Rev.07 del presente Allegato oppure per i collegamenti esistenti realizzati secondo la tecnologia MPLS anche a seguito di adeguamento secondo quanto previsto ai paragrafi 2 e 5.2.1. Al riguardo si specifica che, qualora l'impianto di produzione sia soggetto all'obbligo di installazione dell'UPDM, il collegamento al Sistema di Controllo deve essere realizzato tramite la stessa infrastruttura utilizzata per il collegamento al Sistema di Difesa di Terna secondo le modalità e le tempistiche di cui all'Allegato A.69. Per le altre tipologie di impianti si applica quanto previsto nel presente paragrafo 5.2.2.

In particolare, il Titolare d'impianto è tenuto a garantire la connessione alla rete dati acquisendo almeno due connessioni con le modalità indicate nel presente paragrafo.

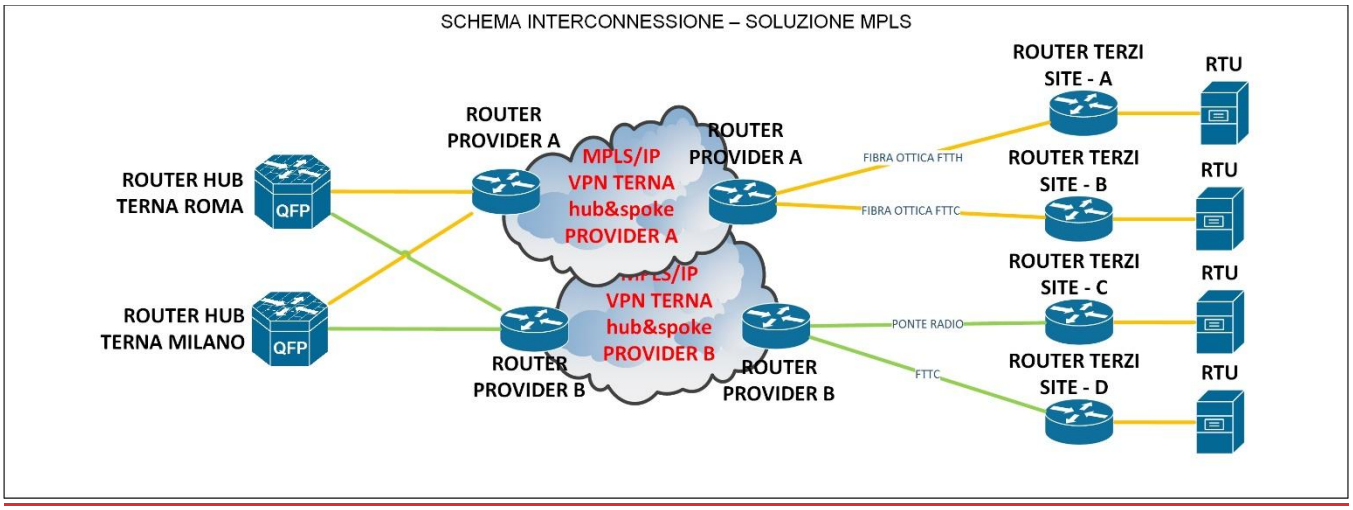
Ai fini dell'implementazione delle soluzioni tecnologiche di cui al presente paragrafo, il Titolare d'impianto è tenuto a:

- inviare a Terna, per approvazione, la proposta tecnica;
- sostenere l'onere relativo alla realizzazione delle connessioni, al canone dei canali di comunicazione e agli apparati router/switch;
- consentire a Terna la gestione esclusiva sia in lettura sia in scrittura del router;
- propedeuticamente all'attivazione della linea dati, comunicare a Terna tramite posta elettronica (tlc.noc@terna.it) gli identificativi dei circuiti dati realizzati dal provider e redigere congiuntamente con Terna adeguato verbale di collaudo, come meglio specificato nei paragrafi successivi;

– comunicare a Terna i riferimenti del proprio punto di contatto per la risoluzione di anomalie o irregolarità relative al sistema di acquisizione dati.

Tali interconnessioni dovranno essere realizzate da due provider distinti con diversificazione di percorso sull'intera tratta, nel rispetto delle prescrizioni di seguito indicate.

Restano valide le prescrizioni indicate al precedente paragrafo relativamente alla connettività Satellitare e alle sue modalità d'accesso.



Per motivi di sicurezza non è ammessa la presenza di provider intermediari tra Terna e l'impianto di produzione/gateway e quindi ciascun collegamento deve essere realizzato da un unico provider end-to-end. Presso il PA di Terna, ogni provider può rilasciare un solo ed unico circuito fisico di raccolta. Quindi lo stesso provider deve includere nel medesimo circuito fisico tutti i circuiti logici derivanti dagli impianti senza alcun onere (tecnico/economico) aggiuntivo per Terna. Non potranno essere rilasciati nei PA Terna apparati quali Router (CPE) e Firewall.

5.2.2.1 Specificità dei collegamenti di accesso

Prescrizioni di base:

- Il Circuito di collegamento (nel seguito Circuito) deve garantire una latenza inferiore a 100ms RTT (round trip time) con minimo 300 byte di Payload pena la mancata attivazione dello stesso;

- Il Circuito non deve essere in alcun modo esposto su Internet;
- Il Circuito deve afferire ad una rete privata tra PA Terna ed il sito di produzione;
- La velocità di connessione deve essere proposta dal Titolare d'impianto sulla base del volume di dati da trasmettere al fine di garantire i tempi richiesti dal sistema di controllo. La velocità proposta deve essere almeno pari a 128 Kbit/s intesa come banda minima garantita (MCR).

Terna si riserva la possibilità di effettuare verifiche in ogni momento sul rispetto delle prescrizioni del presente paragrafo.

Il Collegamento in tecnologia MPLS deve avere le seguenti caratteristiche:

- Il circuito logico deve inserirsi in una VPN Privata (Layer 3) in configurazione hub&spoke;
- La terminazione del circuito deve avvenire sul router del titolare d'impianto mediante link RJ45;
- I provider dovranno consentire l'utilizzo di Crittografia del canale End-to-End;
- Il traffico entrante ed uscente nella VPN deve essere prioritizzato dal provider come traffico "Priority-Queuing" (DSCP 46 o EF) rispetto a tutto il traffico gestito dal provider;
- Il circuito potrà essere realizzato esclusivamente con le portanti trasmissive riportate:
    1. FTTC - Fiber to the Cabinet con coda terminale in Rame mediante uno dei due protocolli (VDSL2 o EVDSL);
    2. FTTH – Fiber to the Home;
    3. Ponti radio (su Frequenze licenziate escluso LTE);
    4. FWA – Fixed Wireless Access.

Al riguardo si precisa inoltre che almeno uno dei due circuiti deve essere realizzato con portante trasmissiva terrestre (Fibra o Rame). Il Titolare d'impianto, in caso di comprovata

impossibilità a realizzare portante trasmissiva terrestre, può realizzare due circuiti Wireless di cui uno almeno su Ponte Radio.

5.2.2.2 SLA dei collegamenti di accesso

I collegamenti devono essere realizzati in modo da garantire i seguenti requisiti minimi di disponibilità e qualità del servizio conformi agli standard della rete. In particolare, per ciascun collegamento devono essere garantiti:

- un livello di disponibilità annua del servizio atteso almeno pari al 99.8%;
- un andamento costante di latenza della rete;
- un tempo di ripristino per i disservizi che provocano la perdita di una delle due connessioni non superiore alle 18 ore;
- un tempo di ripristino per i disservizi che degradano la qualità del servizio non superiore alle 36 ore;
- un'autonoma supervisione del circuito da parte del provider con annessa procedura automatica di segnalazione del guasto;

In generale, il tasso di disponibilità annua delle grandezze elettriche del singolo impianto (previste nell'Allegato A.6) deve essere pari ad almeno il 99.7%.

Qualora uno dei due collegamenti dovesse registrare frequenti malfunzionamenti, anche se di breve durata, il collegamento affetto dal malfunzionamento viene considerato nuovamente disponibile dopo 1 ora di corretto funzionamento a seguito dell'intervento di risoluzione da parte del provider.

5.2.2.3 Rete locale (LAN)

Il Titolare d'impianto è tenuto all'installazione di router dedicati all'invio delle misure. Per motivi di sicurezza le politiche di routing ed il piano di indirizzi IP sono a cura Terna.

