UNIVERSITÀ DEGLI STUDI DI BRESCIA

ESAME DI STATO DI ABILITAZIONE ALL'ESERCIZIO DELLA PROFESSIONE DI INGEGNERE
(Lauree Specialistiche D.M. 509/99 - Lauree Magistrali D.M. 270/04 - Lauree Vecchio Ordinamento)

SEZIONE A - Prima sessione 2016

PRIMA PROVA SCRITTA DEL 15 GIUGNO 2016

SETTORE DELL'INFORMAZIONE

Tema n. 1:

Nell'ambito della realizzazione di sistemi per l'acquisizione, l'elaborazione e la trasmissione dell'informazione, il candidato descriva in modo approfondito le tecnologie e metodologie elettroniche, informatiche e di telecomunicazioni che possono essere utilizzate, facendo riferimento a una delle seguenti tematiche:

- Aspetti e problematiche nell'utilizzo di circuiti elettronici in ambienti caratterizzati da elevati disturbi elettrici.
- Principi di trasduzione di grandezze elettriche e sensori utilizzati per applicazioni di Smart Grid.
- Definizione delle tipologie di sistemi elettronici digitali per l'elaborazione numerica dei segnali ed analisi delle principali problematiche tecniche nel loro utilizzo.

Tema n. 2:

Nell'ambito della realizzazione di sistemi per l'acquisizione, l'elaborazione e la trasmissione dell'informazione, il candidato descriva in modo approfondito le tecnologie e metodologie elettroniche, informatiche e di telecomunicazioni che possono essere utilizzate, facendo riferimento a una delle seguenti tematiche:

- Algoritmi e metodi di compressione e/o trasmissione di segnali per applicazioni che richiedono prestazioni elevate (e.g. video streaming on demand offerto da Netflix).
- Infrastrutture di reti CDN (Content Distribution Networks) per la distribuzione di contenuti.
- Tecniche per l'elaborazione e l'analisi semantica di documenti multimediali (testi, immagini, video).

Tema n. 3:

Nell'ambito della realizzazione di sistemi per l'acquisizione, l'elaborazione e la trasmissione dell'informazione, il candidato descriva in modo approfondito le tecnologie e metodologie elettroniche, informatiche e di telecomunicazioni che possono essere utilizzate, facendo riferimento a una delle seguenti tematiche:

- Progettazione di applicazioni per dispositivi mobili.
- Estrazione di informazioni implicite da collezioni di dati strutturati.
- Progettazione di software, con particolare riferimento agli aspetti di interazione uomo macchina.

Tema n. 4:

Nell'ambito della realizzazione di sistemi per l'acquisizione, l'elaborazione e la trasmissione dell'informazione, il candidato descriva in modo approfondito le tecnologie e metodologie elettroniche, informatiche e di telecomunicazioni che possono essere utilizzate, facendo riferimento a una o più delle seguenti tematiche:

- Tecniche e metodi per la protezione dei sistemi informatici.
- Tecniche e metodi per la verifica dell'integrità dei dati nei sistemi telematici.
- Metodologie e algoritmi per la firma dei documenti elettronici.

UNIVERSITÀ DEGLI STUDI DI BRESCIA

ESAME DI STATO DI ABILITAZIONE ALL'ESERCIZIO DELLA PROFESSIONE DI INGEGNERE
(Lauree Specialistiche D.M. 509/99 - Lauree Magistrali D.M. 270/04 - Lauree Vecchio Ordinamento)

SEZIONE A - Prima sessione 2016

SECONDA PROVA SCRITTA DEL 29 GIUGNO 2016

SETTORE DELL'INFORMAZIONE

Classi di laurea appartenenti al settore:
LM/27 - Ingegneria delle telecomunicazioni;
LM/32 - Ingegneria informatica;
LM/29 - Ingegneria elettronica;
LM/66 - Sicurezza Informatica.

Tema n. 1 (classe LM/29 - Ingegneria elettronica):

Un'azienda attiva da decenni nel settore dell'home automation, vuole integrare il monitoraggio dei consumi elettrici ai suoi sistemi di controllo domestico. Si ricorda che il tipico contratto residenziale italiano è monofase, con tensione neutro-fase 230 V, frequenza nominale 50 Hz e potenza contrattuale di 3 kW, 4.5 kW o 6 kW. Tuttavia, il sistema dovrà poter essere commercializzato anche nel resto del continente (contratto residenziale tipicamente trifase). Il sistema deve poter essere facilmente modificabile per monitorare anche la potenza generata da eventuali impianti di produzione elettrica, quali impianti fotovoltaici, installati presso le abitazioni (potenza di picco pari a 3 kWp).
Il sistema è costituito da uno strumento di monitoraggio dell'energia elettrica da installare presso l'impianto dell'utente, da un dispositivo di raccolta delle informazioni di consumo e di produzione elettrica (di seguito chiamato gateway) e da un sistema informativo remoto per la raccolta e la presentazione dei dati raccolti dalle singole abitazioni.

Si chiede al candidato di immedesimarsi nel responsabile del progetto e:
1. Valutare quale tipologia di sensori, tra quelli disponibili in commercio, vanno utilizzati per la rilevazione della corrente. Le diverse tipologie dovranno tra di loro essere comparate, al fine di identificare chiaramente vantaggi e svantaggi di ognuna.
2. Valutare quale, tra i dispositivi per la misura dell'energia elettrica di cui sono stati forniti i datasheet in allegato, è indicato per l'applicazione (monitoraggio energia prodotta e consumata). Indicare chiaramente il modello e la configurazione, tra quelle proposte dal produttore, che meglio soddisfano i requisiti di progetto.
3. Indicare lo schema di inserzione dei misuratori di energia sulla rete elettrica (alimentazione del dispositivo e connessione alle fasi della rete elettrica).
4. Fornire uno schema a blocchi completo del sistema di monitoraggio dell'energia prodotta, dal sensore in campo (se necessario), fino al sistema informativo di raccolta dell'informazione. Evidenziare quali informazioni sono raccolte da ogni blocco (corredate da relativa unità di misura) e quali sono le operazioni di elaborazione effettuate.
5. Valutare la miglior soluzione tecnologica per la realizzazione del gateway per la raccolta delle informazioni dai dispositivi in campo. Si consideri che il sistema dovrà essere integrato anche ad altri sistemi di domotica che l'azienda già produce. I parametri da considerare sono il costo di produzione, la versatilità, i tempi ed il costo di sviluppo.

