



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 – Seconda sessione 2025

PRIMA PROVA SCRITTA DEL 14 NOVEMBRE 2025

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 e discuta criticamente (evidenziandone anche accuratamente i pregi e i difetti) le tecnologie e metodologie elettroniche, informatiche e di telecomunicazioni applicabili, facendo riferimento a una delle seguenti tematiche (si indichi chiaramente la tematica prescelta all'inizio dell'elaborato):

- problematiche e soluzioni dei sistemi di misura in ambienti con elevati disturbi elettrici;
- tecniche di elaborazione di segnali analogici;
- descrizione delle principali tecniche di progettazione e realizzazione di sensori MEMS e le principali applicazioni di tale tecnologia.

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 e discuta criticamente (evidenziandone anche accuratamente i pregi e i difetti) le tecnologie e metodologie elettroniche, informatiche e di telecomunicazioni applicabili, facendo riferimento a una delle seguenti tematiche (si indichi chiaramente la tematica prescelta all'inizio dell'elaborato):

- metodologie di progettazione del software, anche con riferimento all'automazione del ciclo di sviluppo, al testing continuo e alla gestione collaborativa dei team di lavoro;
- progettazione e sviluppo di applicazioni Web, anche data-intensive, con approfondimento sulla componente server-side e sulla gestione della persistenza dei dati;
- principi, tecniche e strumenti per la progettazione di sistemi di Business Intelligence, con riferimento ai processi di integrazione, analisi e trasformazione dei dati a supporto alle decisioni strategiche.

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 e discuta criticamente (evidenziandone anche accuratamente i pregi e i difetti) le tecnologie e metodologie elettroniche, informatiche e di telecomunicazioni applicabili, facendo riferimento a una delle seguenti tematiche (si indichi chiaramente la tematica prescelta all'inizio dell'elaborato):

- sistemi di comunicazione per il trasferimento di informazioni analogiche o numeriche in ambito industriale;
- protocolli di comunicazione su reti di calcolatori;
- tecniche di codifica dell'informazione e di dati multimediali.



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 – Seconda sessione 2025

SECONDA PROVA SCRITTA DEL 1° DICEMBRE 2025

SETTORE DELL'INFORMAZIONE

Tema n. 1 (valido per: classe LM/29 - Ingegneria Elettronica, classe LM/31 - Ingegneria Gestionale, classe LM/32 - Ingegneria Informatica)

Un'azienda attiva nel settore delle misure chimico-fisiche per analisi avanzate di superfici e processi in ambiente controllato, intende sviluppare una nuova camera a vuoto destinata alle attività di ricerca e sviluppo nei settori dei materiali avanzati e deposizione di film sottili.

La camera a vuoto dovrà essere in grado di monitorare in tempo reale i principali parametri fisici interni all'ambiente di misura mediante i seguenti sensori di cui sono indicate le specifiche:

- pressione interna compresa tra 10^{-6} mbar e 10^{-2} mbar,
- temperatura compresa tra -20 °C e $+200$ °C,
- massa degli analiti depositati rilevata con un opportuno sensore avente risoluzione inferiore al nanogrammo,
- flusso dei gas iniettati nella camera per i processi di reazione o deposizione compreso tra 0.1 sccm e 50 sccm ($1 \text{ sccm} = 1 \text{ cm}^3/\text{min}$).

La camera a vuoto è dotata di un sistema di misura dei parametri fisici interni e di un'unità di controllo esterna. Il sistema di misura dei parametri fisici interni è costituito dai circuiti dedicati al condizionamento dei segnali provenienti da ciascun sensore e da un'unità a microcontrollore e circuiti accessori, responsabili della loro conversione in formato digitale, dell'elaborazione e invio all'unità di controllo esterna. L'unità di controllo esterna è basata su un opportuno microcontrollore che in base ai dati ricevuti gestisce l'attuazione della pompa a vuoto, la regolazione delle valvole di flusso per l'immissione degli analiti e dell'aria nonché l'input dei parametri di processo da parte dell'utente e la memorizzazione (*logging*) dei dati sperimentali. L'unità di controllo esterna inoltre implementa un meccanismo di allerta in caso di condizioni anomale, quali:

- pressione superiore a 10^{-2} mbar,
- temperatura superiore a 200 °C o inferiore a -20 °C,
- flusso dei gas fuori dal range impostato dall'operatore,
- instabilità o saturazione del sensore di massa.

Con riferimento alla descrizione precedente, il candidato:

1. definisca la tipologia che ritiene più adatta, motivandone la scelta, dei sensori necessari al funzionamento della camera, tenendo in considerazione le specifiche di progetto riportate;

2. proponga uno schema circuitale generale ma completo del circuito che realizza il sistema di misura dei parametri fisici interni basato sulle scelte effettuate al punto precedente. Nello specifico si proponga per ciascun sensore individuato un opportuno circuito di condizionamento e le specifiche del corrispondente stadio di conversione analogico/digitale (quando necessario), descrivendo e motivando le scelte progettuali. Si specifichi inoltre come le grandezze convertite in digitale possono essere trasferite all'unità di controllo esterna;
3. proponga uno schema a blocchi dettagliato, completo e opportunamente commentato dell'unità di controllo esterna tenendo quindi in considerazione tutte le funzioni precedentemente specificate;
4. definisca quali strategie adottare al fine di realizzare un sistema automatico di rilevazione dei guasti dei sensori e degli attuatori camera a vuoto in modo da avvisare l'operatore che il sistema non è più in grado di funzionare correttamente;
5. definisca il diagramma di flusso completo del firmware del microcontrollore della unità di controllo esterna in base anche alle scelte precedentemente effettuate.