Il router dedicato al servizio deve svolgere anche la funzione di "switch ethernet". Non è possibile installare uno switch esterno al router. Il router e l'operatore telefonico devono poter dialogare mediante protocollo di routing dinamico BGP, definito dallo standard internazionale RFC 4271. Per consentire adeguata sicurezza sul canale logico di comunicazione è necessario che il router del Titolare d'impianto sia abilitato, mediante

apposite licenze software, alla criptazione del canale di comunicazione secondo standard internazionale RFC 2401-2412 (IPSec)

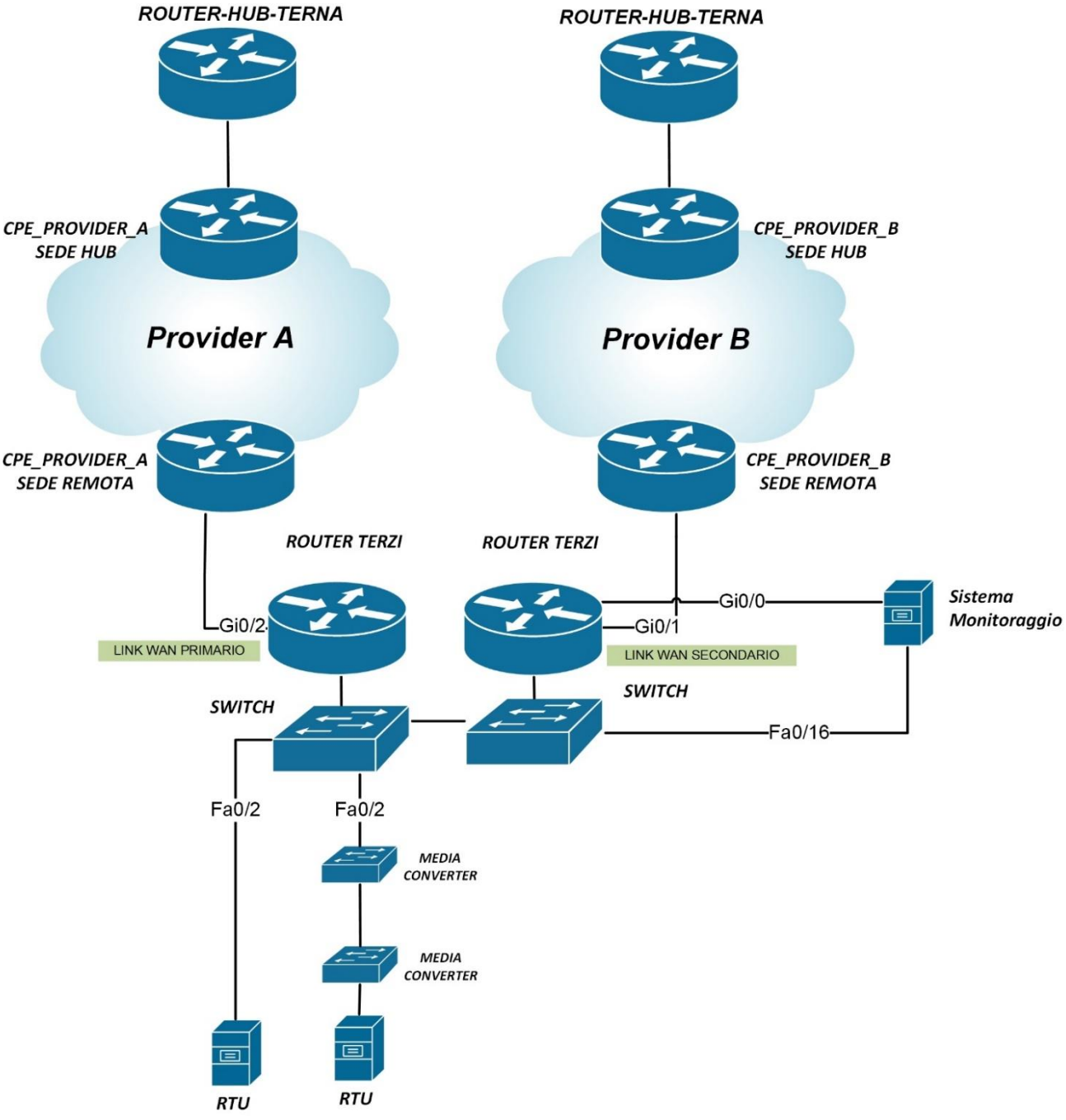
Gli apparati RTU devono essere connessi al router/switch direttamente, uno per ogni porta ethernet, e identificati tramite MAC address.

È consentito l'uso di fibre ottiche per connettere apparati installati a notevole distanza dal router/switch; in tale caso è necessario l'utilizzo di dispositivi media-converter di tipo industriale, gestibili dal router/switch.

5.2.2.4 Monitoraggio dei collegamenti ai punti di accesso

Il Titolare d'impianto dovrà dotarsi di annesso sistema di monitoraggio o definire con l'operatore telefonico adeguata soluzione di monitoraggio proattivo al fine di intervenire tempestivamente nella risoluzione del guasto delle linee di comunicazioni con Terna. Il sistema di monitoraggio, qualora realizzato dal Titolare d'impianto, può essere connesso ad una particolare porta ethernet dello switch integrato. La porta dovrà essere configurata per utilizzare solo il protocollo SNMP su un piano di indirizzamento avulso da quello di esercizio (VRF) al fine di monitorare lo stato delle linee di comunicazione. Il piano di indirizzamento IPv4 per il monitoraggio verrà fornito da Terna.

Il Titolare d'impianto, qualora dovesse verificarsi un guasto sulle linee dati, dovrà tempestivamente comunicare a Terna, mediante casella di posta tlc.noc@terna.it, la segnalazione di guasto e la relativa risoluzione. Le informazioni acquisite dal sistema possono essere utilizzate esclusivamente nel rispetto della normativa vigente in materia di riservatezza dei dati.



L'eventuale riparazione o sostituzione dei router di proprietà del Titolare d'impianto, o noleggiati da Provider telefonici, o da fornitori prescelti dai Titolari d'impianto, dovrà essere effettuata entro 3 giorni lavorativi dalla segnalazione del guasto.

Se il Titolare d'impianto decide di cambiare il provider di comunicazione scelto, deve informare Terna, almeno 60 giorni prima del cambio, al fine di pianificare gli interventi necessari sulla rete dati.

5.2.2.5 Collaudo dei collegamenti ai punti di accesso

Il Titolare d'impianto, una volta attivato il collegamento dati, deve contattare Terna per la fase di "collaudo *tecnico*" dell'impianto di rete TLC. La fase di "collaudo tecnico" verrà svolta da remoto da Terna per una durata non inferiore alle 8h lavorative nelle quali si verificheranno le rispondenze rispetto ai requisiti di rete indicati nel presente documento.

Il Titolare d'impianto dovrà inoltre fornire elementi di "*documentazione tecnica"* che contribuiranno alla certificazione dell'impianto:

1. Documentazione di progetto;
2. Codice identificativo della linea dati;
3. Riferimento Tecnico d'impianto.

La certificazione può ritenersi:

a. "superata positivamente" se collaudo e documentazione tecnica sono stati verificati con esito positivo;
b. "superata con riserva" se collaudo tecnico e almeno due elementi della documentazione tecnica sono stati verificati con esito positivo;
c. "non superata" qualora il collaudo ha avuto esito negativo o la documentazione tecnica risulti incompleta;

Il Titolare d'impianto deve quindi attendere la comunicazione di Terna in merito all'esito del collaudo. A valle della comunicazione dell'esito positivo del collaudo, Terna pone in esercizio il collegamento dati. In caso di certificazione superata con riserva/non superata, il Titolare d'impianto è tenuto a fornire tempestivamente la documentazione completa. Una volta verificata la completezza della documentazione tecnica e la corrispondenza ai requisiti tecnici di cui al presente paragrafo, Terna pone in esercizio del collegamento dati.

~~5.2.1~~5.2.3 Punti di accesso per gli impianti installati in Sardegna e Sicilia

In condizioni normali di esercizio, le funzionalità di Controllo della rete nazionale, incluse Sicilia e Sardegna, sono svolte da un sistema centrale Scada situato sul continente. Nel caso di indisponibilità delle comunicazioni tra un'isola ed il continente, viene attivato automaticamente un sistema Scada di riserva posizionato sull'isola, che assume il controllo della relativa rete ed acquisisce in modalità autonoma i dati degli impianti di competenza.

Al fine di consentire tale modalità di acquisizione, è necessario che i dati di tali impianti siano inviati verso il sistema Scada di Terna da apparati RTU o concentratori Gateway installati nell'isola stessa, attraverso due collegamenti dedicati:

- quello principale va attestato verso la sede Terna di riferimento dell'isola: Cagliari per la Sardegna e Palermo per la Sicilia;
- il secondario va attestato verso una sede PA Terna del continente.

Nel caso in cui il Titolare possieda un impianto sul continente e un impianto in Sicilia o Sardegna, esso dovrà installare un apparato RTU presso l'impianto del continente ed un apparato RTU nell'isola, attivando 2 link per ciascuna RTU.

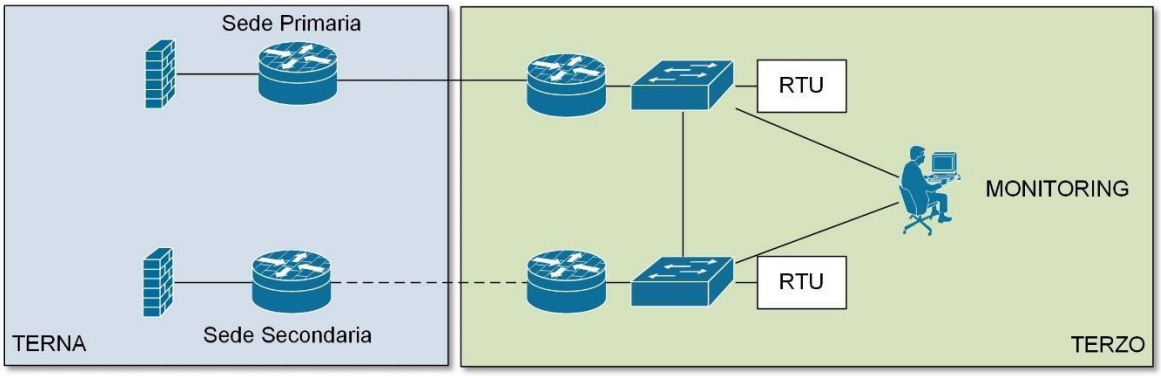
Nel caso di utilizzo di concentratore-gateway, come indicato al successivo paragrafo 7, esso deve essere installato presso una sede dell'isola e dedicato ai soli impianti dell'isola stessa.

Per poter acquisire i dati a livello applicativo mediante il citato protocollo IEC 104, le RTU che saranno installate presso le isole, dovranno avere una sessione IEC 104 in più dedicata agli scada Terna installati nelle isole, come meglio specificato in seguito.

~~5.2.2~~5.2.4 Monitoraggio dei collegamenti

Al fine di supportare il Titolare nel monitoraggio delle linee di comunicazione, Terna ne esporrà lo stato attraverso community SNMP. Pertanto, il Titolare potrà usufruire di tale

servizio per segnalare al provider l'eventuale malfunzionamento degli apparati e/o del collegamento.