6. Proporre e descrivere il sistema di comunicazione (e il/i protocolli di comunicazione) utilizzato per connettere le diverse unità che compongono il sistema di monitoraggio. La scelta del sistema di comunicazione deve essere motivata e giustificata dalle specifiche del sistema di monitoraggio e dai vincoli di installazione presenti in ambiente domestico.
7. Descrivere l'interfaccia utente del sistema, fornendo anche una descrizione di quali devono essere i dati aggregati da fornire all'utente.
8. Valutare le strategie di implementazione del software del gateway per la raccolta delle informazioni dai dispositivi di misura dell'energia e la presentazione di queste informazioni al sistema di supervisione.

Tema n. 2 (Classe LM-66 – Sicurezza informatica):

Il comune di Pian Di Tavolo vuole realizzare un sistema informatico al servizio dei cittadini che permetta di accedere ai vari servizi erogati come richieste di certificati anagrafici, rinnovi carte d'identità, accesso ai dati relativi al conto rifiuti etc. Le credenziali di importanza crescente da usare a seconda del contesto sono costituite da username, password e un dispositivo OTP.

Il sistema deve garantire l'accesso agli utenti attraverso un web browser con tecnologie standard e previa autenticazione forte, e deve soddisfare requisiti di confidenzialità delle informazioni in transito tra il web server e il web client e confidenzialità dei dati degli utenti gestiti dal sistema informatico del comune.

Il candidato:

- tracci un piano di lavoro delineando le attività di progettazione richieste per la realizzazione del sistema informatico/telematico;
- specifichi quando le varie credenziali devono essere usate (es. quando username e password sono sufficienti, quando invece è necessario che l'utente inserisca il codice generato dall'OTP);
- specifichi l'architettura Hardware/Software del sistema lato comune, discutendo le tecnologie che dovranno essere utilizzate sul server (o sui server); specifichi anche le tecnologie da utilizzare lato utente; si considerino sia le tecnologie da utilizzare per l'autorizzazione e l'autenticazione degli utenti che le tecnologie per la confidenzialità dei dati in transito;
- indichi come e dove verranno mantenuti i dati degli utenti, sottolineando quali sottosistemi possono accedere a quali dati e come deve avvenire l'interazione tra i sottosistemi e il sistema di storage;
- discuta la sicurezza del sistema risultante, esaminando in particolare se la sicurezza dipende o meno dal comportamento degli utenti;
- determini infine se il sistema così progettato verifica la proprietà di non-repudiazione: nel caso non la verifichi introdurre un nuovo elemento alla catena di autenticazione che permetta di verificare questa proprietà.

Tema n. 3 (classe LM/27 - Ingegneria delle telecomunicazioni):

Il produttore di aereomobili Airbus vuole realizzare un aereo in grado di volare senza pilota, realizzando un sistema che permetta di comandare da remoto un'aereomobile A320 in caso di emergenza. Per valutare la fattibilità del progetto Airbus vuole acquisire i dati di volo dai display della cabina di pilotaggio mediante una telecamera montata su un supporto e collegata ad un tablet. I dati così acquisiti devono essere inviati dal tablet ogni 5 secondi ad una centrale operativa a terra attraverso il collegamento satellitare dell'aereomobile. Tra i display principali dell'A320, il *navigation display* si presenta idealmente come mostrato in Figura 1:

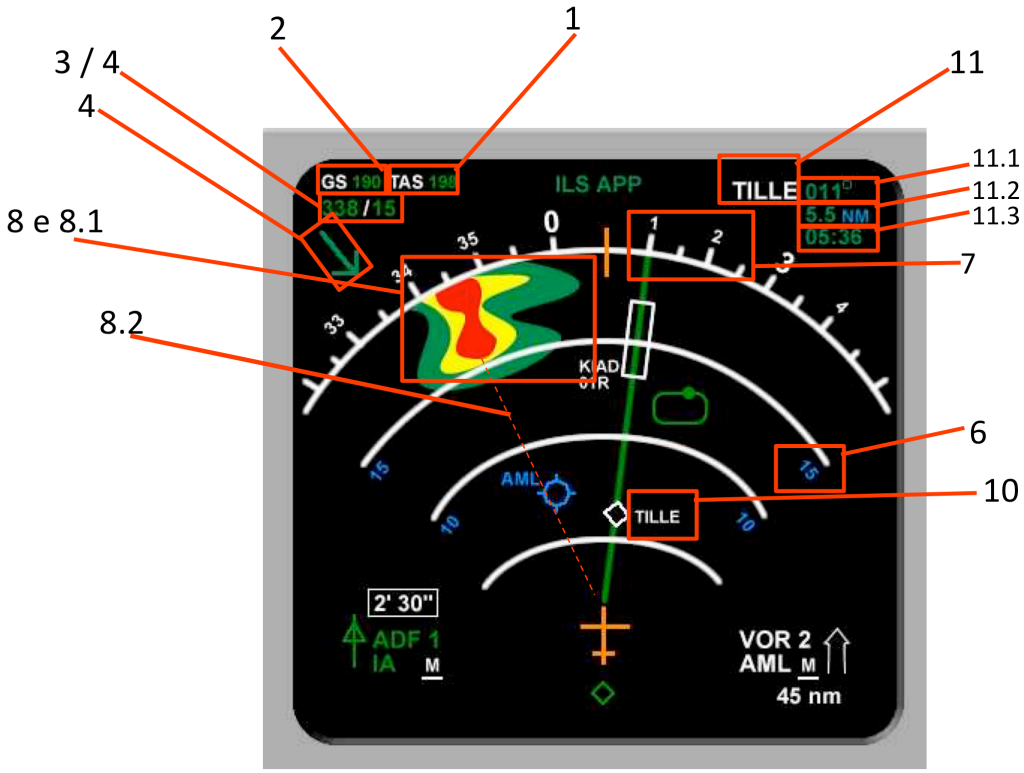

Figura 1: Rappresentazione del navigation display: al centro in basso l'aereomobile stilizzato (in arancio).

