WatchTower

1 Introduzione 3

1.1 Informazioni sul progetto 3

1.2 Abstract 3

1.3 Scopo 3

2 Analisi 4

2.1 Analisi del dominio 4

2.2 Analisi e specifica dei requisiti 4

2.3 Use case 6

2.4 Pianificazione 6

2.5 Analisi dei mezzi 7

2.5.1 Software 7

2.5.2 Hardware 7

3 Progettazione 8

3.1 Design dell’architettura del sistema 8

3.2 Design dei dati e database 9

3.3 Design delle interfacce 9

3.4 Design procedurale 10

3.4.1 Connessione LDAP 10

3.5 Limiti 10

4 Implementazione 11

4.1 Applicativo Web 11

4.1.1 Installazione frontend 11

4.1.2 Installazione backend 11

4.1.3 Frontend 12

4.1.4 Backend 14

4.1.5 Container 17

4.2 Microcontrollore 17

4.2.1 CoreS3 18

4.2.2 NanoC6 19

4.2.3 Architettura implementata 19

4.2.4 Registrazione badge 20

4.2.5 Accesso 21

4.2.6 Comunicazione wireless 22

4.2.7 Sensori 22

4.2.8 Montaggio sistema 22

5 Test 22

5.1 Protocollo di test 22

5.2 Risultati test 25

5.3 Mancanze/limitazioni conosciute 25

6 Consuntivo 25

7 Conclusioni 26

7.1 Sviluppi futuri 26

7.2 Considerazioni personali 26

8 Glossario 26

9 Bibliografia 27

9.1 Bibliografia per articoli di riviste: 27

9.2 Bibliografia per libri 27

9.3 Sitografia 27

10 Allegati 27

11 Indice delle Figure 27

# Introduzione

## Informazioni sul progetto

* Titolo Progetto: WatchTower
* Allievi: Tom Schillerwein I4BC
* Docente responsabile: Pascal Poncini
* Scuola: Arti e Mestieri Trevano, sezione Informatica
* Data di inizio e fine: 03.02.2025 – 03.04.2025
* Data di presentazione: 07 – 11.04.2025

## Abstract

The aim of this project is to implement a physical monitoring system for the server room of the black network at the CPT in Trevano. This monitoring includes temperature, humidity, access control and more and is carried out by means of various sensors specially positioned in the server room. It is also necessary to develop a web application that allows the data collected by the sensors to be visualised in graphs and tables, and a system of notifications and alerts for the network admins and teachers, which can also be managed from the application.

## Scopo

Lo scopo di questo progetto è implementare un sistema di monitoraggio fisico della sala server della rete nera della CPT di Trevano. Questo monitoraggio include la temperatura, l’umidità, il controllo degli accessi e altro. Questo monitoraggio viene eseguito tramite diversi sensori posizionati appositamente nella server room. È inoltre necessario sviluppare un’applicazione web che permette la visualizzazione dei dati raccolti dai sensori in grafici e tabelle e un sistema di notifiche e allerte per i sistemisti della rete e i docenti. Anche queste notifiche sono gestibili dall’applicativo web.

# Analisi

## Analisi del dominio

Questo progetto permette di semplificare il monitoraggio fisico della sala server tramite sensori che trasmettono le informazioni raccolte ad una dashboard a cui i sistemisti hanno accesso. Se i valori rilevati superano un certo livello definito, i sistemisti ricevono un avviso. Al momento i server nella sala vengono monitorati, ma non la sala fisica. Viene unicamente richiesto aprire la porta con un badge con i permessi necessari. Esistono già soluzioni simili, come Monnit, che però sono costose e meno specifiche per la nostra situazione.

## Analisi e specifica dei requisiti

|  |  |
| --- | --- |
| **ID: REQ-001** | |
| **Nome** | Installazione sensori |
| **Priorità** | 1 |
| **Versione** | 1.0 |
| **Note** | Montare i sensori, cavi e controller nella sala server. |
| **Sotto requisiti** | |
| **001** | Avere tutti i componenti hardware necessari per il progetto. |

|  |  |
| --- | --- |
| **ID: REQ-002** | |
| **Nome** | Raccolta dati dai sensori |
| **Priorità** | 1 |
| **Versione** | 1.0 |
| **Note** | Necessita che i sensori siano correttamente configurati e comunicano con il controller. |
| **Sotto requisiti** | |
| **001** | Il sistema deve raccogliere i dati di temperatura e umidità dal sensore ENV III. |
| **002** | Deve raccogliere i dati del sensore di CO2 e azionare il LED. |
| **003** | Deve registrare gli accessi tramite RFID. |
| **004** | Deve rilevare movimento attraverso il sensore PIR. |
| **005** | Deve acquisire input dalla mini tastiera per capire il tipo di accesso. |