~~5.2.3~~5.2.5 ~~5.2.4~~ Data Engineering

È richiesto che il Titolare programmi autonomamente il proprio apparato periferico RTU, o il proprio sistema concentratore di più impianti, connesso logicamente alla rete di comunicazione di TERNA, previo accordo con TERNA e secondo quanto indicato nell'Allegato A.6.

Il Titolare è inoltre responsabile, secondo quanto previsto nell'Allegato A.6, della fornitura a TERNA e dell'aggiornamento degli schemi unifilari di impianto e di tutti i dati necessari per la corretta identificazione dei dati scambiati, necessari per configurare gli impianti nella base dati del sistema di controllo di TERNA. Le modalità di tale fornitura saranno comunicate dai referenti TERNA in sede di primo contatto.

5.3 Tipologie di reti e caratteristiche degli apparati di acquisizione

Per l'accesso alla propria rete di comunicazione, TERNA ha convenzionalmente definito diverse tipologie di connessione di Titolari, basate sul numero di impianti e/o sul tipo di rete utilizzato.

~~Conformemente a quanto indicato in [1] le~~Le modalità di collegamento possono essere di tre tipi:

- Acquisizione diretta (Figura 2);

- Acquisizione diretta, via Intranet (Figura 3);
- Acquisizione indiretta, via Intranet (Figura 4).

Il collegamento deve essere effettuato esclusivamente secondo le modalità previste al paragrafo 5.3.1 - Acquisizione diretta per le seguenti tipologie di impianti:

- per gli impianti di produzione soggetti all'obbligo di istallazione dell'apparato UPDM, per i quali è richiesto l'utilizzo della medesima infrastruttura per le finalità legate alla connessione al Sistema di controllo di Terna di cui al presente Allegato e per le esigenze di connessione al Sistema di Difesa Terna di cui all'Allegato A.69 del Codice di Rete;
- per i sistemi di compensazione continua del reattivo asserviti all'erogazione del servizio di controllo dei profili di tensione e dei flussi di potenza reattiva sulla RTN installati presso impianti di consumo o di distribuzione;
- per impianti composti da almeno una unità abilitata in forma singola o aggregata alla fornitura del servizio di riserva per il ripristino della frequenza ad attivazione automatica (aFRR);
- laddove richiesto da Terna per particolari impianti di produzione e di consumo particolarmente significativi per la gestione in sicurezza del SEN.

5.3.1 Acquisizione Diretta

La tipologia di *Acquisizione Diretta* (Figura 2) con collegamenti dedicati, prevede la corrispondenza *uno-a-uno* fra apparati periferici RTU installati negli impianti ed apparati periferici RTU rappresentati nella base dati del sistema di controllo di TERNA.

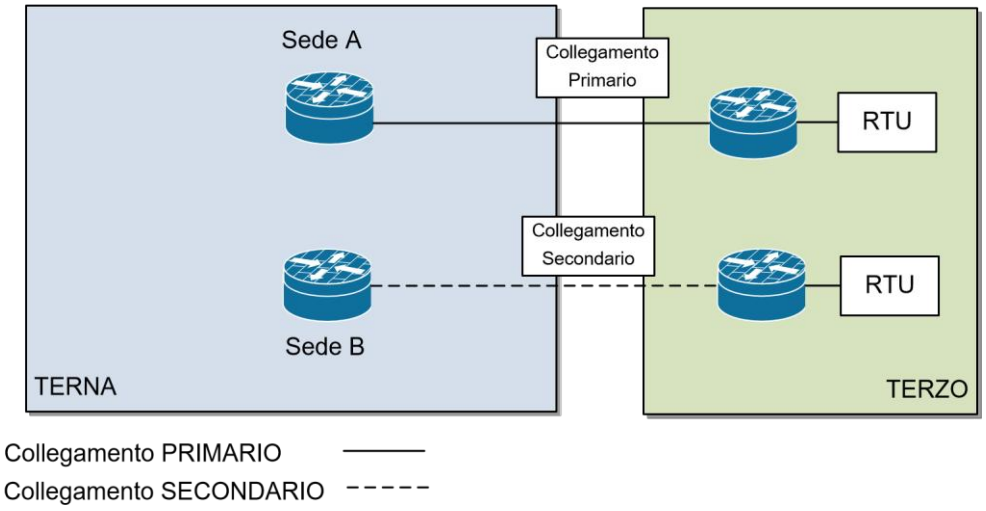


Figura 2 - Acquisizione Diretta

5.3.2 Acquisizione Diretta via Intranet

La tipologia di *Acquisizione Diretta* via Intranet (Figura 3a) prevede l'utilizzo della rete Intranet del Titolare, attraverso cui si rendono raggiungibili gli apparati periferici RTU installati negli impianti, con corrispondenza *uno-a-uno* con gli apparati periferici RTU rappresentati nella base dati del sistema di controllo di TERNA.

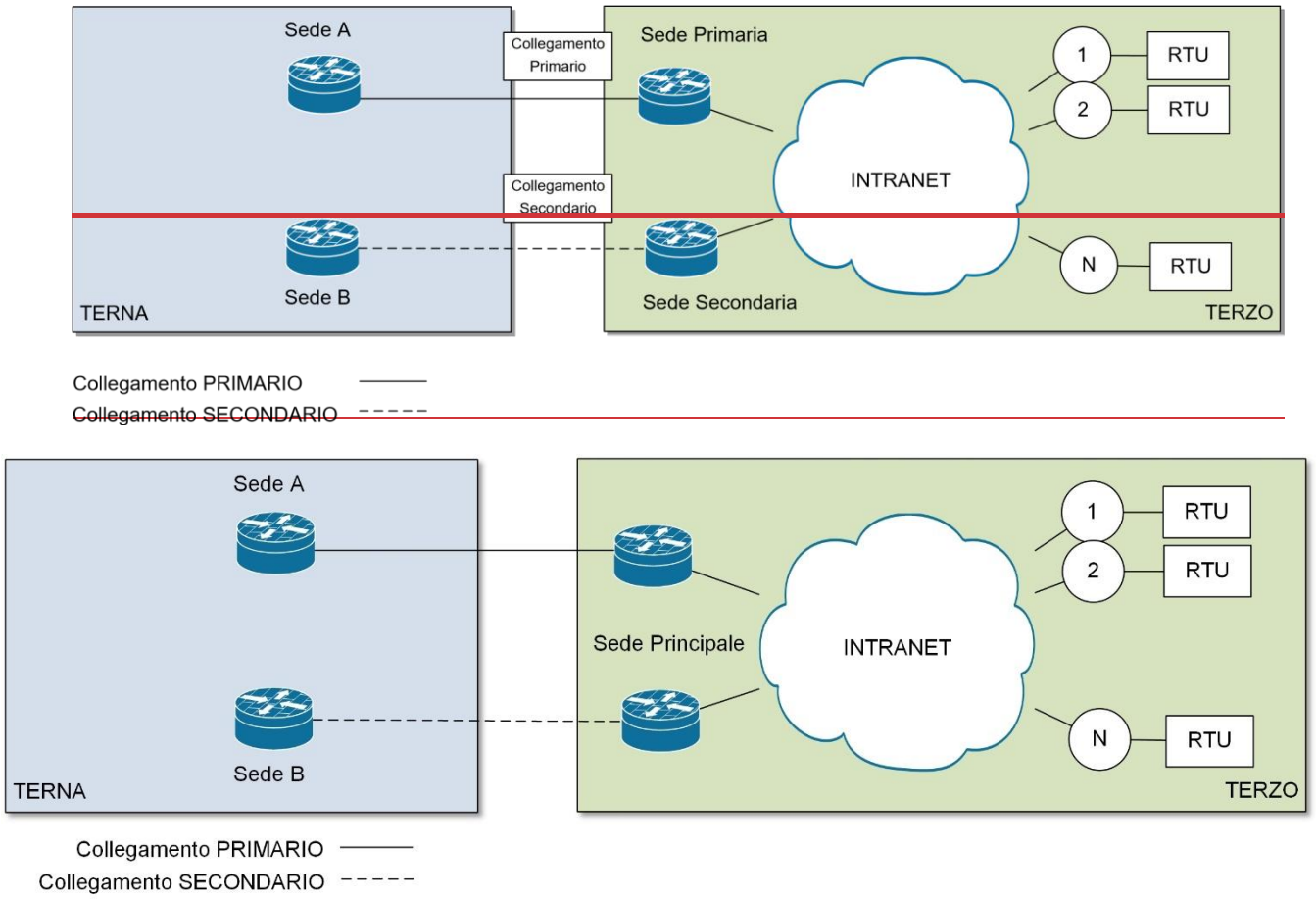


Figura 3a - Acquisizione Diretta - via Intranet

Se la somma della potenza nominale degli impianti di produzione del Titolare connessi al Sistema di Controllo per il tramite dell'intera infrastruttura di telecomunicazione eccede i 1000 MW , deve essere prevista ulteriore ridondanza dei siti di accesso da/verso Terna, nonché l'ulteriore ridondanza delle connessioni verso i punti di accesso Terna, così come indicato nella figura seguente (Figura 3b).