Tema n. 2 (valido per: classe LM/29 - Ingegneria Elettronica, classe LM/31 - Ingegneria Gestionale, classe LM/32 - Ingegneria Informatica)

La Rete Europea di Ricerca Agricola “AgriConnect Hub” è un consorzio internazionale composto da centri di ricerca, università, aziende agricole sperimentali, imprese biotech e istituzioni pubbliche. Il consorzio intende realizzare una piattaforma Web che supporti la gestione operativa dei progetti agricoli e ambientali, facilitando il coordinamento delle attività, la condivisione dei dati e la collaborazione tra le strutture coinvolte.

La piattaforma, accessibile via browser, consentirà a ricercatori, agronomi, tecnici e partner istituzionali di registrarsi e creare un profilo personale, includendo informazioni su competenze, ruolo e attività di ricerca. Ogni utente potrà controllare la visibilità del proprio profilo e aggiornare autonomamente i propri dati.

Gli utenti potranno proporre esperimenti e attività progettuali, sia in campo sia in laboratorio, definendo obiettivi, protocolli, risorse necessarie e tempistiche. Sarà inoltre possibile prenotare strumenti e attrezzature condivise, segnalare problemi sul campo e proporre interventi o modifiche operative. Ogni proposta includerà criteri di partecipazione e scadenze, in modo che altri membri possano aderire o ricevere aggiornamenti.

La piattaforma dovrà gestire diversi tipi di dati, come documenti tecnici, immagini, fogli di calcolo, brevi video, report di attività e dati provenienti da strumenti o applicazioni esterne. Dovrà essere garantita l'organizzazione, la memorizzazione e la consultazione di questi contenuti, supportando metadati minimi, strumenti di ricerca e meccanismi di controllo della qualità dei dati. La piattaforma dovrà assicurare adeguati livelli di protezione dell'accesso e rispetto della proprietà intellettuale dei materiali condivisi.

Lo staff autorizzato di AgriConnect Hub disporrà di un pannello di amministrazione per gestire utenti, moderare i contenuti, monitorare la qualità dei dati caricati, coordinare l'uso delle attrezzature condivise e pubblicare protocolli e linee guida operative. Potrà inoltre supervisionare eventuali finanziamenti e sponsorizzazioni associati ai progetti.

La piattaforma dovrà rispettare requisiti di sicurezza, protezione dei dati, accessibilità e scalabilità, adottando un'architettura modulare che consenta l'integrazione con database di ricerca, repository accademici, strumenti IoT o sistemi GIS utilizzati dai membri del consorzio.

Si richiede al candidato di:

1. Stilare un piano di lavoro che specifichi le varie attività di progettazione richieste per la realizzazione della piattaforma per questo particolare problema e per questi particolari requisiti, spiegando l'attinenza di ogni fase del piano ai requisiti sopra descritti, quali competenze specifiche sono richieste da ciascuna di esse, ed in che ordine tali attività saranno svolte, anche utilizzando appositi diagrammi.
2. Descrivere in modo dettagliato l'architettura hardware e software dell'intero sistema, evidenziando le componenti utilizzate per la memorizzazione e la gestione dei dati, nonché per l'implementazione delle funzionalità richieste.
3. Approfondire, tramite schemi e/o diagrammi debitamente commentati, il funzionamento di un sottosistema specifico a scelta tra: (i) gestione dei progetti e degli esperimenti; (ii) gestione dei contenuti e dei dati condivisi; (iii) gestione utenti, permessi e prenotazione risorse. Per il sottosistema selezionato, descrivere nel dettaglio i moduli software coinvolti nell'elaborazione e nell'archiviazione dei dati, le modalità di interazione tra i componenti interni ed eventuali sistemi esterni, il trattamento dei dati utente (se rilevante) e le tecnologie previste per la sua implementazione operativa.
4. Evidenziare gli aspetti critici legati alla gestione e integrazione dei dati provenienti da fonti eterogenee, analizzando le principali problematiche e proponendo soluzioni architetturali e tecniche che consentano di garantire coerenza, aggiornamento continuo e interoperabilità dei dati all'interno della piattaforma.

Tema n. 3 (valido per: classe LM/29 - Ingegneria Elettronica, classe LM/31 - Ingegneria Gestionale, classe LM/32 - Ingegneria Informatica)

TechSecure S.p.A. è un Global Systems Integrator e Managed Service Provider con sede principale in Italia e una presenza operativa che, nel corso degli anni, si è estesa anche a livello internazionale. L'azienda, che impiega circa 150 dipendenti, opera come fornitore di servizi IT gestiti ad elevata criticità per una clientela Business-to-Business (B2B). Le attività svolte comprendono la gestione di infrastrutture cloud ibride, l'erogazione di servizi di gestione della sicurezza e un supporto applicativo sviluppato su misura in base alle esigenze dei singoli clienti.

