

*Ministero dell'Istruzione e del Merito***A041 – ESAME DI STATO CONCLUSIVO DEL SECONDO CICLO DI ISTRUZIONE**

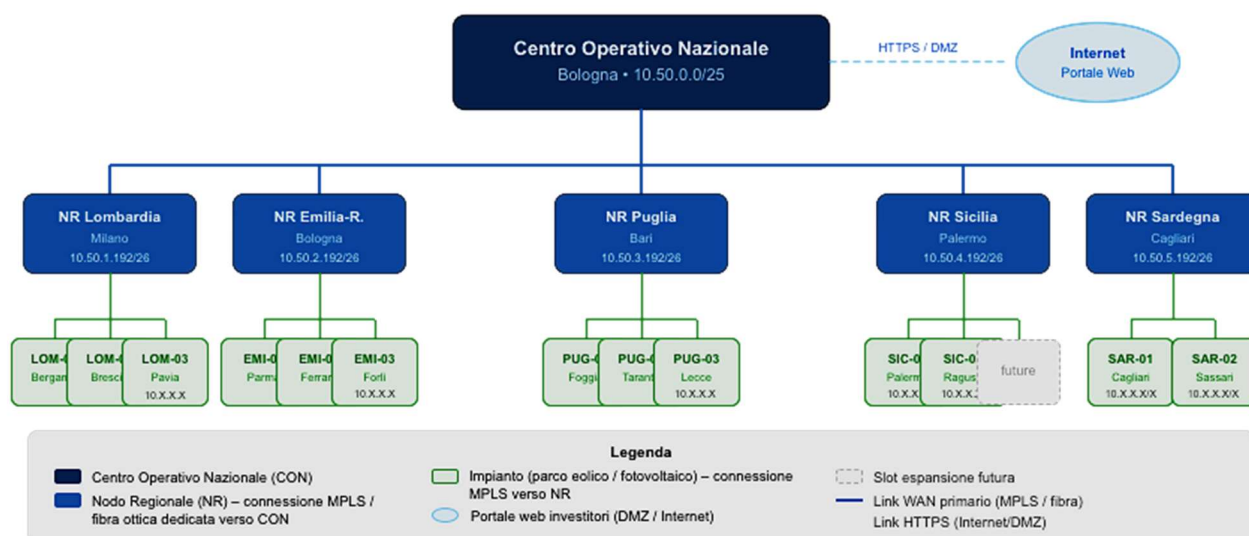
Indirizzo: ITIS - INFORMATICA E TELECOMUNICAZIONI ARTICOLAZIONE "INFORMATICA"

Disciplina: SISTEMI E RETI*Il candidato svolga la prima parte della prova e due tra i quesiti proposti nella seconda parte.***PRIMA PARTE**

GreenWave S.p.A. è una società italiana leader nella produzione di energia rinnovabile, con sede centrale a Bologna. L'azienda gestisce attualmente 15 impianti di produzione – tra parchi eolici e centrali fotovoltaiche – distribuiti in cinque regioni italiane (Lombardia, Emilia-Romagna, Puglia, Sicilia e Sardegna). Ogni impianto è dotato di sensori IoT, PLC (Programmable Logic Controller) e sistemi SCADA locali per il monitoraggio e il controllo della produzione.

In ciascuna regione è presente un Nodo Regionale (NR) che aggrega i dati di tutti gli impianti della propria area geografica prima di trasmetterli al Centro Operativo Nazionale (CON) situato presso la sede di Bologna. Il CON è il cuore del sistema: riceve in tempo reale i dati di produzione da tutti gli impianti, coordina le manovre di emergenza, genera reportistica per gli investitori e interagisce con i gestori delle reti elettriche nazionali (es. Terna S.p.A.).

Lo schema seguente illustra la struttura gerarchica della rete di GreenWave S.p.A.:

Schema infrastruttura GreenNet – GreenWave S.p.A.

GreenWave S.p.A. intende ora ammodernare e centralizzare l'intera infrastruttura IT, sostituendo le connessioni eterogenee attualmente in uso (ADSL, 4G, fibra locale) con una rete privata unificata, sicura e ad alta disponibilità. Il nuovo progetto, denominato internamente "*GreenNet*", prevede l'adozione di un piano di indirizzamento IP coerente e scalabile per tutti i siti.

Ai fini del piano di indirizzamento, GreenWave S.p.A. utilizzerà la rete privata 10.50.0.0/16. Per ogni impianto sono necessari almeno 20 indirizzi IP (sensori, PLC, switch gestiti, access point, server locale). I Nodi Regionali necessitano ciascuno di almeno 50 indirizzi IP. Il Centro Operativo Nazionale richiede almeno 120 indirizzi IP.

Ogni impianto deve poter comunicare esclusivamente con il proprio Nodo Regionale di riferimento; i Nodi Regionali comunicano esclusivamente con il CON. Nessun impianto deve avere accesso diretto agli impianti di un'altra regione o al CON.

Il CON ospita inoltre un portale web dedicato agli investitori istituzionali, accessibile tramite Internet, che mostra in tempo reale i dati aggregati di produzione energetica (senza esporre i dati operativi interni).