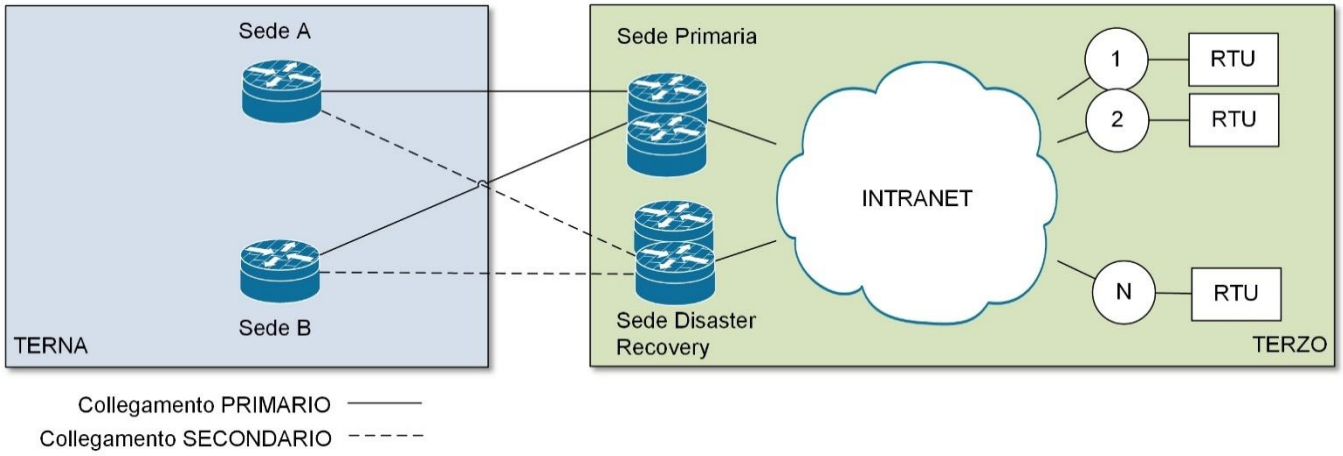
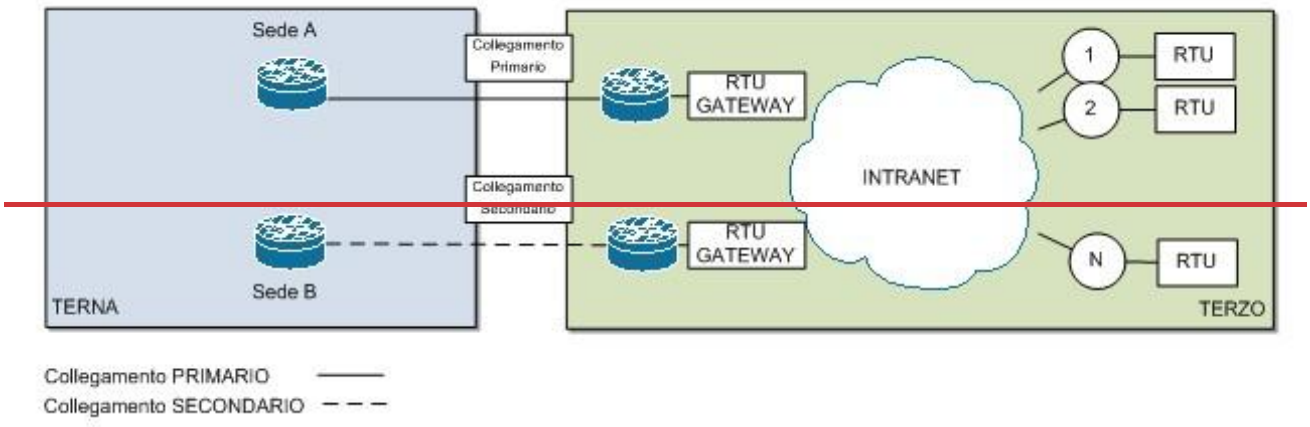


Figura 3b - Acquisizione Diretta - via Intranet ridondata

5.3.3 Acquisizione Indiretta

La terza tipologia di connessione, cioè l'*Acquisizione Indiretta* (Figura 44a) prevede la presenza di un *Concentratore-Gateway* ed utilizza il concetto di *RTU Virtuale* in modo da facilitare la coesistenza del sistema di controllo di TERNA e l'eventuale sistema di controllo e conduzione del Titolare, disaccoppiando logicamente le rispettive basi dati.

Il concentratore-gateway deve essere configurato in modo da accettare connessioni multiple provenienti dai centri di controllo di TERNA, ad esempio fornendo diversi indirizzi IP, in modo da suddividere i dati degli impianti per aree di competenza.



~~Figura 4 - Acquisizione Indiretta - via Intranet~~

Ogni concentratore Gateway può gestire impianti ~~Al fine~~di ~~rispondere ai~~produzione per un totale massimo di 500 MW di potenza nominale o di potenza abilitata nel caso di UVA (Unità virtuali aggregate). Per garantire i requisiti di disponibilità richiesti, il Concentratore-Gateway (GTW) deve essere ~~opportunamente~~ ridondato e, nel caso di Titolari di rilevanza nazionale Terna si riserva la possibilità di richiedere anche la predisposizione di un sito di backup sul quale installare un secondo Concentratore-Gateway ridondato, utilizzabile in caso di indisponibilità del sito primario.

~~*5.3.4*~~

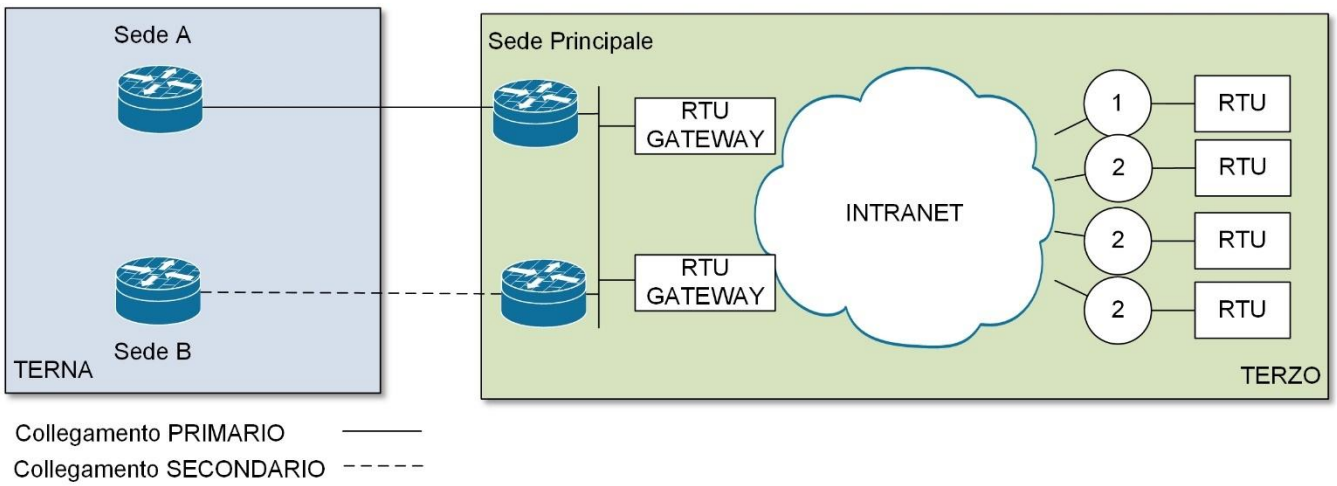


Figura 4a - Acquisizione Indiretta - via Intranet

Se la somma della potenza nominale degli impianti di produzione del Titolare connessi al Sistema di Controllo per il tramite dell'intera infrastruttura di telecomunicazione eccede i 1000 MW, deve essere prevista l'ulteriore ridondanza dei siti di di accesso da/verso Terna e delle connessioni verso i punti di accesso Terna, così come indicato nella figura seguente.

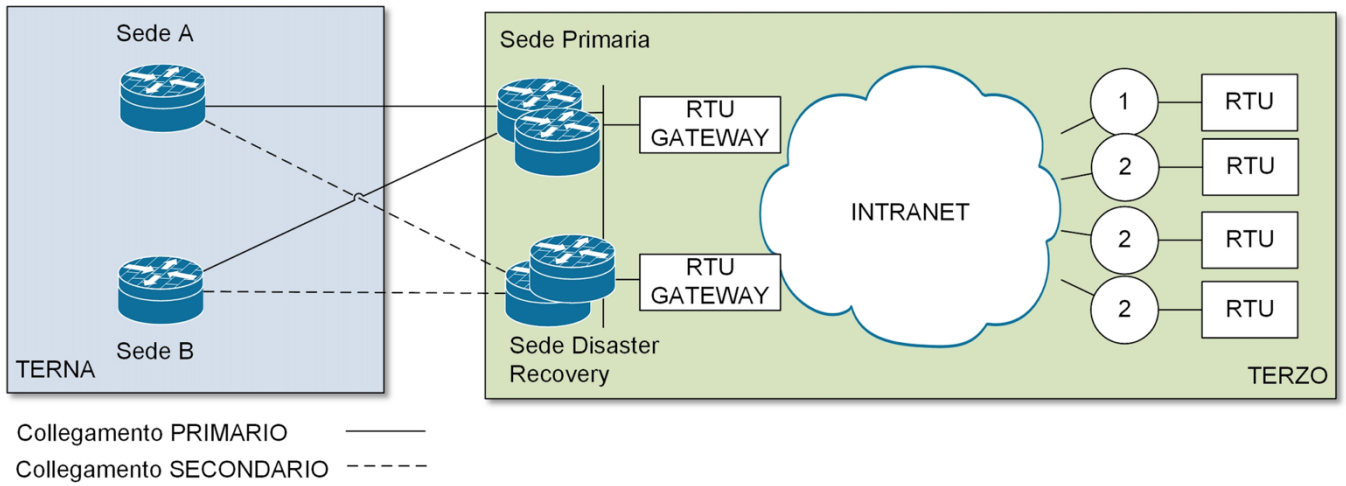


Figura 4b - Acquisizione Indiretta - via Intranet ridondata

Il Titolare deve comunicare a Terna la composizione degli impianti sottesi ad ogni concentratore in termini di taglia e tipologia nonché sottoporre all'approvazione di Terna l'architettura relativa alle infrastrutture di collegamento tra gli apparati concentratori e i singoli apparati installati presso gli impianti.

