

POLITECNICO DI TORINO
ESAMI DI STATO PER L'ABILITAZIONE ALL'ESERCIZIO
DELLA PROFESSIONE DI INGEGNERE DELL'INFORMAZIONE IUNIOR

II Sessione 2015 - Sezione B
Settore dell'Informazione

PROVA PRATICA del 23 dicembre 2015

Il comune di un centro urbano vorrebbe un sistema in grado di monitorare i consumi dei propri edifici pubblici, circa 1000 (mille) con circa 50 (cinquanta) stanze ognuno, per tenere sotto controllo luce e riscaldamento monitorando costantemente nel tempo tali valori per eventualmente limitare i consumi e per rilevare eventualmente guasti. Gli edifici sono dislocati in punti diversi della città non necessariamente limitrofi. Si vuole che tali dati vengano censiti e mantenuti all'interno di un Sistema Informativo centrale che funzioni da cruscotto per il monitoraggio degli edifici controllati. Tali dati recuperati dai vari edifici ogni 2 minuti dovranno essere rappresentati in un grafico che mostri l'andamento del tempo. Il S.I. dovrà permettere l'accesso al solo personale autorizzato e dovrà segnalare variazioni anomale che possono essere dovute a dei carichi di tensione improvvisi o al malfunzionamento degli apparati. Il S.I. dovrà fornire report settimanali via email al personale autorizzato e fornire avvisi immediati anche via SMS.

Gli edifici, non necessariamente cablati, dovranno prevedere l'installazione di apparati atti a tale scopo e che forniscono la sicurezza delle informazioni trasmesse al S.I. centrale cercando di evitare manomissioni da parte di personale non autorizzato e confidenza sul dato trasmesso.

Si richiede che il candidato nel progetto:

1. esprima e motivi ipotesi aggiuntive sulle caratteristiche del S.I. ritenute utili per soddisfare i requisiti generali espressi e per garantirne affidabilità, qualità, facilità d'uso, accessibilità, economicità e facilità di gestione;
2. elenchi e dettagli, tramite diagrammi UML, le funzionalità del sistema, i principali processi e i principali archivi.
3. definisca tramite diagrammi UML i macro-blocchi del S.I. e di Telecomunicazione nelle diverse componenti centrali e/o distribuite;
4. definisca e descriva sinteticamente le misure adottate per la sicurezza, la difesa della privacy, la business continuity, il disaster recovery e la difesa da eventuali truffe;
5. individui eventuali sovraccarichi del S.I. ed indichi misure atte a prevenirli e/o a risolverli.