Il candidato, fatte le opportune ipotesi aggiuntive:

1. Sviluppi un piano di indirizzamento IP completo per la rete GreenNet, specificando: la subnet assegnata a ciascun impianto (indicando un esempio rappresentativo per ogni regione), le subnet dei cinque Nodi Regionali, la subnet del Centro Operativo Nazionale. Motivi le scelte di subnetting adottate e verifichi la compatibilità con i requisiti dimensionali indicati nel testo.
2. Illustri il progetto dell'infrastruttura di rete necessaria per realizzare GreenNet, dettagliando:
 - a. la tipologia e le caratteristiche dei dispositivi di rete presenti in ciascun impianto, nel Nodo Regionale e nel Centro Operativo Nazionale;
 - b. le tecnologie di connessione (link fisico/logico) tra gli impianti e il rispettivo Nodo Regionale, e tra i Nodi Regionali e il CON, motivando le scelte in base alle caratteristiche geografiche e ai requisiti di affidabilità;
 - c. la configurazione e l'architettura del CON, con particolare riferimento all'organizzazione della DMZ necessaria per ospitare il portale web degli investitori, sviluppando e discutendo almeno due soluzioni alternative (una completamente on-premise e una ibrida con servizi cloud), scegliendo motivatamente quella ritenuta più adeguata.
3. Approfondisca gli aspetti legati alla sicurezza della rete GreenNet, con particolare attenzione alla protezione della rete SCADA* (infrastruttura critica), alla cifratura delle comunicazioni tra impianti e CON, alle politiche di autenticazione e controllo degli accessi per gli operatori del CON e per gli utenti del portale web investitori. Discuta inoltre le misure di *business continuity* e *fault tolerance* ritenute necessarie per garantire la continuità del monitoraggio degli impianti.

SECONDA PARTE

- I. In relazione al tema proposto nella prima parte, si vuole permettere agli operatori del CON di consultare in tempo reale lo storico degli eventi registrati da ciascun impianto (allarmi, variazioni di produzione, manovre effettuate) e il stato attuale di ogni sensore. Il candidato progetti lo schema concettuale (E-R) e il modello logico relazionale della porzione di base

- di dati necessaria; realizzi poi la query SQL che restituisce, per un dato impianto, l'elenco di tutti gli allarmi attivati nelle ultime 24 ore ordinati per timestamp decrescente.
- II. In relazione al tema proposto nella prima parte, ogni impianto di GreenWave S.p.A. ospita dispositivi appartenenti a categorie funzionali distinte: apparati OT (PLC, sensori industriali), dispositivi IT (server SCADA locale, PC degli operatori) e apparati di gestione di rete (switch, access point). Il candidato illustri come la tecnologia VLAN (Virtual Local Area Network) possa essere utilizzata per segmentare logicamente la rete locale di un impianto, separando il traffico OT da quello IT e da quello di gestione. Il candidato descriva il funzionamento delle VLAN e dei trunk, proponga un piano di assegnazione delle VLAN per l'impianto e mostri un esempio di configurazione su uno switch con almeno tre VLAN, specificando le porte in modalità access e trunk e le motivazioni delle scelte adottate.
- III. Il portale web degli investitori di GreenWave S.p.A. riceve un numero variabile di richieste durante la giornata, con picchi nelle ore di contrattazione dei mercati energetici. Il candidato illustri i principali protocolli e le tecnologie di rete che consentono di garantire alta disponibilità e scalabilità al portale (es. bilanciamento del carico, proxy, firewall), descrivendo per ciascuna il funzionamento e i vantaggi apportati nel contesto specifico.
- IV. Le comunicazioni tra gli impianti e il CON generano un flusso continuo di dati che deve essere protetto da intercettazioni e manomissioni. Il candidato descriva le principali minacce informatiche cui è esposta una rete SCADA (es. attacchi Man-in-the-Middle, replay attack**, accesso non autorizzato ai PLC) e proponga per ciascuna le contromisure tecnologiche specifiche, motivando le scelte in funzione del contesto di infrastruttura critica.

** Generalmente il termine SCADA può identificare un software, installato su personal computer o server, che permette la realizzazione, il funzionamento e la gestione di sistemi di supervisione, controllo e telecontrollo senza dover necessariamente scrivere codice attraverso linguaggi di programmazione. Normalmente i sistemi SCADA vengono impiegati all'interno delle centrali di controllo delle fabbriche, delle stazioni ferroviarie, degli aeroporti, degli acquedotti o dei grandi complessi di edifici, così come - per i sistemi più piccoli - in prossimità del processo da controllare.*

*** Il replay-attack è una forma di attacco informatico che ha come bersaglio reti informatiche allo scopo di impossessarsi di una credenziale di autenticazione comunicata da un host ad un altro, e riproporla successivamente simulando l'identità dell'emittente. In genere l'azione viene compiuta da un attaccante che s'interpone tra i due lati comunicanti.*

Durata massima della prova: 6 ore.

È consentito l'uso di manuali tecnici e di calcolatrici scientifiche o grafiche purché non siano dotate della capacità di elaborazione simbolica algebrica e non abbiano la disponibilità di connessione a Internet.

È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.

Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla consegna della traccia.