Il portafoglio clienti è particolarmente concentrato nel settore *finanziario*, caratterizzato dalla presenza di dati transazionali sensibili e da processi di identificazione e verifica della clientela (Know Your Customer) e *sanitario*, dove vengono trattati dati relativi alle cartelle cliniche elettroniche e informazioni personali sensibili. In questi contesti, la capacità dell'azienda di mantenere un rigoroso equilibrio tra qualità operativa e sicurezza delle informazioni rappresenta un elemento essenziale non solo per la continuità dei servizi, ma anche per la fiducia degli stakeholder e per la conformità ai requisiti normativi.

Nel corso degli ultimi tre anni, TechSecure S.p.A. ha sperimentato una crescita significativa, che ha comportato un incremento della complessità organizzativa e tecnica e, di conseguenza, l'emersione di alcune criticità:

- *Vulnerabilità alla sicurezza* - Un attacco ransomware, recentemente mitigato, ha messo in luce lacune nei protocolli di cybersecurity, oltre alla presenza di processi interni non documentati o applicati in modo non sistematico.
- *Problemi di qualità del servizio* - È stato registrato un aumento dei reclami relativi alla reattività del supporto tecnico e a una gestione del Change Management che, risultando inefficace, ha generato interruzioni non previste dei servizi.
- *Dipendenza da terze parti* - Circa il 30% delle operazioni cloud è affidato a provider di secondo livello e a sub-fornitori che garantiscono supporto sistemistico, ma il livello di controllo e governance su tali fornitori risulta insufficiente.
- *Esternalizzazione del SIEM* - La manutenzione del sistema di monitoraggio della sicurezza (Security Information and Event Management, SIEM) è esternalizzata al Sub-Fornitore X, che richiede accessi amministrativi e che può trattare dati personali dei clienti.

Consapevole della necessità di rafforzare la propria struttura interna, migliorare la coerenza e l'affidabilità dei processi operativi e consolidare la relazione con clienti e fornitori, la Direzione aziendale ha deciso di avviare l'implementazione di un Sistema di Gestione Integrato (SGI), che unisca in un unico quadro metodologico gli aspetti relativi alla qualità del servizio e alla sicurezza delle informazioni. La decisione nasce dall'esigenza di dare evidenza concreta dell'impegno dell'azienda nella protezione dei dati trattati e nella qualità delle prestazioni erogate, oltre che dalla volontà di adottare un modello più strutturato, orientato al miglioramento continuo.

Si richiede al candidato di approfondire e sviluppare i punti seguenti.

1. Identificare almeno quattro parti interessate interne e/o esterne rilevanti per il SGI, motivandone la scelta e definendo, per ciascuna di esse, almeno un requisito chiave che incida sia sulla qualità del servizio sia sulla sicurezza delle informazioni.
2. Individuare i principali rischi che TechSecure S.p.A. deve affrontare. Proporre un sistema di valutazione del rischio (metodologia, criteri di probabilità e impatto) e fornire una rappresentazione organizzata dei rischi individuati. Per ogni rischio, definire un piano di mitigazione operativo e organizzativo.
3. Analizzare i rischi e le opportunità connessi all'esternalizzazione delle attività aziendali. Proporre un sistema di indicatori per la valutazione delle prestazioni e della rischiosità dei fornitori, includendo Key Performance Indicators (KPI) e Key Risk Indicators (KRI), e individuare azioni tecniche e organizzative per ridurre i rischi derivanti dall'utilizzo di terze parti.
4. Progettare una roadmap operativa per l'implementazione dell'SGI, includendo le principali milestone, le tempistiche previste, i ruoli e le responsabilità coinvolte, nonché le attività di formazione e di comunicazione interna. Definire inoltre i criteri e i metodi necessari per la verifica, la certificazione o la validazione del sistema.



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 – Seconda sessione 2025

PROVA PRATICA DI PROGETTAZIONE DEL 15 DICEMBRE 2025

SETTORE DELL'INFORMAZIONE

Tema n. 1 (valido per: classe LM/29 - Ingegneria Elettronica, classe LM/31 - Ingegneria Gestionale, classe LM/32 - Ingegneria Informatica)

Un'azienda operante nel settore dei dispositivi indossabili intende realizzare un orologio da polso dotato di un sistema avanzato per la misura della frequenza del battito cardiaco tramite la tecnica della fotoplethysmografia (PPG). Il sensore PPG potrà essere integrato nel cinturino oppure sul fondo dell'orologio, in entrambi i casi a contatto con la pelle dell'utente. La frequenza del battito cardiaco è definita come il numero di contrazioni del cuore in un minuto, generate dalla depolarizzazione dei nodi sino-atriali e atrio-ventricolari. Il metodo fotoplethysmografico permette di misurare le variazioni del volume sanguigno in un tessuto collegato al flusso sanguigno. Nello specifico, il metodo fotoplethysmografico utilizza un sensore ottico costituito da un LED e un fotodiodo/fototransistor. Il LED illumina la pelle nella regione dell'infrarosso o del visibile, mentre il fotodiodo misura la luce riflessa o trasmessa attraverso il tessuto. Poiché il sangue assorbe più luce rispetto ai tessuti circostanti, l'intensità luminosa rilevata è modulata in funzione di ogni battito cardiaco. Il segnale PPG ottenuto è pertanto principalmente costituito da:

- una **componente continua** (DC), legata alla trasmittanza/assorbanza media del tessuto;
- una **componente variabile** (AC), più piccola ma direttamente correlata al battito cardiaco.