|  |  |
| --- | --- |
| **ID: REQ-003** | |
| **Nome** | Creazione database |
| **Priorità** | 1 |
| **Versione** | 1.0 |
| **Note** | Si necessitano i permessi di root |
| **Sotto requisiti** | |
| **001** | Il database deve supportare la memorizzazione dei dati rilevati dai sensori. |

|  |  |
| --- | --- |
| **ID: REQ-004** | |
| **Nome** | Creazione dashboard |
| **Priorità** | 1 |
| **Versione** | 1.0 |
| **Note** | Sviluppare un'interfaccia utente chiara e responsive. |
| **Sotto requisiti** | |
| **001** | Si necessita una maschera di login |
| **002** | Bisogna visualizzare i dati dei sensori in tempo reale. |
| **003** | Grafici con storico dei dati. |
| **004** | Possibilità di configurare notifiche e allerte per valori specifici. |

|  |  |
| --- | --- |
| **ID: REQ-005** | |
| **Nome** | Notifiche e allerte |
| **Priorità** | 1 |
| **Versione** | 1.0 |
| **Note** | Si necessitano i permessi di root / Dipende dal requisito REQ-001 (Creazione DB) |
| **Sotto requisiti** | |
| **001** | Invio email in base a valori di default o custom. |

## Use case

|  |
| --- |
| 1 Use Case |

## Pianificazione

|  |
| --- |
| 2 Diagramma di Gantt preventivo |

## Analisi dei mezzi

Per questo progetto utilizzo un PC scolastico per lo sviluppo, un controller M5Stack CoreS3 e alcuni sensori.

### Software

* Visual Studio Code 1.93, come editor di testo
* Google Chrome 131.0, come browser per visualizzare il sito durante lo sviluppo
* Mozilla Firefox 126.0, per testare la visualizzazione del sito
* Onlinegantt.com, per il Gantt
* Microsoft Visio, per fare lo Use Case
* Microsoft Word e Obsidian, per redigere la documentazione, il QdC e il diario
* GitLab, come Repository locale della scuola
* Excalidraw, per creare schemi e diagrammi

### Hardware

Computer utilizzato per le ricerche e lo sviluppo:

* Processore: Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz
* RAM: 32GB
* Scheda Video: NVIDIA GeForce RTX 2060
* SSD: 512GB
* Monitor 1920x1080 60Hz
* Monitor 1600x900 60Hz

Componenti M5Stack:

* Cores3
* NanoC6
* Mini keyboard
* RFID sensor
* PIR sensor
* ENV III sensor
* 2x LED RGB
* Tvoc/eCO2

# Progettazione

## Design dell’architettura del sistema

Per quanto riguardo la parte IoT del progetto, esso viene create con dei microcontrollori e sensori M5Stack. I microcontrollori Nano C6 comunicano con il microcontrollore principale CoreS3 tramite “PROTOCOLLO”, invece i Nano C6 comunicano con Led, sensori e input tramite cavo Grove. Per collegare più sensori ad un singolo Nano C6, perché ha senso metterli insieme, uso dei hub per convertire 1 port in 3.

|  |
| --- |
| 3 Schema Microcontrollore e Sensori |

Questo schema rappresenta l’architettura principale del sito web con il CoreS3 che comunica i dati al backend, e questo li salva successivamente nel DB MySQL. Se il frontend fa una richiesta questa viene gestita dal Back End e se necessario prende i dati dal DB.

|  |
| --- |
| 4 Architettura sistema |

## Design dei dati e database

Il database serve soprattutto a salvare i dati provenienti dai sensori, ma anche per salvare le notifiche e le impostazioni di esse degli utenti e il collegamento tra utenti e badge. Infatti, utilizzando LDAP non mi è necessario gestire gli utenti nel DB e devo soltanto salvare il nome univoco degli utenti per le notifiche e le impostazioni. Ho optato per l’uso di enum in alcune tabelle per semplificare il database e perché i possibili valori di questi campi sono moto pochi.

|  |
| --- |
| 5 Diagramma ER |

## Design delle interfacce

Ho creato questa struttura di interfacce, per capire quali dovrò creare, inoltre ho messo in esse un design di base che poi verrà finalizzato quando le implementerò. Per le pagine che visualizzano i dati (temperatura, umidità, livello di CO2, ecc.) userò lo stesso layout di pagina, cambiando semplicemente descrizione, dati e colori.