dove i vari elementi sono descritti come in Tabella seguente:

1	TAS (True AirSpeed)	Espressa in nodi (1 nodo = 1,852 Km/h), velocità in aria (rispetto al vento)
2	Ground Speed	Espressa in nodi (1 nodo = 1,852 Km/h), velocità rispetto al suolo
3/4	Direz. e velocità del vento	Espressa in nodi (1 nodo = 1,852 Km/h), velocità del vento
6	Distanza	Ogni arco ha associata la distanza in miglia nautiche (nm). L'arco più ampio è graduato.
7	Heading (direzione)	Direzione da seguire per arrivare al prossimo punto di passaggio (come 11.1). Va letta sull'arco di cerchio più ampio usando come riferimento le tacche (a 10° l'una dall'altra)
8	Turbolenza	Descritta da area e distanza. L'area dipende dalla scala usata (vedi Distanza)
8.1	Turbolenza	Il colore indica intensità crescente: Verde, Giallo, Rosso, Magenta
8.2	Distanza turbolenza	Si stima grazie agli archi di cerchio che indicano le distanze (in miglia nautiche, nm)
10	Punti di passaggio	Indicano dei riferimenti geografici al suolo. L'ultimo è la destinazione.
11	Prox punto di passaggio	Punto di passaggio presso il quale avviene il prossimo cambio di rotta (in Fig. "Tille")
11.1	Rotta da seguire	Rotta da seguire per arrivare al prox punto di passaggio che segnerà il prox cambio di rotta
11.2	Dist. dal prox punto di passaggio	Distanza in miglia dal punto di passaggio verso il quale ci si sta dirigendo (in Fig. "Tille")
11.3	Tempo stimato	Tempo in ore e minuti stimato prima del raggiungimento del prox punto di passaggio

Un'immagine del *navigation display* acquisita dalla telecamera si potrebbe presentare come in Figura 2:

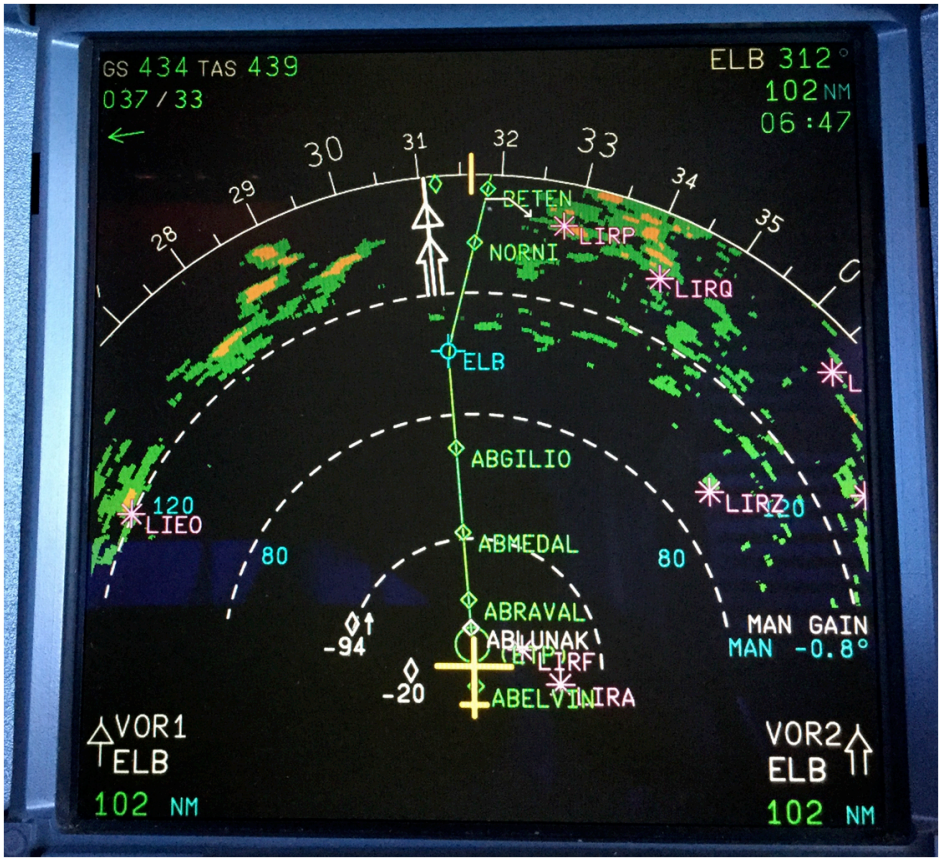

Figura 2: navigation display di un A320 inquadrato da una telecamera.