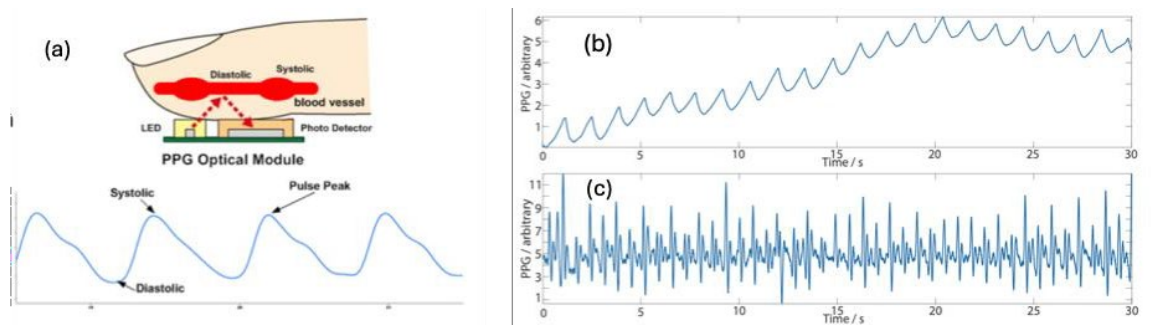


Figura 1 – Schema di funzionamento della fotoplethysmografia a riflessione con un tipico esempio di segnale nel caso di sensore posto in corrispondenza di un dito (a). Andamento tipico del segnale acquisito con il sensore posizionato sul polso quando il soggetto è a riposo (b) e durante una corsa (c).

Nell'applicazione in esame si utilizzerà il metodo fotoplethysmografico basato sulla luce riflessa, in quanto risulta di più facile implementazione. La Figura 1(a) mostra il principio di funzionamento corredato con una tipica forma

d'onda misurata nel caso in cui il sensore è posizionato in corrispondenza della punta del dito. Nel caso di sensore posizionato in corrispondenza del polso, si può assumere come andamento tipico per una persona a riposo quello di Figura 1(b), mentre la Figura 1(c) fa riferimento al tracciato di una persona durante una corsa. Dopo un'analisi dei dispositivi in commercio si è deciso di utilizzare come dispositivo ottico il modulo OSRAM SFH 7050 che contiene al suo interno un led infrarosso, un led rosso, un led verde e un rilevatore. Per il funzionamento di base del sistema si utilizzerà la sorgente infrarossa (IR) perché tale lunghezza d'onda presenta la maggiore modulazione del segnale a causa dell'assorbimento della luce infrarossa dovuta all'emoglobina del sangue. L'Allegato A riporta le principali caratteristiche della sorgente IR e del fotorivelatore.

L'azienda vuole sviluppare un sistema completo che includa:

- il sensore ottico PPG (LED + fotodiodo/fototransistor);
- l'elettronica per il condizionamento e acquisizione del segnale;
- il microcontrollore dell'orologio per l'elaborazione dell'informazione;
- il sistema di visualizzazione locale e di trasmissione wireless dei dati verso smartphone;
- il contenimento dei consumi e la miniaturizzazione necessaria a un dispositivo da polso.

Il Candidato dovrà effettuare la progettazione della scheda di interfaccia elettronica per il condizionamento, l'acquisizione e l'elaborazione 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. Pertanto, al Candidato si chiede di:

1. Fornire lo schema a blocchi del circuito di alimentazione, condizionamento ed elaborazione dei segnali.
2. Supponendo che la scheda venga alimentata attraverso una batteria Li-ion interna (tensione nominale 3.6 V), e sapendo che l'elettronica di condizionamento dovrà essere alimentata a 1.8 V, si progetti e dimensiona opportunamente lo stadio di regolazione e di alimentazione della scheda elettronica comprensiva dei 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 passante dei filtri, corrente di alimentazione, eventuali condensatori e resistori), considerando che il tipico segnale fornito da un PPG a riflessione è quello riportato in Figura 1(b).
4. Supponendo di utilizzare un convertitore ADC a 12 bit interfacciato attraverso una porta SPI a un a 32 bit, entrambi alimentati a 1.8 V, si dimensiona 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. Supponendo che l'orologio si debba interfacciare a uno smartphone in modalità non cablata, identificare la tecnologia di comunicazione più adatta alla trasmissione delle informazioni, tenendo conto dei vincoli di minimizzazione dei costi e del consumo.
7. 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. Definire possibili strategie e proporre modifiche circuitali e/o di elaborazione per compensare i disturbi introdotti dal movimento.