5.3.4 Caratteristiche degli apparati periferici RTU/GTW

Le caratteristiche degli apparati periferici RTU devono essere tali da rispondere ai requisiti di affidabilità e disponibilità richiesti:

- disponibilità maggiore o uguale a 99,9%;
- l'apparato RTU dovrà essere equipaggiato con CPU ridondate
- l'apparato RTU/GTW dovrà essere predisposto per gestire le seguenti sessioni logiche verso i sistemi Terna (multisessione IEC104): o 3 sessioni nel caso di impianti situati nel continente; o 4 sessioni nel caso di impianti situati nelle isole;
- l'apparato RTU utilizzato nelle modalità di acquisizione diretta deve essere dedicato ad utilizzo esclusivo dello scambio dati con TERNA. Nel caso in cui il Titolare abbia necessità di connettere l'apparato RTU anche ai propri sistemi, il firmware in esso

installato dovrà poter gestire tutte le sessioni IEC 104 necessarie: quelle del Titolare e quelle dedicate ai sistemi Terna, con separazione logica dei dati e dei relativi identificatori IEC 60870-5-104;

- se l'apparato RTU è predisposto per gestire il riconoscimento del centro chiamante (master IEC104) attraverso l'indirizzo IP dello stesso, si richiede che ogni sessione dovrà poter gestire almeno 4 indirizzi IP da utilizzare alternativamente in funzione del centro Terna chiamante;
- se l'apparato RTU o Gateway è ad uso esclusivo Terna, esso deve essere dotato di interfaccia LAN dedicata per garantire che la connettività verso i sistemi di Terna avvenga su segmenti di LAN fisicamente separati dal resto dell'impianto e da altri servizi del Terzo. Negli altri casi deve essere garantita la segregazione dei flussi logici con modalità da condividere con Terna.

5.3.5 Caratteristiche degli apparati periferici Router

Le caratteristiche degli apparati Router devono essere tali da rispondere ai requisiti di affidabilità e disponibilità richiesti:

- l'apparato Router e Switch (integrato) dovrà essere conforme alle specifiche IEC61850-3 e IEC-1613;
- doppia Alimentazione;
- supporto alla criptazione (IPSEC);
- possibilità di Interfacciarsi con collegamenti in Fibra Ottica Multimodale;
- supporto ai protocolli di Routing più comuni.

Gli apparati saranno richiesti, uno per provider, dal Titolare all'atto della sottoscrizione del Contratto previo inoltro dell'offerta Tecnica alle strutture Terna competenti. L'apparato dovrà essere coperto da Garanzia del Titolare al fine di attuare le politiche di ripristino in caso di guasto o malfunzionamento secondo le prescrizioni di cui al presente Allegato. Gli apparati Router e le RTU finali dovranno essere interconnessi in maniera diretta tramite lo switch integrato.

5.3.6 Protocollo di comunicazione

Gli apparati RTU/GTW comunicano in multisessione con i sistemi Terna mediante protocollo applicativo IEC 60870-5-104 con profilo Terna, le cui caratteristiche principali sono indicate di seguito.

Il protocollo deve implementare la multisessione effettiva prevista dalla norma usando sempre la porta 2404 lato client. Pertanto, non sono ammesse implementazioni della multisessione che usano porte differenti.

~~Nei prossimi anni Terna adotterà il protocollo IEC-62351 (cosiddetto IEC104 sicuro) che implementa modalità di trasferimento dei dati sicura sia a livello di trasporto (TLS) sia a livello applicativo. Si richiede che L~~le RTU istallate ~~siano già~~devono essere predisposte per la migrazione su ~~tale~~ protocollo IEC-62351 che avverrà gradualmente secondo un piano condiviso con i Titolari~~.~~.

5.3.6.1 Caratteristiche del profilo 104 Terna e parametri

Common Address	2 ottetti (byte)	
Information object address	3 ottetti	
Cause of transmission	2 ottetti	
Massima lunghezza APDU	253 ottetti	
Parametro T0	30 secondi	modificabile durante point to point
Parametro T1	90 secondi	modificabile durante point to point
Parametro T2	10 secondi	modificabile durante point to point
Parametro T3	30 secondi	modificabile durante point to point
Finestra K	Tipicamente 12 APDUs	modificabile durante point to point
Finestra W	Tipicamente 8 APDUs	Modificabile durante point to point
Numero porta TCP	2404	

5.3.6.2 Operatività e performance dell'apparato RTU

- Sincronizzazione esterna: l'RTU/GTW non deve aspettarsi il segnale di sincronizzazione dagli SCADA Terna.
- Gli indirizzi IP chiamanti (lo SCADA di Terna è client e la RTU/Gateway è server) devono essere >= 4 con le sessioni contemporanee specificate nel paragrafo precedente.
- L'apparato RTU/GTW deve rispondere correttamente al comando di GENERAL INTERROGATION (telegramma 104 "C_IC_NA_1") inviato dai sistemi Terna nella fase iniziale di start della connessione in 104. Tale comando viene inviato per ogni common address. Nel caso di Gateway si avrà un common address generale del GTW sul quale, nella fase di General Interrogation, deve essere inviata la diagnostica principale e un common address per ciascuna sub-RTU sul quale, nella fase di General Interrogation, saranno inviate le Telesegnalazioni (TS) di diagnostica della sub-RTU, le TS relative agli stati d'organo di manovra e ad altri segnali operativi configurati nell'apparato nonchè le posizioni dei Variatori sotto carico (causa di trasmissione "interrogato da General Interrogation").
- A parte la fase iniziale di General Interrogation, durante la restante parte della sessione attiva, le TS relative alla posizione di organi (tipologia DPI) e agli altri segnali operativi, devono essere trasmessi con causa di trasmissione "spontanea" e attraverso il ciclo di background scan programmato ogni minuto. Se la causa di trasmissione è "spontanea" il telegramma deve essere di tipo M_DP_TB_1 o M_SP_TB_1 se si dispone di clock agganciato a GPS, mentre in tutti gli altri casi i segnali devono essere trasmessi con telegramma M_DP_NA_1 o M_SP_NA_1.
- Le misure (tipologia AMI) devono essere trasmesse ciclicamente (causa di trasmissione periodica) tipicamente ogni 4s per le TM generiche degli impianti di produzione e Utenza, ogni 2s per le TM relative alla teleregolazione di tensione, di 20s per gli impianti di distribuzione. Esse devono avere valori normalizzati a 1. Il telegramma sarà M_ME_NA_1. Inoltre, essendo trasmesse ciclicamente, le misure non devono avere soglie di aggiornamento (data reduction).

- Nel caso in cui la RTU fosse collegata lato campo in modalità digitale attraverso LAN o bus, se il tempo di campionamento è programmato a 2 o 4 secondi, necessita assicurare che il tempo di latenza delle TM all'interno degli apparati da cui vengono prelevate sia inferiore al secondo.
- Le posizioni dei VSC (variatori sotto carico) codificate in BCD (binary code decimal) con tipologia DMI, devono essere trasmesse spontaneamente (causa di trasmissione spontanea) e con ciclo ci background scan a 1 minuto. Il telegramma sarà M_ST_NA_1.
- Il sistema Terna invia i setpoint per la teleregolazione di frequenza/potenza e per la teleregolazione di tensione con ASDU C_SE_NA_1. La frequenza di invio è di 2s sia per la teleregolazione di frequenza/potenza, sia per la teleregolazione di tensione. Inoltre, i setpoint per la teleregolazione di tensione sono 2. La RTU deve avere prestazioni sufficienti a garantire l'elaborazione di tali oggetti scada con tempi complessivi di risposta inferiori a 500ms per ciascuno dei setpoint, gestendo anche l'invio in parallelo dei setpoint dai nostri centri. Infine, la RTU deve adottare una logica di automazione in grado di rilevare il mancato invio dei setpoint per ciascuna tipologia di regolazione ed inviarla al regolatore.
- La RTU deve essere in grado di ricevere e di trasmettere file secondo le modalità previste dal protocollo IEC-104.
-

5.3.6.3 Diagnostica RTU

Nell'apparato RTU/GTW deve essere implementata la diagnostica in conformità al citato profilo IEC-104 di Terna. Gli oggetti di diagnostica vengono battezzati per object address.

Tutti gli oggetti di diagnostica devono essere trasmessi con messaggi 104 di tipo "M_SP_NA_1" con causa trasmissione "spontanea" e con ciclo di background scan a 1 minuto (oltre che in risposta alla GENERAL INTERROGATION).

Gli oggetti di diagnostica da implementare sono:

Common address = xxx, object address = 12845079 - Gateway/RTU guasto

Common address = xxx, object address = 12845080 - Gateway/RTU attivo

Common address = xxx, object address = 12845081 - Gateway/RTU sincronizzato
Common address = xxx, object address = 12845082 - Clock esterno inoperabile
Common address = xxx, object address = 12845115 - Alimentazione guasta
Common address = xxx, object address = 12845116 - CPU 1 on line
Common address = xxx, object address = 12845117 - CPU 2 on line
Common address = xxx, object address = 12845118 - CPU 1 operabile
Common address = xxx, object address = 12845119 - CPU 2 operabile

Per ogni sub-RTU del Gateway devono essere trasmessi i seguenti oggetti di diagnostica:

Common address = yyyy, object address = 12845104 - SUBRTU inoperable
Common address = yyyy, object address = 12845105 - SUBRTU out of service dove yyyy è il Common address della sub-rtu

5.3.7 RTU Virtuali

L'architettura logica per la gestione dell'Acquisizione Indiretta prevede due livelli di scambio dati secondo il protocollo applicativo IEC 60870-5-104:

- il primo è rappresentato dall'interazione fra RTU Virtuali, residenti nei concentratori-gateway (che svolgono le funzioni di slave), ed i Front-End del sistema di controllo di TERNA (che svolgono le funzioni di master);
- il secondo livello è rappresentato dall'interazione tra gli apparati RTU, residenti negli impianti (con funzioni di *slave*), ed i concentratori-gateway (con funzione di *master*), che utilizzano al loro interno una struttura dati specifica per ogni RTU definita convenzionalmente *sub RTU*;

pertanto, all'interno dei concentratori-gateway i dati dovranno essere organizzati secondo dette regole che, oltre a garantire l'interoperabilità verso il sistema di controllo di TERNA, permettono al Titolare di definire senza vincoli le modalità per la gestione dello scambio dati tra i propri centri e gli impianti (Figura 5).