Il candidato disegni uno schema generale di come realizzerebbe il sistema di acquisizione ed invio dei dati utilizzando dei diagrammi a blocchi. Il candidato proponga in particolare delle strategie adeguate per risolvere il maggior numero possibile tra i seguenti problemi:

- **Calibrazione**: all'accensione della telecamera il sistema deve consentire all'operatore di effettuare una calibrazione per garantire che non siano intervenuti rilevanti spostamenti fisici della telecamera rispetto al display inquadrato;
- **Segmentazione**: dato che la telecamera inquadrerà una porzione più ampia della plancia, sarà necessario isolare il navigation display dagli altri elementi in cabina;
- **Correzione prospettica**: dato che la telecamera non sarà perfettamente in asse rispetto al display (come in Figura 2), sarà necessario correggere gli errori dovuti alla non perpendicolarità della ripresa;
- **Lettura indicatori alfanumerici**: gli elementi alfanumerici del display (ad esempio gli indicatori 1, 2, etc. in Tabella) dovranno essere acquisiti ed inviati alla centrale operativa a terra in forma testuale;
- **Acquisizione turbolenze**: le zone colorate relative alle turbolenze dovranno essere acquisite, codificate ed inviate in coordinate angolari al fine di permettere alla centrale operativa di ricostruirle a terra;
- **Codifica delle informazioni**: i dati alfanumerici e quelli relativi alle turbolenze dovranno essere codificati minimizzando i bit utilizzati per l'invio.

Opzionalmente si affrontino anche le seguenti problematiche:

- **Riflessi**: si discuta come risolvere il problema di eventuali riflessi dovuti alla luce solare che potrebbero inficiare la qualità delle immagini acquisite dal display;
- **Risorse HW**: si discuta su come risolvere i problemi dovuti alle limitate risorse hardware per effettuare l'elaborazione e la trasmissione dei dati nei tempi richiesti.

Tema n. 4 (classe LM/32 - Ingegneria informatica):

Si consideri un albergo situato nei pressi di alcune piste da sci aperte agli sciatori da maggio a novembre. In estate l'albergo diventa la meta di appassionati sciatori, interessati soprattutto ad avvalersi del supporto di una squadra di maestri di sci alle dipendenze dell'albergo. Attualmente i clienti dell'albergo possono prenotare le camere dell'albergo e le lezioni di sci tramite l'ausilio del telefono e/o email, e versare caparre tramite bonifico bancario. Le persone comunicano all'albergo il proprio periodo di soggiorno desiderato, il numero di persone di cui è costituito il proprio gruppo, le tipologie di camere desiderate, il maestro di sci di cui intendono avvalersi oppure, per ciascuna persona del gruppo, la sua capacità di sciare. Ogni maestro ha proprie disponibilità di orari, categorie di sciatori che è in grado di gestire (bronzo/argento/oro base/avanzato), massimo numero di sciatori di una certa categoria che può gestire contemporaneamente, compensi orari secondo la categoria e/o la numerosità del gruppo di sciatori. Si ipotizzi che l'albergo voglia dotarsi di un sistema informatico fruibile via internet per gestire (i) i maestri di sci e le camere dell'albergo, (ii) le prenotazioni e gli acquisti via internet. Le funzionalità del sistema includono: l'aggiunta, rimozione e la modifica dei dati relativi a stanze d'albergo, maestri di sci, disponibilità, clienti, e prenotazioni; la visualizzazione per i clienti delle disponibilità di camere d'albergo e di maestri di sci; la visualizzazione per i maestri di sci del programma giornaliero e settimanale – comprensivo dei nominativi e dei recapiti delle persone assegnate al maestro; la gestione delle camere d'albergo e dei pagamenti ai maestri.

Si richiede al candidato di:

- stilare schematicamente un piano di lavoro che specifichi le varie attività di progettazione richieste per la realizzazione del sistema informatico, quali competenze specifiche sono richieste da ciascuna di esse, ed in che ordine tali attività saranno svolte;
- definire in modo organizzato il modello concettuale della base dati sottostante, utilizzando schemi e diagrammi opportuni;
- specificare in modo dettagliato l'architettura HW/SW del sistema, sia per la memorizzazione e la corretta gestione di tutti i dati, sia per l'implementazione delle funzionalità richieste;
- descrivere l'interfaccia operativa delle procedure, o classi software, principali;
- evidenziare in modo esaustivo gli aspetti critici dal punto di vista dell'usabilità del sistema per l'utente, proponendo soluzioni specifiche per il problema presentato.

UNIVERSITÀ DEGLI STUDI DI BRESCIA

ESAME DI STATO DI ABILITAZIONE ALL'ESERCIZIO DELLA PROFESSIONE DI INGEGNERE
(Lauree Specialistiche D.M. 509/99 - Lauree Magistrali D.M. 270/04 - Lauree Vecchio Ordinamento)

SEZIONE A - Prima sessione 2016

PROVA PRATICA DI PROGETTAZIONE DEL 19 LUGLIO 2016

SETTORE DELL'INFORMAZIONE

Classi di laurea appartenenti al settore:
LM/27 - Ingegneria delle telecomunicazioni;
LM/32 - Ingegneria informatica;
LM/29 - Ingegneria elettronica;
LM/66 - Sicurezza Informatica.

Tema n. 1 (LM/32 - Ingegneria informatica)

Si supponga di voler progettare e sviluppare il sistema informatico (hardware/software) di una società per la navigazione del lago di "Nessudove". La società possiede porti presso le cittadine affacciate sul lago, biglietterie presso alcuni (non ognuno) dei porti, una flotta di motonavi operanti sul lago, ed una sede centrale con compiti sia amministrativi che operativi. Alle sue dipendenze ha capitani, marinai e impiegati presso le biglietterie e gli uffici della sede centrale. I compiti assegnati ai marinai includono la vendita e la vidimazione dei biglietti, i quali possono riferirsi sia a specifiche corse (ad es. il battello in partenza dalla città di Nessundove alle ore 8:00) che a tratte di navigazione (ad es. andata e ritorno da Nessundove a Qualchedove con eventuali cambi di motonavi) per più persone.
Gli utenti a cui il sistema informatico intende rivolgersi sono il personale amministrativo della Società, il personale operante presso le biglietterie, i capitani, i marinai, ed i clienti. Il sistema informatico dovrà consentire ai responsabili amministrativi:

- la definizione degli spostamenti stagionali delle motonavi, con la corrispondente definizione degli orari stagionali e la disponibilità di posti prenotabili nelle varie tratte;
- l'automatizzazione della contabilità e degli incassi con l'invio presso la sede centrale del fatturato dei biglietti emessi dalle biglietterie e dai marinai a bordo delle motonavi;
- la gestione dei turni di capitani e marinai.