ALLEGATO A

CARATTERISTICHE DEL DIODO INFRAROSSO E DEL FOTODIODO OSRAM SFH 7050A

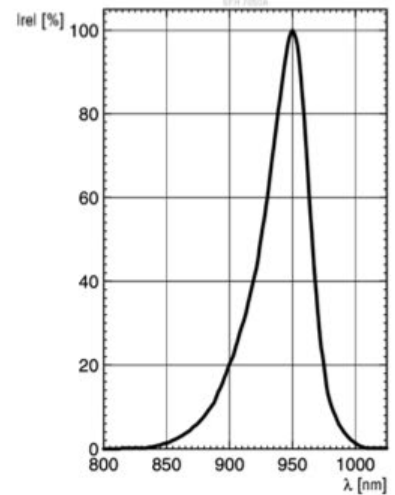
Characteristics

$T_A = 25^\circ\text{C}$

Parameter	Symbol	Values
Infrared Emitter		
Peak wavelength $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	λ_{peak}	typ. 950 nm
Centroid Wavelength ⁴⁾ $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	$\lambda_{\text{centroid}}$	min. 930 nm
		typ. 940 nm
		max. 950 nm
Spectral bandwidth at 50% $I_{\text{rel,max}}$ (FWHM) $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	$\Delta\lambda$	typ. 42 nm
Half angle	Φ	typ. $\pm 60^\circ$
Rise time (10%/ 90%) $I_F = 100\text{ mA}; R_L = 50\ \Omega$	t_r	typ. 16 ns
Fall time (10%/ 90%) $I_F = 100\text{ mA}; R_L = 50\ \Omega$	t_f	typ. 16 ns
Forward voltage ⁴⁾ $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	V_F	typ. 1.3 V
		max. 1.8 V
Reverse current $V_R = 5\text{ V}$	I_R	Not designed for reverse operation
Radiant intensity $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	I_e	typ. 2 mW / sr
Total radiant flux $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	Φ_e	typ. 5.3 mW
Temperature coefficient of brightness $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	TC_I	typ. $-0.3\ \% / \text{K}$
Temperature coefficient of wavelength $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	TC_λ	typ. $0.25\text{ nm} / \text{K}$
Temperature coefficient of voltage $I_F = 20\text{ mA}; t_p = 20\text{ ms}$	TC_V	typ. $-0.8\text{ mV} / \text{K}$
Thermal resistance junction ambient real	R_{thja}	max. 230 K/W

Relative Spectral Emission ^{1), 2)}

■ infrared (940 nm): $I_{e,rel} = f(\lambda); I_F = 20\text{ mA}; t_p = 20\text{ ms}$



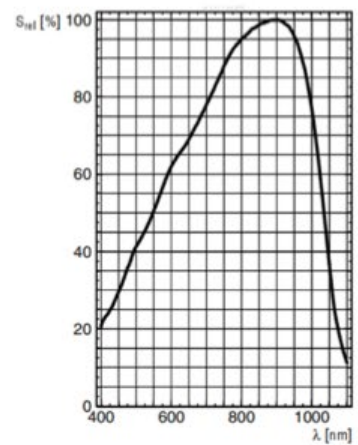
Characteristics

$T_A = 25^\circ\text{C}$

Parameter	Symbol	Values
Broadband Photodiode		
Wavelength of max. sensitivity	$\lambda_{S\text{max}}$	typ. 900 nm
Spectral range of sensitivity	$\lambda_{10\%}$	typ. 400 ... 1100 nm
Photocurrent $E_e = 0.1\text{ mW/cm}^2; \lambda = 530\text{ nm}; V_R = 5\text{ V}$	I_P	typ. 0.5 μA
Photocurrent $E_e = 0.1\text{ mW/cm}^2; \lambda = 655\text{ nm}; V_R = 5\text{ V}$	I_P	typ. 0.75 μA
Photocurrent $E_e = 0.1\text{ mW/cm}^2; \lambda = 940\text{ nm}; V_R = 5\text{ V}$	I_P	typ. 1.22 μA
Radiant sensitive area	A	typ. 1.51 mm ²
Dimensions of active chip area	$L \times W$	typ. 1.23 x 1.23 mm x mm
Dark current $V_R = 5\text{ V}; E = 0$	I_R	typ. 0.1 nA
		max. 25 nA
Spectral sensitivity of the chip $\lambda = 535\text{ nm}$	S_λ	typ. 0.34 A / W
Open-circuit voltage $E_e = 0.1\text{ mW/cm}^2; \lambda = 530\text{ nm}$	V_O	typ. 510 mV
Rise time (10%/ 90%) $V_R = 5\text{ V}; R_L = 50\ \Omega; \lambda = 535\text{ nm}$	t_r	typ. 47 ns
Fall time (10%/ 90%) $V_R = 5\text{ V}; R_L = 50\ \Omega; \lambda = 535\text{ nm}$	t_f	typ. 67 ns
Forward voltage $I_F = 10\text{ mA}; E = 0$	V_F	typ. 0.95 V
Capacitance $V_R = 0\text{ V}; f = 1\text{ MHz}; E = 0$	C_0	typ. 13.4 pF

Relative Spectral Sensitivity ^{1), 2)}

■ photodiode: $S_{rel} = f(\lambda)$



Tema n. 2 (valido per: classe LM/29 - Ingegneria Elettronica, classe LM/31 - Ingegneria Gestionale, classe LM/32 - Ingegneria Informatica)

Si consideri il caso di EventConsortium, un ente consortile dedicato alla gestione e al coordinamento degli attori coinvolti nell'organizzazione e nello svolgimento di eventi dal vivo, intesi come manifestazioni culturali, artistiche o di intrattenimento fruite dal pubblico in presenza e caratterizzate da un'esecuzione o rappresentazione in tempo reale (quali concerti, rappresentazioni teatrali, spettacoli performativi e performance artistiche). Il consorzio riunisce organizzatori, tecnici, artisti, fornitori di beni e servizi e agenzie di biglietteria, con l'obiettivo di aumentare la trasparenza e l'efficienza nel settore degli eventi dal vivo, promuovendo standard condivisi per la gestione dei dati relativi agli eventi e per la tracciabilità delle operazioni, dalla programmazione iniziale fino alla conclusione dell'evento.