|  |
| --- |
| 6 Struttura interfacce |

## Design procedurale

### Connessione LDAP

Il mio progetto richiede l'integrazione con un servizio LDAP per l'autenticazione degli utenti in quanto solo persone della scuola devono avere la possibilità di accedere al mio applicativo. Inoltre usando questa tecnologia, non devo gestire i permessi dei singoli utenti, ma posso semplicemente capire di quale gruppo fa parte un utente e in base a questo decidere cosa può fare/vedere. Per eseguire il bind (autenticazione) iniziale con il server LDAP, utilizzo un utente di servizio creato apposta per il mio applicativo (watch.tower). In seguito faccio la ricerca dell’utente che ha immesso le proprie credenziali, tramite username, che nel LDAP della rete nera corrisponde a sAMAccountName.Se l’utente viene trovato, provo a fare un bind anche di questo utente con la sua password, e se questa riesce vuol dire che l’utente ha immesso username e password corrette. Se questo è il caso viene generato un JWT per l’utente che viene poi reindirizzato alla home page.

|  |
| --- |
| 7 Protocollo LDAP |

## Limiti

Questa implementazione, con M5Stack e i sensori scelti, presenta ovviamente delle limitazioni di cosa è possibile rilevare, di seguito viene elencato ciò che è possibile rilevare con i vari sensori. Inoltre è importante notare che questo sistema può non registrare dati o registrarne di errati, generando potenzialmente falsi allarmi o non generandone degli alri.

***ENV III:*** rileva periodicamente la temperatura e l’umidità dell’ambiente, ma non ne traggono conclusioni, sta perciò all’utente che legge i dati capire i problemi a partire dai dati forniti.

***Tvoc/eCO2:*** rileva periodicamente la concentrazione di CO2 nell’aria, con discetta precisione. Come per il sensore di temperatura e umidità, non è in grado di trarre conclusioni dai dati rilevati e li riporta semplicemente. Per questo motivo non è un rilevatore di incendi, ma semplicemente un indicatore che qualcosa potrebbe essere al di fuori dal normale se i valori rilevati sono troppo elevati.

***PIR:*** rileva il movimento di una persona, tuttavia, tramite dei test con il sensore, ho notato che questo non è accurato al 100%, infatti ogni tanto un movimento non viene rilevato da esso, questo potrebbe portare ad un accesso non autorizzato che non viene colto dal sistema.

***Keyboard:*** tramite questa mini tastiera vengono immessi gli input di un utente, sia per motivare la propria presenza, sia per creare il link tra badge e utente che per segnalare l’uscita dalla sala server. È necessario premere invio dopo l’inserimento dell’input desiderato, per garantire che ciò che è stato scritto venga trasmesso.

***RFID:*** legge lo UID del badge scolastico e lo inva al microcontrollore. Nessuna limitazione conosciuta in questo ambito.

***LED:*** mostrano tramite delle luci lo stato di alcuni valori, per esempio quello di contrentazione di CO2. Nessuna limitazione conosciuta in questo ambito.

# Implementazione

## Applicativo Web

### Installazione frontend

Il frontend dell'applicazione è sviluppato con Vue.js e utilizza Tailwind CSS e Shadcn Vue per la gestione dei componenti UI.

Prima di iniziare l’installazione verificare che node.js e npm sono installati tramite il comando:

node -v

npm -v

Installazione di Vue.js:

npm install -g @vue/cli

npm create vue@latest

cd watchtower

npm install

Installazione di tailwind:

npm install -D tailwindcss@3 postcss autoprefixer

npx tailwindcss init -p

Installazione di Shadcn Vue:

npm install shadcn-vue

npx shadcn-vue@latest init

Per aggiungere i componenti di Shadcn Vue:

npx shadcn-vue@latest add *nome\_componente (es: button)*

Per fare partire il server:

npm run dev

### Installazione backend

Il backend è basato su Node.js e utilizza Express.js, Prisma, LDAP.js, JWT e un database MySQL.

Prima di iniziare l’installazione verificare che node.js e MySQL siano installati.

Creazione progetto Node.js con i pacchetti necessari al progetto:

npm init

npm install express cors dotenv mysql2 @prisma/client ldapjs jsonwebtoken nodemailer winston

npx prisma init

Modificare i file .env (connessione e credenziali DV) e schema.prisma (modello dei dati) con le informazioni giuste dopodiché utilizzare il seguente comando prisma per creare una migrazione:

npx prisma migrate dev --name *nome\_migrazione*

### Frontend

Il frontend è sviluppato con Vue.js usando la sintassi di script setup e composition api. Per la parte grafica ho usato Tailwind CSS in combinazione con Shadcn Vue. Ho strutturato le view utilizzando soprattutto componenti di Shadcn aggiustandoli in modo da soddisfare le mie necessità.

|  |
| --- |
| 8 Struttura cartelle frontend |

#### Componenti

Per rendere il codice più leggibile e riutilizzabile, oltre a usare i componenti Shadcn, ho creato dei componenti custom, che una volta definiti posso riutilizzare nell’intero applicativo. Questo è molto comodo soprattutto perché questi componenti sono parametrizzabili, perciò dalla view principale è possibile modificare i dati visualizzati dai componenti.