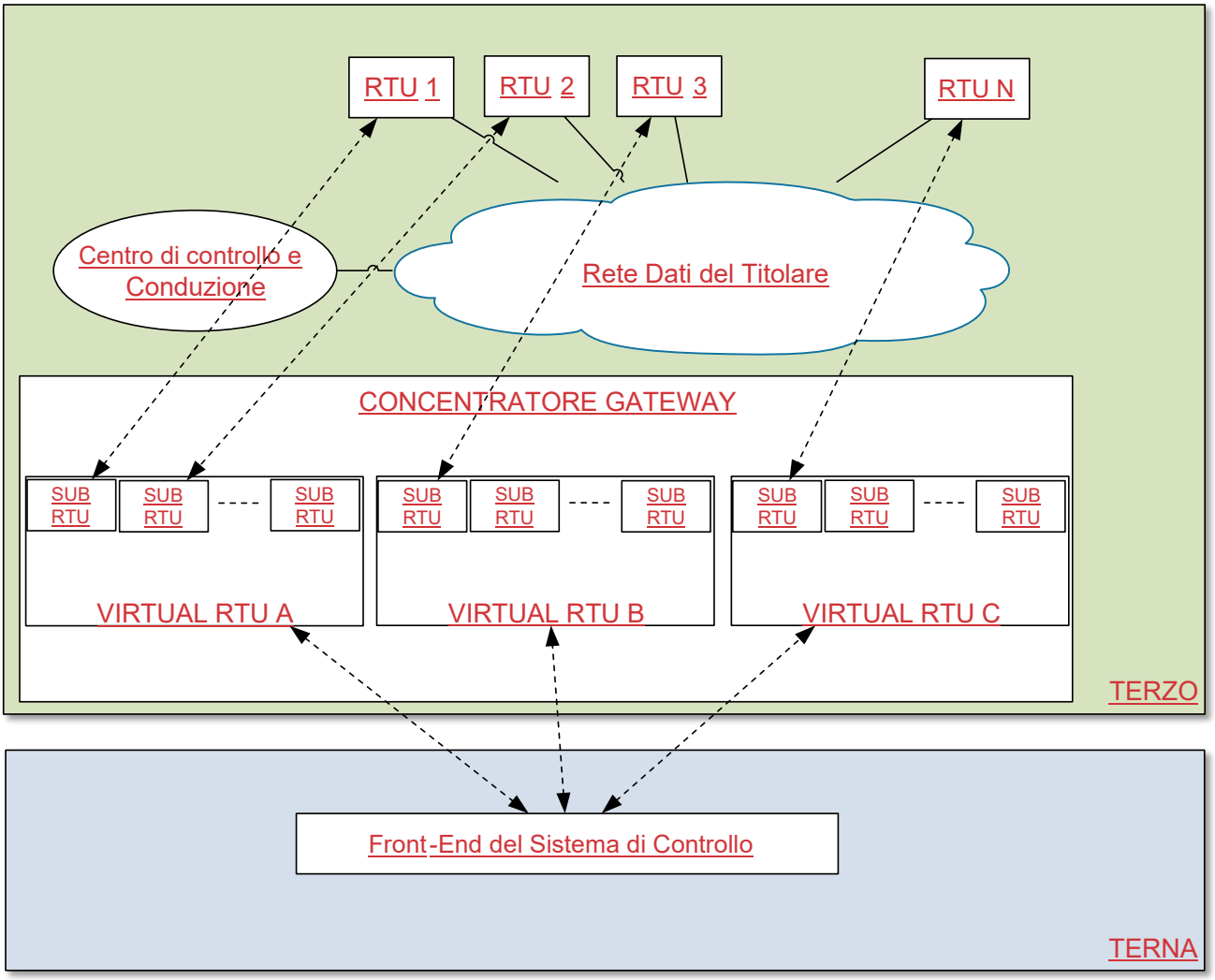


Figura 5

Il numero e la configurazione delle RTU Virtuali e delle Sub RTU, da predisporre nei Concentratori-Gateway, sarà concordata fra Titolare e TERNA, in modo da tenere in considerazione il numero di Front-End coinvolti.

Ogni RTU Virtuale dovrà essere identificata attraverso un indirizzo IP ed utilizzerà un Common- address per ogni Sub RTU. Il Common-address sarà composto da un campo denominato Common line (identificatore della RTU Virtuale), e da un campo denominato RTU number (identificatore del Sub RTU).

La ridondanza dei Concentratori-Gateway, al fine di ottenere i valori di disponibilità richiesti, dovrà essere gestita dal Titolare in modo da garantire la corrispondenza degli identificatori a livello IP in caso di commutazione automatica sull'apparato di back-up.

5.3.8 Piani di indirizzamento

Per garantire la separazione della rete di comunicazione e per provocare il minimo impatto ai sistemi dei Titolari, TERNA ha definito delle classi di indirizzamento che saranno assegnate ai singoli utenti della rete. L'assegnazione di dette classi agevolerà anche l'attività di identificazione e controllo degli accessi.

Nel caso di impianti connessi direttamente al Punto di Accesso (Figura 2), questi dovranno essere dotati di un router dedicato e di una LAN dedicata, in modo da evitare rischi di accessi non desiderati.

Nel caso di connessione con una rete Intranet (Figg. 3 e 4) è necessario che anche il Titolare preveda l'attivazione di sistemi per la sicurezza perimetrale (Firewall), per segregare la porzione di rete dal resto della rete intranet. Le politiche di sicurezza da applicare sul Firewall dovranno essere concordate con TERNA.

Qualora il piano di indirizzamento assegnato da TERNA non coincida con quello del titolare è opportuno che quest'ultimo attivi la funzione di Network Address Translation (NAT) pr mantenere invariata la politica di gestione della propria rete ed assicurare la conformità ai requisiti di TERNA.

6 Prescrizioni per gli impianti di produzione connessi in MT alla rete di distribuzione

Le prescrizioni contenute nel presente paragrafo riguardano le modalità e i requisiti tecnici e prestazionali da rispettare nell'invio delle grandezze elettriche, di cui all'Allegato A.6 del Codice di Rete, relative agli impianti elencati alla lettera f) del precedente paragrafo 2 vale a dire impianti di produzione collegati sulla rete MT di distribuzione[1].

Le grandezze elettriche dell'allegato A.6 devono essere inviate al sistema informatico di Terna per il tramite del distributore alla cui rete sono connessi gli impianti di produzione. A tal fine, il distributore competente può avvalersi anche di un distributore terzo per l'espletamento del servizio.

Le modalità di invio sono disciplinate al successivo paragrafo 6.1[2].

Con riferimento alle modalità di invio si segnala che:

- il rispetto dei requisiti tecnici e prestazionali degli apparati di campo installati presso gli impianti di produzione (Controllore Centrale di Impianto, CCI[3]) deve essere garantito dal titolare dell'impianto di produzione (nel seguito Titolare);
- il rispetto dei requisiti tecnici e prestazionali dei canali di comunicazione funzionali all'invio dei dati verso Terna, deve essere garantito dal distributore (nel seguito, "distributore").

6.1 Descrizione del Sistema di acquisizione dati – Invio tramite il Distributore

L'invio dei dati al sistema di Terna di acquisizione per il tramite del distributore deve avvenire mediante l'utilizzo di un sistema concentratore/gateway.

La potenza massima installata degli impianti di produzione sottesi a ciascun Concentratore-Gateway (GTW) non può superare 500 MW.

Il distributore deve comunicare a Terna la composizione degli impianti sottesi ad ogni concentratore in termini di taglia e tipologia. Il distributore deve garantire il rispetto degli stessi

[1] Ivi inclusi gli impianti connessi su reti appartenenti a sistemi di distribuzione chiusi.

[2] Le modalità di calcolo e di monitoraggio dei requisiti tecnici e prestazionali verranno condivisi in un apposito tavolo tecnico con i distributori

[3] Le cui specifiche tecniche sono contenute negli Allegati O e T alla Norma CEI-016.

requisiti indicati al precedente paragrafo 5, sia relativamente alle caratteristiche dei collegamenti verso Terna sia alla ridondanza degli apparati di rete e del concentratore/gateway. In particolare, vanno garantiti i requisiti di disponibilità annua non inferiore al 99,8% per i collegamenti verso i punti di accesso Terna e non inferiore al 99,9% per il concentratore Gateway.

In aggiunta a tali requisiti, è necessario garantire una disponibilità delle grandezze elettriche del singolo impianto di produzione superiore al 98%. A tal fine:

- Il titolare dell'impianto di produzione, responsabile dell'installazione e manutenzione del CCI[1], deve garantirne una disponibilità annua non inferiore al 99%;
- Il distributore deve garantire che la disponibilità annua del collegamento verso il CCI non sia inferiore al 99,3% e verificare che nella trasmissione a Terna delle grandezze elettriche del singolo impianto sia rispettato il tasso di disponibilità di almeno il 98%.