Per la vidimazione dei biglietti a bordo delle motonavi la società intende dotare i mariani di opportuni dispositivi mobili. Il sistema informatico dovrà consentire ai marinai la vidimazione e l'emissione di biglietti, l'eventuale annullamento di biglietti emessi per errore, la visualizzazione dei biglietti emessi e dell'incasso, la trasmissione dell'incasso giornaliero. Il sistema informatico dovrà inoltre permettere ai clienti l'acquisto di biglietti via web, cosicché sarà possibile che i clienti si presentino presso le motonavi con un biglietto acquistato via web, un biglietto acquistato presso le biglietterie, oppure sprovvisti di biglietto con l'intenzione di acquistarlo a bordo delle motonavi. Il sistema informatico dovrà infine comunicare ai clienti eventuali ritardi delle motonavi operanti sul lago. Per questo compito la società intende dotare le motonavi di opportuni dispositivi per la georeferenziazione.
Si richiede al Candidato di:

(1) specificare *schematicamente* i requisiti funzionali e non funzionali del sistema informatico dettagliandoli opportunamente; il Candidato può quindi aggiungere nuovi requisiti e raffinare i requisiti dati sulla base della propria esperienza e di ragionevoli ipotesi;

(2) proporre un progetto di massima del sistema informatico e di telecomunicazioni complessivo da realizzare a livello di architettura software e hardware;

(3) specificare, attraverso opportuni linguaggi di modellazione grafici (ad esempio UML), i principali moduli di elaborazione dati;

(4) indicare *schematicamente* quali parametri utilizzare per stimare il costo di realizzazione del sistema informatico e di telecomunicazioni;

(5) approfondire gli aspetti del progetto che riguardano il disaster recovery, la sicurezza e la privacy, ed infine la robustezza e l'efficienza (tempo di risposta) del sistema anche considerando il caso di un'eccezionale afflusso turistico.

Tema n. 2 (LM/27 - Ingegneria delle telecomunicazioni)

La situazione politica nello stato di Flatlandia è molto instabile. Il dittatore Franco Poliedrik intende istallare un sistema di sorveglianza per le due camere del parlamento, quella alta e quella bassa, che monitori comportamenti e conversazioni dei parlamentari, ai fini di garantire un pronto intervento da parte della polizia in caso di disordini e/o tentativi di colpi di stato. A tale scopo dà incarico di realizzare, per ogni camera del parlamento, un sistema multitelecamera che impieghi n=5 videocamere ad alta definizione con risoluzione spaziale fullHD 1920x1080 [*pixel*] a 30 [*frame/sec*]. Lo schema di campionamento spaziale di tali telecamere è *Yuv 4:2:2* dove la componente di luminanza viene rappresentata con 12 [*bit/pixel*] mentre le crominanze sono rappresentate con 8 [*bit/pixel*]. Oltre ad acquisire il video, si vuole anche monitorare l'audio per identificare eventuali cospiratori e così svelare i loro piani. A tale scopo sono istallati m=12 microfoni per ogni camera del parlamento, i cui ingressi vengono campionati ad una frequenza f_c=44,1 [*KHz*] e quantizzati con 8 bit. I segnali audio e video multiplati vengono infine inviati alla centrale di polizia che si trova ad una distanza d=24 [*km*] mediante un ponte radio su n_T=6 tratte di uguale lunghezza l.

Il candidato affronti i seguenti punti:

1. Si disegni lo **schema a blocchi** dettagliato del sistema complessivo, scegliendo in modo adeguato la tecnologia trasmissiva da utilizzarsi e le **frequenze** di modulazione per la tratta in ponte radio, sapendo che essa utilizza uno schema di **modulazione QAM** ad impulsi a coseno rialzato;
2. Sapendo che i dati vengono trasmessi su tratte **rigenerative** le cui apparecchiature sono caratterizzate da una figura di rumore F=5, che si vuole tollerare una probabilità totale di fuori servizio pari a $P_{FS} = 10^{-3}$, calcolare la potenza P_T necessaria al fine di trasmettere con una probabilità di errore sul bit in ricezione $P_b(E) < 10^{-7}$ ed indicare l'occupazione di banda B_T;
3. Ripetere i calcoli al punto precedente nel caso di utilizzo di tratte **amplificative**, e discutere i risultati ottenuti;
4. Al fine di ridurre l'occupazione del segnale video, si proponga uno schema di **codifica intra-frame** con perdita a qualità costante con un *PSNR*=48 [*dB*], spiegando come si può derivare il rapporto di compressione ottenibile in funzione della distorsione introdotta;
5. Si discuta l'effetto causato dagli **errori** rispetto allo schema di codifica di sorgente utilizzato;
6. Si progetti uno schema di **codifica di canale** e di riorganizzazione del flusso dati che permetta di ridurre gli effetti evidenziati al punto precedente;
7. Calcolare la **capacità del canale** discreto che modella una modulazione M-QAM (scegliendo M limitato per semplificare il problema) su una singola tratta, e confrontarla con la capacità di un canale gaussiano che utilizzi la stessa potenza;
8. Proporre al dittatore di Flatlandia **uno schema e/o dei suggerimenti, non necessariamente tecnologici**, per meglio gestire e monitorare la situazione a Flatlandia con lo ultimo di ridurre la possibilità di disordini.