La gestione di un evento dal vivo comprende l'insieme delle attività necessarie per organizzarne e realizzarne lo svolgimento, tra cui la pianificazione, la prenotazione delle location, la stipula dei contratti con artisti e fornitori, la vendita dei biglietti e la verifica delle autorizzazioni e delle certificazioni di sicurezza. Tali attività coinvolgono sia soggetti privati sia enti pubblici, come uffici comunali, vigili del fuoco ed enti preposti alla sicurezza sul lavoro.

Per favorire una gestione coordinata delle informazioni relative agli eventi, EventConsortium commissiona la progettazione e lo sviluppo di una piattaforma Web in grado di raccogliere, organizzare e rendere accessibili i dati ai diversi attori coinvolti, supportando la tracciabilità delle operazioni organizzative e dei relativi flussi documentali.

All'interno del consorzio operano attori con ruoli distinti e complementari, ciascuno con responsabilità specifiche nell'organizzazione e nello svolgimento degli eventi dal vivo.

- Gli organizzatori pianificano e gestiscono gli eventi, occupandosi di definire date, location, caratteristiche dello spettacolo, elenco dei partecipanti e documentazione legale. Sono responsabili della stipula dei contratti con artisti e fornitori, della gestione dei permessi e delle autorizzazioni legali e di sicurezza necessarie allo svolgimento dell'evento e della supervisione complessiva del programma dell'evento.
- I tecnici e responsabili della logistica sovrintendono all'allestimento, alle prove tecniche e alla sicurezza, gestendo tutte le attività operative necessarie al corretto svolgimento dello spettacolo.
- Gli artisti partecipano agli spettacoli e contribuiscono alla realizzazione del programma, portando la loro performance e coordinandosi con gli altri attori coinvolti.
- I fornitori mettono a disposizione materiali, attrezzature e servizi fondamentali per la buona riuscita dell'evento, come impianti audio e luci, attrezzature e materiali per allestimenti scenici.
- Le agenzie di biglietteria gestiscono la vendita dei biglietti e il monitoraggio delle prenotazioni, garantendo la corretta allocazione dei posti e il rispetto dei vincoli autorizzativi previsti per l'evento, quali le capienze massime delle location, le condizioni stabilite nei permessi comunali e le prescrizioni di sicurezza definite dalle autorità competenti.

Attualmente, la gestione delle informazioni risulta frammentata, con ciascun attore che amministra i propri dati in modo indipendente. Gli organizzatori utilizzano sistemi locali non integrati, i documenti legali e logistici vengono spesso trasmessi tramite e-mail o cartaceo, e le informazioni sugli eventi non sono facilmente condivisibili tra le parti coinvolte. Questa situazione rende complessa la ricostruzione della storia completa di un evento, dalla pianificazione fino alla sua conclusione, e complica la gestione delle segnalazioni relative a problemi, anomalie o richieste di intervento emerse durante le varie fasi dell'evento. La frammentazione comporta inoltre ritardi operativi, duplicazione delle verifiche e maggiori rischi di errori o omissioni documentali.

La piattaforma Web di EventConsortium fornirà strumenti specifici per ciascun ruolo, con livelli di accesso differenziati e sistemi per il tracciamento delle modifiche e delle operazioni effettuate.

Gli organizzatori potranno creare schede evento standardizzate contenenti le informazioni principali, quali descrizione, stato legale (livello di conformità normativa e validità di permessi, licenze e certificazioni), valutazione dei rischi, documentazione tecnica e disponibilità dei posti, e potranno inoltre caricare e aggiornare permessi e planimetrie. Saranno inoltre responsabili della gestione dei contratti con artisti e fornitori e della pubblicazione dei dati per pubblico e partner, garantendo continuità e completezza delle informazioni lungo tutte le fasi dell'evento. I tecnici e responsabili della logistica registreranno rapporti, checklist operative e certificazioni relative agli allestimenti e alle prove, consentendo il monitoraggio dello stato delle attività. Gli artisti vedranno registrata la propria disponibilità, i ruoli nel programma e la documentazione relativa alla partecipazione. I fornitori potranno aggiornare informazioni su materiali, attrezzature e servizi forniti e inviare documenti in modo sicuro, assicurando la disponibilità delle risorse necessarie all'evento. Le agenzie di biglietteria avranno accesso ai dati sugli eventi e sulla disponibilità dei posti, gestendo vendite e prenotazioni in modo chiaro, trasparente e conforme alle normative.

Un elemento centrale della piattaforma sarà costituito da un sistema documentale unico, che consentirà la gestione strutturata di contratti, permessi, certificazioni e documenti di conformità, garantendo il controllo delle versioni e delle validità temporali dei documenti. Il sistema dovrà inoltre fornire strumenti per ricercare rapidamente i documenti e verificare automaticamente che tutti i documenti richiesti siano presenti, aggiornati e completi, segnalando eventuali mancanze o scadenze.