6.1.1 Data engineering

È richiesto che il distributore programmi autonomamente ciascun sistema concentratore/gateway di più impianti, connesso logicamente alla rete di comunicazione di Terna, previo accordo con Terna e secondo quanto indicato nell'Allegato A.6.

Il distributore è inoltre responsabile, sempre secondo quanto previsto nell'Allegato A.6, della fornitura a Terna di tutte le informazioni necessarie per la corretta identificazione dei dati scambiati.

6.1.2 Collegamenti logici

Infine, si precisa che i flussi dati della GD inviati dal distributore verso Terna devono essere indipendenti dai flussi già attivi per le finalità di telecontrollo della rete AT e del sistema di difesa. Nel caso in cui un distributore abbia già un collegamento IEC60870-5104 utilizzato per alimentare in tempo reale i suddetti sistemi di Terna, il distributore deve pertanto attivare

[1] Il tasso di disponibilità riguarda sia l'apparato campo (CCI) che il relativo sistema di comunicazione a livello di impianto di produzione che consente la rilevazione dei dati oggetto di scambio e la messa a disposizione degli stessi al punto di confine con il distributore.

un nuovo concentratore/gateway (virtuale o fisico), dedicato alla GD, che dovrà essere identificato in rete attraverso un nuovo indirizzamento IP (Internet Protocol).

7 ~~7~~ Requisiti dei collegamenti alla rete dati del sistema di controllo per gli Impianti connessi a sezioni a 36kV di Stazioni Terna

Le prescrizioni contenute nel presente paragrafo riguardano le modalità e i requisiti tecnici e prestazionali per i collegamenti alla rete dati da realizzare ai fini dell'invio delle grandezze elettriche, di cui all'Allegato A.6 del Codice di Rete, relative agli impianti connessi a sezioni 36 kV di Stazioni Terna.

7.1 Regole di connessione alla Rete di comunicazione

La soluzione tecnologica per la connessione alla rete dati del sistema di Controllo Terna deve essere utilizzata anche per la connessione ai sistemi Terna di difesa e monitoraggio (cfr. Allegato A.69) e prevede l'utilizzo di Fibra Ottica proveniente dall'impianto del Titolare alla Stazione Terna di connessione. A tal fine il Titolare d'impianto è tenuto a:

- Predisporre due cavi fisici distinti realizzati mediante Fibra ottica Monomodale (G.652D) diretta verso la Stazione Terna adiacente;
- Realizzare un pannello di terminazione Fibra Ottica da installare all'interno dell'edificio Terna adibito allo scopo, nelle modalità che verranno indicate da Terna in fase progettuale;
- Manutenere i due canali in Fibra Ottica nel rispetto del paragrafo 7.1.2;
- Installare e manutenere presso il proprio impianto due Router dedicati al servizio in oggetto.

Il confine tra il canale in FO de Titolare d'impianto e quello di Terna è posto nella cassetta di giunzione presente all'interno dell'edificio 36 kV di Stazione.

7.1.1 Rete locale (LAN)

I router dedicati al servizio devono svolgere anche la funzione di "switch ethernet" e devono essere gestiti da Terna (il modello di router/switch deve essere quindi compatibile con l'architettura di rete Terna). Il router deve poter dialogare mediante protocollo di routing

dinamico BGP, definito dallo standard internazionale RFC 4271. Per consentire adeguata sicurezza sul canale logico di comunicazione è necessario che il router del Titolare d'impianto sia abilitato, mediante apposite licenze software, alla criptazione del canale di comunicazione secondo standard internazionale RFC 2401-2412 (IPSec).

Non è possibile installare uno switch esterno al router. Gli apparati di campo devono essere connessi al router/switch direttamente mediante porta RJ45, ed identificati tramite MAC address.

È consentito l'uso di fibre ottiche per connettere apparati installati a notevole distanza dal router/switch; in tale caso è necessario l'utilizzo di dispositivi media-converter di tipo industriale.

I nodi Router devono consentire l'interconnessione alla Stazione Terna mediante FO Monomodale; pertanto, è necessario che gli stessi vengano equipaggiati con trasduttori elettroottici (SFP) adatti allo scopo.

7.1.2 SLA dei nuovi collegamenti di accesso

I collegamenti devono essere realizzati in modo da garantire i seguenti requisiti minimi di disponibilità e qualità del servizio conformi agli standard della rete. In particolare, per ciascun collegamento devono essere garantiti:

- un livello di disponibilità annua del servizio atteso almeno pari al 99.8%;
- un andamento costante di latenza della rete;
- un tempo di ripristino per i disservizi che provocano la perdita di una delle due connessioni non superiore alle 18 ore;
- un tempo di ripristino per i disservizi che degradano la qualità del servizio non superiore alle 36 ore;
- un'autonoma supervisione del circuito da parte del provider con annessa procedura automatica di segnalazione del guasto.

In generale, il tasso di disponibilità annua delle grandezze elettriche del singolo impianto (previste nell'Allegato A.6) deve essere pari ad almeno il 99.7%.

7.1.3 Monitoraggio e Manutenzione dei collegamenti in Fibra Ottica e apparati di rete

Il Titolare d'impianto deve identificare adeguata soluzione di manutenzione al fine di intervenire tempestivamente sia nella risoluzione del guasto delle Fibre ottiche con Terna che su guasti HW dei nodi di rete. Il Titolare deve dotarsi di sistema di monitoraggio locale e autonomamente gestito. Il sistema di monitoraggio, qualora realizzato dal Titolare d'impianto, può essere connesso ad una particolare porta ethernet dello switch integrato. La porta deve essere configurata per utilizzare solo il protocollo SNMP su un piano di indirizzamento avulso da quello di esercizio al fine di monitorare lo stato delle linee di comunicazione. Il piano di indirizzamento IPv4 per il monitoraggio viene fornito da Terna.

Il Titolare d'impianto, qualora dovesse verificare un guasto sulle linee dati, è tenuto a comunicare tempestivamente a Terna, mediante casella di posta tlc.noc@terna.it, la segnalazione di guasto e la relativa risoluzione. Le informazioni acquisite dal sistema possono essere utilizzate esclusivamente nel rispetto della normativa vigente in materia di riservatezza dei dati.

7.1.4 Collaudo dei collegamenti ai punti di accesso

Il Titolare d'impianto, una volta attivato il collegamento dati, deve contattare Terna per la fase di "*collaudo tecnico*" dell'impianto di rete TLC. La fase di "collaudo tecnico" verrà svolta da remoto da Terna per una durata non inferiore alle 8h lavorative nelle quali si verificheranno le rispondenze rispetto ai requisiti di rete indicati nel presente documento.

Il Titolare d'impianto dovrà inoltre fornire elementi di "*documentazione tecnica"* che contribuiranno alla certificazione dell'impianto:

a. Prove di continuità dei vettori in Fibra Ottica;
b. Riferimento Tecnico d'impianto;

La certificazione può ritenersi:

a. "superata positivamente" se collaudo e documentazione tecnica sono stati verificati con esito positivo;
b. "superata con riserva" se collaudo tecnico e almeno due elementi della documentazione tecnica sono stati verificati con esito positivo;

c. “non superata” qualora il collaudo ha avuto esito negativo o la documentazione tecnica risulti incompleta.

Il Titolare d’impianto deve quindi attendere la comunicazione di Terna in merito all’esito del collaudo. A valle della comunicazione dell’esito positivo del collaudo, Terna pone in esercizio il collegamento dati. In caso di certificazione superata con riserva/non superata, il Titolare d’impianto è tenuto a fornire tempestivamente la documentazione completa. Una volta verificata la completezza della documentazione tecnica e la corrispondenza ai requisiti tecnici di cui al presente paragrafo, Terna pone in esercizio del collegamento dati.

~~7~~8 Cyber Security

~~7.1~~ Le prescrizioni del presente paragrafo si applicano a tutte le tipologie di impianti elencate nel paragrafo 2 del presente Allegato. Il Titolare dell’impianto è tenuto a rispettare tali prescrizioni nella definizione e gestione dell’infrastruttura che va dall’impianto fino al punto di accesso di Terna.

~~7.1~~8.1 Politiche di Sicurezza

~~La~~Le politiche di sicurezza consistono nell’insieme di regole e configurazioni necessarie per garantire la confidenzialità, l'integrità e la disponibilità delle informazioni e dei servizi informativi a supporto dell’impianto.

Nei successi paragrafi sono definite le linee guida implementative che il Titolare dell’impianto deve seguire per la progettazione, la validazione, la realizzazione e l’esercizio di soluzioni tecnologiche di cui al presente Allegato. Tali linee guida riguardano principalmente:

- Asset Inventory ed Elenco Terze Parti;
- Monitoraggio di Cyber Security e gestione degli incidenti;
- Protezione da malware e isolamento del Traffico;
- Autenticazione e Autorizzazione;
- Sicurezza delle comunicazioni e crittografia;
- Filtraggio dei Pacchetti;
- Aggiornamenti e Patching;

- Logging;
- Backup e Ripristino.

8.1.1 Asset Inventory ed Elenco Terze Parti

Il Titolare dell'impianto deve mantenere aggiornati e deve rendere consultabili a Terna gli inventari degli asset digitali attestati sull'infrastruttura di scambio con Terna relativi a dispositivi (IT, IoT, OT e mobili) hardware e software, nonché l'elenco dei flussi di comunicazione ed eventualmente, su richiesta motivata di Terna, gli inventari degli ulteriori asset utilizzati per le finalità del presente Allegato.

8.1.2 Monitoraggio di Cyber Security e gestione degli incidenti

Il Titolare dell'impianto deve garantire la protezione ed il monitoraggio ~~delle comunicazioni per prevenire e~~di sicurezza sulla propria infrastruttura e sui propri sistemi, per rilevare accessi non autorizzati ai canali di comunicazione con Terna~~, provenienti sia da Internet che~~ da host residenti nelle proprie reti cablate e wireless ~~è in carico al soggetto Responsabile individuato come:~~e/o compromissione dei propri dispositivi (IT, OT, IoT e mobili).