Tema n. 3 (classe LM/29 - Ingegneria elettronica):

Un'azienda operante da anni nel settore biomedicale vuole realizzare un sistema per la rilevazione della frequenza del battito cardiaco. Tale dispositivo dovrà rilevare il parametro fisiologico e rendere disponibile tale informazione all'utente. Il battito cardiaco è definito come il numero di volte che il cuore di un soggetto batte in un minuto ed è prodotto dalla depolarizzazione dei nodi sinoatriali e atrioventricolari. Un sistema di rilevazione del battito cardiaco è costituito da un elemento sensibile posizionato sul soggetto di cui monitorare il battito cardiaco, e da un sistema di acquisizione per il calcolo ed eventualmente la visualizzazione dell'informazione.
La fotopletismografia è una tecnica che permette di misurare i cambi di volume di alcune parti del corpo. Il cambio di volume della parte misurata (dV/dt) è legato al flusso sanguino (F) dalla seguente relazione F=k*dV/dt. La tecnica fotopletismografica può essere utilizzata per misurare la frequenza di battito cardiaco.
L'elemento sensibile può essere connesso al lobo dell'orecchio, alle dita delle mani o dei piedi, o in altre posizioni del corpo in funzione del principio di trasduzione (a riflessione o a trasmissione, rispettivamente mostrati in figura 1.a e figura 1.b).

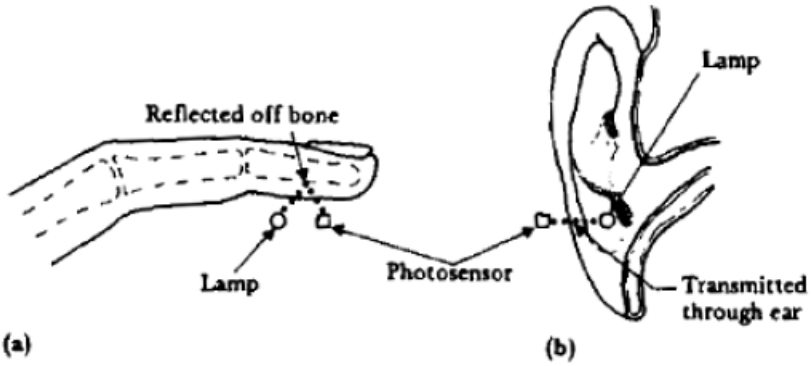

Figura 1: Confronto tra metodo di trasduzione fotoplestismografico a riflessione (a) e a trasmissione (b).

Il principio di funzionamento di un sensore PPG a riflessione è mostrato in figura 2.a. Esso è composto da una sorgente luminosa (tipicamente un led) che colpisce una parte del corpo del soggetto. Tale luce viene riflessa e viene ricevuto da un fototransistor, che trasforma il segnale luminoso in segnale elettrico (figura 2.b). Nel caso di un sensore PPG configurato in modalità a trasmissione, la luce, invece di essere riflessa, attraversa il tessuto del soggetto sotto esame (tipicamente in questo caso la misura si effettua sul lobo dell'orecchio). In entrambe le modalità, il segnale riflesso (o trasmesso) risulta modulato dalla variazione del volume della parte del corpo monitorata, legata alla variazione del flusso sanguigno dovuta al battito cardiaco. Tipicamente viene utilizzata una sorgente luminosa infrarossa perché tale lunghezza d'onda presenta la maggiore modulazione del segnale a causa dell'assorbimento della luce infrarossa dovuta all'emoglobina del sangue. L'uscita del fototransistor, sia nel caso di PPG a trasmissione che a riflessione, è caratterizzato da un segnale principale legato alla trasmittanza (definita come la frazione di luce che attraversa un campione in esame), modulato da un piccolo segnale dovuto alla pulsazione del sangue nel tessuto, che rappresenta la parte di segnale utile per l'applicazione.

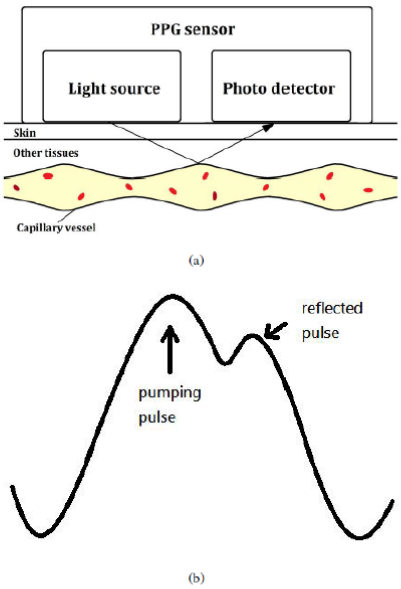

Figura 2: Meccanismo di funzionamento di un sensore PPG (a), ed esempio di un segnale fornito da un PPG a riflessione (b) dopo opportuna elaborazione.

Il responsabile dello progetto, dopo attenta analisi dei requisiti, ha selezionato il metodo fotopletismografico a trasmissione come possibile metodo di trasduzione del battito cardiaco. Il trasduttore verrà posizionato sul lobo dell'orecchio. Dopo attenta analisi del mercato, viene identificato come elemento sensibile da utilizzare per la trasduzione del battito cardiaco il sensore TCZT8020, prodotto dalla Vishay, di cui si allega il datasheet. Il prodotto è costituito da una coppia led emettitore/ fototransistor ricevitore, che possono essere utilizzati sia per realizzare sensori PPG a trasmissione che a riflessione. Il led emette alla frequenza di 950 nm, ovvero nella banda dell'infrarosso, come richiesto dall'applicazione. Inoltre, il package dei dispositivi è stato realizzato in modo da bloccare la luce nello spettro del visibile, e quindi di alterare il risultato della misurazione. In figura 3, viene riportato un esempio di segnale ottenuto dal sensore connesso al lobo di un soggetto sano, senza alcuno stadio di elaborazione, ed acquisto attraverso un oscilloscopio.