La piattaforma includerà inoltre un modulo direzionale per le analisi strategiche, rivolto in particolare al board direttivo di EventConsortium e alle figure di coordinamento del consorzio. Tale componente consentirà di aggregare e analizzare i dati provenienti dall'intera rete di eventi, offrendo strumenti di analisi, dashboard e report utili per il monitoraggio della qualità degli eventi, la valutazione delle performance degli organizzatori, l'individuazione di criticità ricorrenti di natura tecnica o logistica e la pianificazione di interventi mirati al miglioramento dei processi.

Si richiede al Candidato di sviluppare, con riferimento allo specifico caso descritto, alle particolari necessità e motivazioni fornite (e quindi non in maniera generica), i seguenti punti:

1. Specificare i requisiti del sistema informatico, dettagliandoli opportunamente; il Candidato può aggiungere nuovi requisiti o raffinare quelli forniti sulla base della propria esperienza e di ipotesi ragionevoli, mantenendo la coerenza con gli obiettivi operativi, organizzativi e strategici di EventConsortium.
2. Proporre un progetto di massima del sistema informatico e di telecomunicazioni complessivo a supporto della piattaforma, descrivendo l'architettura software (sistemi operativi, framework applicativi, DBMS, servizi backend, componenti di integrazione con sistemi esterni) e hardware (server, storage, reti, modalità di interconnessione). Il Candidato dovrà evidenziare le scelte infrastrutturali adottate per garantire affidabilità, scalabilità e resilienza del sistema, illustrando inoltre le soluzioni previste per la continuità operativa, il disaster recovery, il monitoraggio delle performance e la gestione delle anomalie, specificando strumenti e procedure per backup sicuri, ridondanza, failover e monitoraggio continuo della piattaforma.
3. Specificare, mediante opportuni linguaggi grafici (ad esempio diagrammi UML), i principali moduli della piattaforma dedicati all'elaborazione, alla gestione e all'archiviazione dei dati, evidenziandone le relazioni reciproche e le interazioni con i principali sottosistemi della piattaforma.
4. Progettare il modulo direzionale della piattaforma, descrivendone in modo strutturato le funzionalità principali e i relativi flussi informativi. La progettazione dovrà indicare le tecnologie previste, definire i KPI (Key Performance Indicators) utili per il monitoraggio dell'andamento degli eventi e della qualità dei

processi di pianificazione, allestimento, esecuzione e gestione delle prenotazioni, specificare le fonti dati da cui tali indicatori sono alimentati e illustrare le modalità di presentazione delle informazioni a supporto delle decisioni del board consortile di EventConsortium.

5. La direzione consortile di EventConsortium osserva: *“Nonostante i benefici offerti dalla piattaforma Web, che semplifica la raccolta, l’aggiornamento e la condivisione delle informazioni tra i diversi attori, permangono criticità legate all’immutabilità dei dati, alla verificabilità indipendente delle informazioni e alla trasparenza tra soggetti diversi. Ad esempio, la piattaforma Web, pur garantendo il tracciamento delle modifiche, il controllo delle versioni e la gestione dei ruoli, non impedisce modifiche ai dati effettuate direttamente sulla base dati della piattaforma, bypassando il livello applicativo, da parte di utenti amministratori con privilegi elevati. Tale possibilità compromette l’immutabilità delle informazioni, la verificabilità indipendente della storia di un evento e la trasparenza tra soggetti diversi. In questo scenario, diventa difficile fornire prove incontestabili delle verifiche tecniche effettuate, delle certificazioni rilasciate e di altri passaggi chiave, mettendo a rischio la credibilità del sistema agli occhi di autorità di vigilanza e organismi di controllo.”*

Il Candidato discuta criticamente se tali perplessità di EventConsortium siano fondate o meno, motivando la propria posizione. Qualora ritenga fondate le preoccupazioni di EventConsortium, proponga soluzioni tecnologiche e architetturali e illustri le implicazioni per i soggetti aderenti al consorzio.

Tema n. 3 (valido per: classe LM/29 - Ingegneria Elettronica, classe LM/31 - Ingegneria Gestionale, classe LM/32 - Ingegneria Informatica)

La sicurezza delle informazioni rappresenta un requisito essenziale in qualunque contesto operativo, assumendo un ruolo particolarmente critico negli ambienti aeroportuali. Un aeroporto gestisce un insieme eterogeneo di dati sensibili (informazioni personali dei passeggeri, dati relativi ai voli, transazioni finanziarie, informazioni sul personale, dati di sicurezza fisica e logica) la cui protezione è determinante sia per la tutela della privacy sia per la continuità operativa e la sicurezza dell’infrastruttura.

La norma *ISO/IEC 27001* fornisce un riferimento strutturato per l’implementazione di un *Sistema di Gestione della Sicurezza delle Informazioni (SGSI)*, volto a proteggere i dati, identificare e mitigare i rischi, garantire la continuità dei servizi e assicurare conformità alle normative vigenti. In ambito aeroportuale, l’applicazione della norma assume particolare rilevanza al fine di prevenire attacchi informatici, proteggere le informazioni critiche e garantire la disponibilità costante dei sistemi a supporto delle operazioni di volo.

Prima parte

Sulla base delle premesse fornite, si richiede al Candidato di sviluppare i seguenti punti.