- ~~per gli impianti di produzione connessi alla rete elettrica rilevante: Titolare di impianto (cap.5) ;~~
- ~~per gli impianti di produzione connessi in MT: il Distributore.~~

In particolare, il ~~Responsabile~~Titolare dell'impianto deve:

- preventivamente comunicare a Terna i riferimenti del proprio punto di contatto, con disponibilità H24 in tutti i giorni dell'anno, da contattare per la risoluzione di incidenti di sicurezza nel canale di comunicazione che richiedono interventi sul proprio lato;
- garantire e monitorare, sulla propria rete, l'integrità e la disponibilità delle informazioni scambiate con Terna garantendone al contempo la riservatezza;
- ~~mantenere logicamente segregate reti informatiche e canali di comunicazione destinati allo scambio di dati con Terna;~~
- notificare tempestivamente, e comunque non oltre le 4 ore dal rilevamento dell'evento, a Terna (cert@terna.it) gli ~~incidenti~~eventi di sicurezza che ~~interessano le comunicazioni con Terna~~ possano interessare:
  - i dispositivi (IT, IoT, OT e mobili) connessi alla Rete;

- l'infrastruttura di comunicazione tra i propri sistemi e Terna;
- le informazioni riguardanti l'interconnessione e in generale documentazione inerente a Terna (configurazioni, contratti, etc);
- eventuali eventi occorsi alla propria catena di fornitura (ad es. fornitori di servizi), afferente all'interconnessione con la RTN ed i sistemi di Terna.

- collaborare con ~~la stessa~~Terna nelle attività di contenimento, risposta e risoluzione~~.~~ degli incidenti di sicurezza.

~~Al fine di rendere sicuro il colloquio tra i Front-End dei sistemi Terna e gli apparati RTU/CCI dei singoli impianti, o il concentratore-gateway di più impianti, Terna impone l'utilizzo di connessioni Virtual Private Network (VPN), per tutti gli impianti di acquisizione che sfruttano la rete intranet.~~

~~La VPN dovrà essere instaurata tra un concentratore VPN, posizionato all'interno della rete Terna, e un terminatore VPN presente presso la rete del Titolare qualora il collegamento tra le sedi sia realizzato mediante collegamento di tipo shared (es. MPLS, Satellite, intranet), si veda Figura 8.~~

~~Per il terminatore VPN non è necessario un indirizzo pubblico statico, ma dovrà essere in grado di segregare la rete in cui sono presenti gli apparati di rete degli impianti (RTU).~~

~~Lo standard utilizzato per la creazione della VPN sarà IPSec.~~

~~La soluzione deve generare i log di sicurezza, contenente il time stamp sincronizzato, con il livello di dettaglio stabilito.~~

8.1.3 Protezione da malware e isolamento del Traffico

Il Titolare dell'impianto deve garantire la presenza di soluzioni anti malware aggiornate sui dispositivi (IT, OT, IoT e mobili) dei propri impianti, in grado di prevenire la compromissione degli stessi e la propagazione delle minacce Cyber.

Le infrastrutture di sicurezza del Titolare dell'impianto devono garantire un adeguato isolamento del traffico tra diverse VPN, laddove previsto all'interno della rete MPLS. Ciò implica l'implementazione di meccanismi di separazione, che impediscono al traffico di una

VPN di essere visibile o accessibile da un'altra, e di segregazione logica di reti informatiche e canali di comunicazione destinati allo scambio di dati con Terna.

8.1.4 Autenticazione e Autorizzazione

Il Titolare dell'impianto deve implementare tecnologie e procedure di autenticazione per garantire che solo i dispositivi e gli utenti autorizzati possano accedere alla rete. L'autorizzazione deve essere configurata in modo da limitare l'accesso alle risorse solo a chi ne ha il diritto. La configurazione della soluzione deve garantire che le credenziali di accesso ai dispositivi di gestione della rete siano robuste (es. MFA).

8.1.5 Sicurezza delle comunicazioni e crittografia

Il Titolare dell'impianto deve prevedere l'utilizzo di meccanismi di sicurezza delle comunicazioni per proteggere il traffico che attraversa la rete dati e predisporsi allo standard IEC-62351, cosiddetto IEC104 sicuro come indicato nel paragrafo 5.3.6.

Il Titolare dell'impianto deve adottare soluzioni crittografiche in linea con quelle previste dalle Linee Guida sulla crittografia e sulla conservazione delle *password* adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali[1].

8.1.6 Filtraggio dei Pacchetti

Il Titolare dell'impianto deve prevedere soluzioni di sicurezza perimetrale (es. Firewall) per proteggere le proprie infrastrutture ed implementare policy di sicurezza su indicazione di Terna, per la protezione dei flussi di traffico dati da e verso le infrastrutture Terna.

8.1.7 Aggiornamenti e Patching

È necessario mantenere aggiornati tutti i dispositivi (IT, OT, NETWORK e CYBER) applicando regolarmente, e almeno con cadenza semestrale, patch di sicurezza per correggere vulnerabilità note.

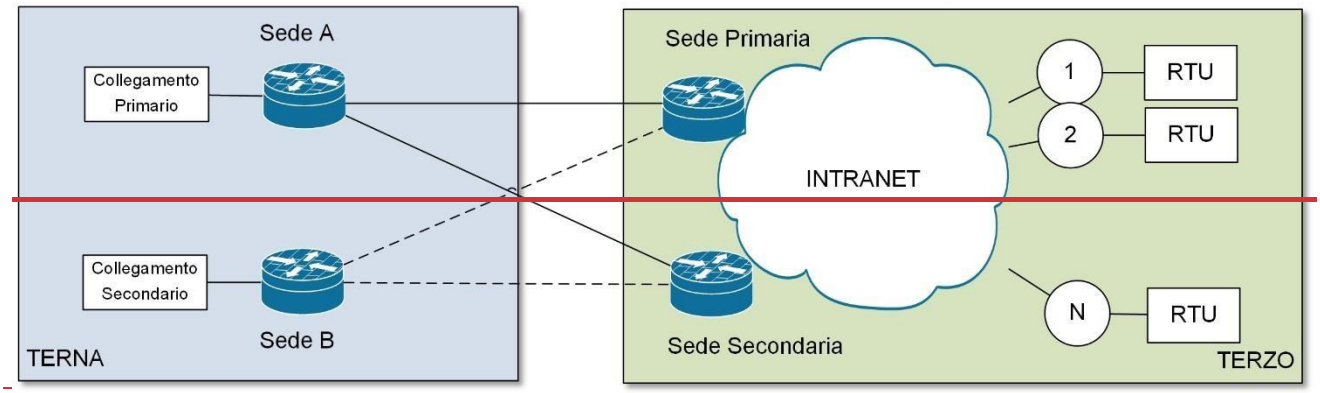
8.1.8 Logging

Ove necessario e su richiesta di Terna, il ~~Responsabile~~Titolare dell'impianto deve rendere disponibili i log di sicurezza secondo modalità standard (ad es. syslog, report, flat file) al

[1] https://www.acn.gov.it/portale/crittografia

CERT (cert@terna.it) di Terna. Il periodo di retention dei log che il Titolare dell'impianto deve garantire è almeno 6 mesi.

~~Inoltre, si precisa che Terna richiede idonee misure di sicurezza che garantiscano mutua autenticazione tra Titolare e Terna.~~



~~*Figura 8 – Connessioni*~~

8.1.9 Backup e Ripristino

Devono essere implementate procedure regolari di backup e ripristino per garantire la continuità operativa in caso di attacco o malfunzionamento del sistema. Il Titolare dell'impianto dovrà attuare e garantire tempistiche di RTO (Recovery Time Objective) e RPO (Recovery Point Objective) del sistema non superiori a 4 ore.

~~7.2~~8.2 ~~7.2 Conformità~~ Verifiche di conformità alle Politiche di Sicurezza

Il ~~Responsabile~~Titolare dell'impianto deve esibire ~~a~~, su richiesta di Terna, apposita documentazione tecnica che certifica la conformità delle soluzioni adottate~~.~~ sulla base di quanto indicato al paragrafo precedente.

~~7.3 Verifiche di conformità~~

Il Titolare dell'impianto deve consentire l'accesso all'impianto al personale di Terna (o Terze Parti da questa delegate) per eseguire verifiche di conformità delle soluzioni implementate nei confronti delle Politiche di Sicurezza e delle prescrizioni del presente documento.

~~**7.4 Segnalazione degli incidenti di sicurezza**~~

~~Il Responsabile deve inoltre comunicare tempestivamente al referente della Sicurezza Terna eventuali violazioni nel canale di comunicazione con Terna.~~

~~**7.5 Gestione degli incidenti di sicurezza**~~

~~Il Responsabile deve comunicare a Terna i riferimenti del proprio punto di contatto, da ingaggiare per la risoluzione di incidenti di sicurezza nel canale di comunicazione che richiedono interventi sul proprio lato.~~

~~7.6~~ Il Titolare dell'Impianto è tenuto all'esecuzione periodica di Cyber Security Assessment sulla propria infrastruttura e a dare evidenza dei rapporti di Assessment a Terna, ove richiesto.

~~7.3~~8.3 Tutela della sicurezza dei sistemi Terna

Terna si riserva il diritto di bloccare il flusso informativo con le RTU/CCI o con il concentratore gateway del Titolare dell'impianto, dandone informazione allo stesso, qualora rilevasse la presenza di minacce ~~contro~~Cyber verso i propri sistemi veicolate sul relativo canale di comunicazione~~.~~ o venisse a conoscenza di gravi incidenti di sicurezza nell'ambito della rete e delle infrastrutture del Titolare dell'impianto.