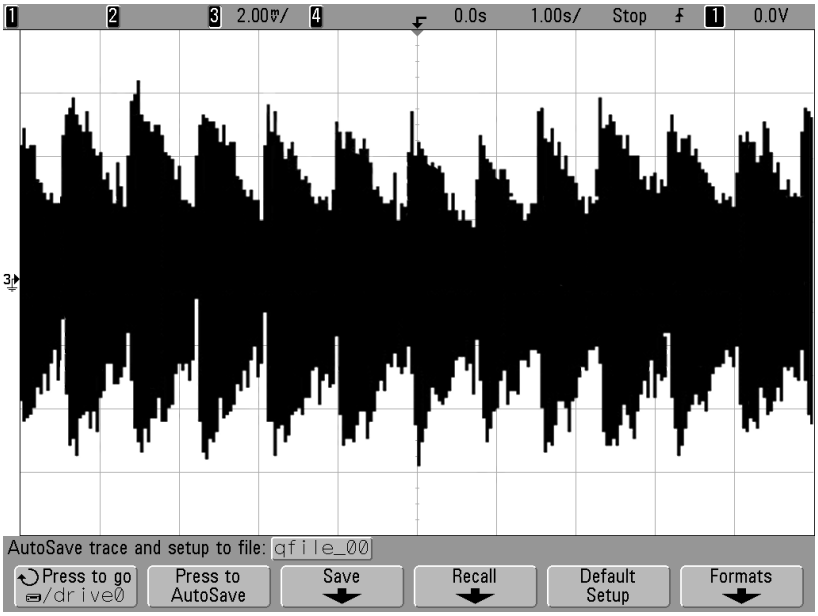

Figura 3: Segnale PPG a trasmissione acquisito da un oscilloscopio, prima dello stadio di elaborazione.

Il candidato dovrà effettuare la progettazione della scheda di interfaccia elettronica, per l'elaborazione, la trasmissione e la presentazione del dato di battito cardiaco. Il candidato, durante la fase di progettazione, dovrà tenere in considerazione, durante il dimensionamento del sistema, i vincoli di basso costo e basso consumo. Al candidato si chiede di:

(1) Fornire lo schema a blocchi del circuito di alimentazione, condizionamento, elaborazione, trasmissione e presentazione dell'informazione.

(2) Supponendo che la scheda venga alimentata attraverso un'alimentazione a 5 V non regolata, e sapendo che l'elettronica di condizionamento dovrà essere alimentata a 3.3 V, si progetti e dimensioni opportunamente lo stadio di regolazione e di alimentazione della scheda elettronica. Il candidato dovrà anche dimensionare opportunamente i condensatori di filtraggio delle alimentazioni.

(3) Fornire lo schema circuitale dei vari blocchi che compongono il sistema di condizionamento e alimentazione del sensore e dimensionare opportunamente i vari componenti (guadagno degli amplificatori, banda bassante dei filtri, corrente di alimentazione, eventuali condensatori e resistori), considerando che il tipico segnale fornito da un PPG a trasmissione è quello riportato in figura 3.

(4) Supponendo di utilizzare un convertitore ADC a 12 bit interfacciato attraverso una porta SPI ad processore della famiglia PIC18F Microchip ad 8 bit, entrambi alimentati a 3.3 V, si dimensioni opportunamente lo stadio di guadagno ed il filtro anti aliasing. Inoltre, il candidato fornisca un'analisi della risoluzione massima che può essere ottenuta con un tale sistema e quali possono essere le strategie per migliorare la risoluzione.

(5) Fornire il diagramma di flusso dell'algoritmo da sviluppare nel microprocessore per l'estrazione del battito cardiaco, utilizzando il segnale opportunamente condizionato.

(6) Fornire una possibile strategia per la realizzazione dell'interfaccia utente locale.

(7) Supponendo che la scheda da realizzare debba essere interfacciata ad un dispositivo per la raccolta dei dati, identificare la tecnologia di comunicazione più adatta alla trasmissione delle informazioni, tenendo conto dei vincoli di minimizzazione dei costi e del consumo, ma al tempo stesso garantisca la compatibilità con dispositivi commerciali

(8) Indicare le principali criticità nella realizzazione integrata di tale circuito

(9) Un sensore PPG è solitamente in grado di monitorare con buona approssimazione il battito cardiaco di un soggetto a riposo. Tuttavia, ogni movimento del sensore si traduce in un'ampia variazione della trasmittanza che è molto più ampia del segnale di misura utile. Questi artifizi, legati al movimento saturano gli amplificatori. Definire possibili strategie e proporre modifiche circuitali/o di elaborazione per compensare i disturbi introdotti dal movimento.

Tema n. 4 (Classe LM-66 – Sicurezza informatica):

Nel comune marino di Pian di Tavolo vivono circa 55.000 persone. La popolazione è molto giovane ed estremamente aperta all'utilizzo di nuove tecnologie. Circa l'80% della popolazione possiede uno SmartPhone moderno compatibile con il protocollo 802.11ac a due stream spaziali che viene usato per connettersi ai social network e per scaricare video on-demand. Il territorio comunale (visibile in Figure 1) è pianeggiante e la popolazione è uniformemente distribuita.