1. Descrivere come il modello RID (Riservatezza, Integrità, Disponibilità) si applichi ai sistemi informativi aeroportuali. Fornire esempi relativi alla protezione dei dati dei passeggeri, ai sistemi di programmazione dei voli e ai sistemi di sicurezza aeroportuale.
2. Illustrare il processo di valutazione del rischio applicato a un contesto aeroportuale. Identificare i principali rischi di sicurezza delle informazioni, descrivendo le fasi di identificazione, analisi, valutazione e mitigazione, con indicazione delle misure che possono essere adottate.
3. Descrivere i controlli fisici (ad es. gestione degli accessi ad aree sensibili) e logici (autenticazione e autorizzazione ai sistemi informativi) che devono essere implementati con riferimento alla norma *ISO/IEC 27001*, con esempi applicabili alla realtà aeroportuale.

4. Definire gli elementi che una procedura di gestione degli incidenti informatici deve contenere in un contesto aeroportuale. Si spieghi come un sistema di gestione della sicurezza delle informazioni possa supportare la gestione di eventi quali attacchi *malware* o *ransomware* che interessino sistemi critici (es. controllo dei voli, database passeggeri). Inoltre, si individuino gli aspetti principali per la preparazione di un audit di conformità alla norma ISO/IEC 27001 in ambito aeroportuale e si descriva come un'organizzazione aeroportuale possa assicurare l'allineamento alle normative nazionali e internazionali sulla sicurezza delle informazioni.

Seconda parte - Caso di studio in ambito aeroportuale

Un aeroporto di medie dimensioni, che gestisce sia traffico passeggeri sia traffico cargo, movimentata annualmente circa 10 milioni di passeggeri e un volume di merci pari a circa 500.000 tonnellate. L'infrastruttura informatica a supporto delle attività operative è altamente integrata e tratta una vasta gamma di informazioni sensibili: dati personali dei passeggeri, dettagli relativi ai voli, informazioni di pagamento, dati riguardanti le spedizioni cargo, documentazione di trasporto e certificati di sicurezza, oltre ai dati provenienti dai sistemi di sicurezza fisica, quali controllo degli accessi, videosorveglianza e monitoraggio delle aree sensibili. L'aeroporto è inoltre responsabile della gestione delle operazioni di volo, dell'assegnazione degli slot alle compagnie aeree, della gestione dei bagagli e della tutela della sicurezza dei passeggeri.

Di recente l'aeroporto è stato oggetto di un tentativo di attacco informatico mirato, volto ad accedere a informazioni sensibili del sistema di gestione dei voli e del database dei passeggeri. L'intrusione, condotta tramite un malware sofisticato, è stata individuata tempestivamente grazie ai controlli di sicurezza già in essere. L'incidente è stato contenuto senza conseguenze rilevanti grazie alla rapidità degli interventi e alla corretta gestione dell'emergenza, ma ha comunque evidenziato alcune vulnerabilità nei sistemi di accesso e nei meccanismi di protezione, sollevando dubbi sulla robustezza delle misure di sicurezza e sulla capacità dell'aeroporto di garantire adeguata continuità operativa in situazioni critiche. A seguito dell'evento, il management ha disposto una revisione complessiva delle misure di sicurezza informatica e delle politiche di sicurezza, richiedendo un riallineamento alle prescrizioni della norma ISO/IEC 27001 al fine di incrementare la resilienza del sistema e prevenire il verificarsi di minacce analoghe.

Con riferimento allo scenario descritto, si richiede al Candidato di sviluppare i seguenti punti.

5. Descrivere in che modo un SGSI possa supportare lo sviluppo di una politica di continuità operativa e di piani di recupero in caso di disastro, ad esempio in seguito a un attacco informatico che comprometta i sistemi di gestione dei voli e i dati dei passeggeri. Occorre inoltre indicare: (i) le misure specifiche da adottare per garantire la disponibilità continua dei sistemi critici, come il controllo dei voli e l'accesso ai dati dei passeggeri, durante un'emergenza; (ii) esempi pratici di implementazione di misure preventive, tra cui backup, ridondanza e pianificazione delle risorse; (iii) esempi pratici di misure reattive, come procedure di recupero e comunicazione con i clienti, al fine di assicurare che le operazioni aeroportuali non vengano interrotte.
6. Descrivere come debbano essere gestiti i controlli di accesso, sia fisici sia logici, e chiarire in che modo un SGSI debba influire sulla gestione dell'accesso alle aree sensibili, come sale server, sistemi di gestione dei voli e informazioni riservate relative a passeggeri e spedizioni cargo. Si dovranno inoltre specificare: (i) le misure di autenticazione, autorizzazione e audit da implementare per prevenire accessi non autorizzati e garantire la protezione dei dati sensibili; (ii) le modalità di gestione dei permessi di accesso ai sistemi per dipendenti e fornitori esterni, quali compagnie aeree, agenzie di sicurezza o imprese di spedizione.

7. Descrivere come la norma ISO/IEC 27001 promuova il miglioramento continuo nel contesto di un aeroporto che gestisce sia passeggeri sia cargo, specificando in che modo debba essere effettuato il monitoraggio continuo dei rischi e delle misure di sicurezza. Occorre illustrare: (i) come audit interni, revisioni periodiche e analisi delle performance possano contribuire a migliorare la gestione della sicurezza delle informazioni; (ii) come debba essere monitorata l'efficacia dei controlli in un ambiente che integra sistemi diversi, quali gestione dei voli, gestione del cargo e accesso alle aree sicure; (iii) in che modo la revisione degli incidenti passati possa supportare il miglioramento delle politiche di sicurezza e delle procedure operative.