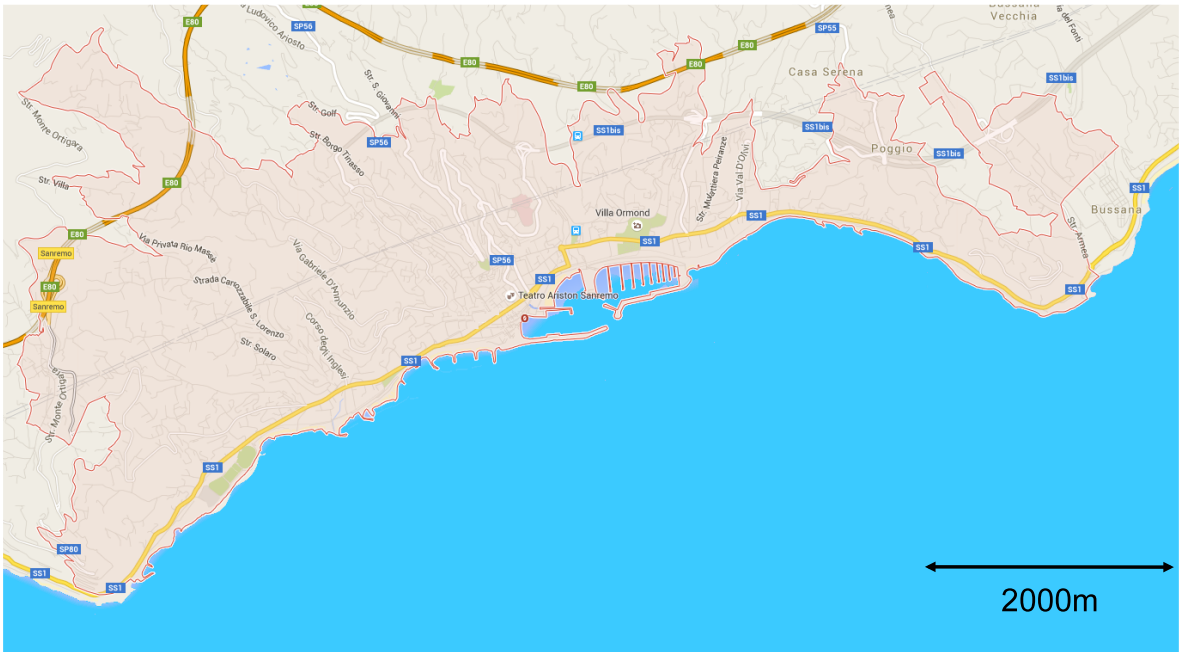

Figure 1 Mappa comunale

La giunta comunale decide di realizzare un progetto di copertura Wi-Fi cittadino che comprende l'acquisto di un certo numero di Access Point di class enterprise dotati di due radio nella banda 5GHz compatibili con lo standard 802.11ac e retrocompatibile con 802.11a. I canali ac vengono configurati a 40MHz per rendere più semplice la pianificazione delle frequenze.

Una rete in fibra ottica a 1Gb/s collega gli Access Point al provider a cui il comune fa riferimento: la sicurezza della rete di distribuzione è garantita dall'utilizzo del protocollo IPsec in azione tra ogni AP e i router del provider. L'autenticazione degli utenti alla rete è garantita attraverso WPA2-Enterprise con EAP-PEAP: gli utenti devono immettere username e password quando richiesto. La rete è autenticata dai terminali mobili mediante un certificato.

1. Si determini il throughput massimo nominale che ogni client è in grado di gestire in downlink e in uplink quando connesso ad un AP in modalità 11ac due stream;

2. Si ipotizzi (spiegando il ragionamento) un modello di connettività realistico (es. numero N di utenti attivi contemporaneamente con esigenza di throughput medio T – esprimere un valore per N e per T).

3. Si calcoli il numero di AP da acquisire e distribuire sul territorio comunale per soddisfare nei momenti di punta il 40% del throughput richiesto dai client in downlink (non si esprimono vincoli per il traffico in uplink).

4. Si determini sulla base del modello di connettività il massimo numero di autenticazioni al secondo che devono essere servite dal sistema: si consideri di non utilizzare alcun protocollo di trasferimento delle chiavi di sessione e di ri-autenticare ogni client in caso di roaming e ri-negoziare le chiavi ogni 3600 secondi;

5. Si valuti come terminare le sessioni IPsec tra gli AP e la sala macchine del provider considerando di utilizzare router enterprise con schede di accelerazione (si consideri un valore di 2Gb/s con IPsec 3DES a scheda);

6. Si dimensioni il front-end di autenticazione stabilendo il numero di server Radius da utilizzare considerando che ogni server (virtualizzato) è connesso all'infrastruttura della sala macchine attraverso un canale a 1Gb/s. Si valuti anche come costruire il back-end per lo storage delle password degli utenti: si abbia cura di non introdurre eventuali bottle-neck (e.g., si consideri che il server di back-end è connesso alla stessa infrastruttura con un canale a 1Gb/s);

7. Si determini come configurare il sistema di autenticazione in modo che non sia possibile che malintenzionati configurino Access Point con il medesimo beacon della rete del comune e ottengano gli username e password degli utenti: a questo proposito scegliere se il certificato per l'autenticazione della rete ai client

    - deve essere firmato da una Certification Authority (CA) costituita dal comune per questo scopo: in tal caso bisognerà distribuire il certificato Cert1 della CA ai client e configurare i client perché si fidino solo di server di autenticazione il cui certificato è stato firmato dalla chiave privata associata a Cert1;

    - può essere acquistato da una CA pubblica (ad esempio Verisign) il cui certificato è Cert2 e configurare i client perché si fidino solo di server di autenticazione il cui certificato è stato firmato dalla chiave privata associata a Cert2;

    Si giustifichi la scelta alla luce delle garanzie di sicurezza che questa comporta.

8. Si determini come autenticare gli AP all'infrastruttura (nel momento in cui stabiliscono la sessione IPsec con il/i router presso la sala macchine);

9. Si delinei una procedura standard da seguire per emettere una credenziale utente, la durata della sua validità, e si descrivano condizioni di allerta per cui la credenziale deve essere automaticamente sospesa.