Esempio di componente custom parametrizzabile, in questo caso la card dell’home page:

<MetricCard v-if="co2Data" :title="'CO₂'" :value="co2Data.value + ' ppm'"

:description="co2Data.description" link="/co2">

<template #icon>

            <CloudIcon class="size-4 text-gray-500" />

      </template>

</MetricCard>

#### Interfacce

Per poter confrontare il design iniziale e il risultato finale delle interfacce grafiche di seguito viene mostrato il risultato finale della pagina home e della pagina della temperatura. Come si può notare la disposizione degli elementi è rimasta uguale, e ho semplicemente popolato di scritte, valori e grafici le pagine.

|  |
| --- |
| 9 Pagina Home |

|  |
| --- |
| 10 Pagina Temperatura |

Per ogni pagina dei dati, è possibile cambiare il grafico da “ultima ora”, a “ultimo giorno” e “ultima settimana” dove in base al grafico cambia la scala temporale e di dati visualizzati.

### Backend

Il backend è basato su Node.js con Express per gestire le API.

|  |
| --- |
| 11 Struttura cartelle backend |

Ho strutturato il progetto secondo le best practice di Node.js, per permettere una buona leggibilità del codice e una facile modifica del progetto.

Ho inoltre utilizzato le seguenti tecnologie per implementare le funzionalità richieste:

* Express 🡪 Framework web per gestire API REST.
* Prisma ORM 🡪 Gestione del database MySQL in modo efficiente.
* LDAP.js 🡪 Connessione e autenticazione con il server LDAP.
* JWT 🡪 Gestione della sessione degli utenti.
* Nodemailer 🡪 Invio delle email di notifica.
* Winston 🡪 Gestione dei log.

#### Autenticazione

L’utente si autentica tramite LDAP, una volta che le credenziali inserite sono validate dal server LDAP, il mio applicativo crea un JWT, il quale scade dopo 6 ore dalla creazione. Questo token deve essere incluso nelle richieste successive fatte dal client al server, altrimenti risulteranno con una risposta di errore. Il server può verificare la validità del token JWT e autorizzare l'accesso alle risorse in base alle informazioni contenute nel token (tramite middleware), per esempio in base al ruolo (allievo o sistemista/docente).

Nel codice seguente c’è la funzione per verificare un JWT passato nella richiesta del client, dove per prima cosa viene estratto il token dall’header della richiesta, dopodiché viene verificato se il token è presente e infine verificato, usando anche la secret key con cui era stato creato. Se il token è valido il middleware non interviene e fa continuare l’esecuzione altrimenti ritorna un errore:

function authenticateToken(req, res, next) {

  const token = req.headers["authorization"];

  if (!token) {

    return res.status(403).json({ message: "Access denied" });

  }

  jwt.verify(token, process.env.SECRET\_KEY, (err, user) => {

    if (err) {

      return res.status(403).json({ message: "Invalid token" });

    }

    req.user = user;

    next();

  });

}

#### Log

In questo progetto ho dato importanza anche ai log, utilizzando Winston per la loro creazione, in questo modo posso gestire la gravità degli eventi e categorizzarli in info, warning e error. Ho inoltre diviso i log in tre file diversi: nel primo si trovano i log del server, per esempio di quando si accende; nel secondo si trovano i log che riguardano l’autenticazione di un utente e l’ultimo contiene tutti i log degli endpoint del server, siano essi chiamati dal frontend o dal microcontrollore. Di seguito un esempio di creazione di log e il suo risultato in forma scritta nel file di log:

Codice:

logger.info(`API call to /${type}/lastHour`);

Risultato:

14-02-2025, 11:19:17 [INFO]: API call to /temperature/lastHour

#### Salvataggio dati

Gli endpoint per salvare dati nel DB sono preceduti da /api, e verranno chiamata dal microcontrollore per salvare i dati rilevati dai sensori. C’è un endpoint per ogni categoria di dati rilevata (temperatura, umidità, accessi e CO2), qui i dati vengono validati e successivamente salvati nella corrispondente tabella.

#### Fetch dei dati

Gli endpoint che permettono all’applicativo web di prendere i dati per i grafici e le tabelle per ogni tipo di dato sono situati in /. Qui ho creato un endpoint comune per ogni tipo di grafico in cui dinamicamente viene utilizzato il tipo giusto in base al parametro della richiesta:

router.get("/:type/lastHour", authenticateToken, async (req, res) => {

  await getLastHourData(req.params.type, res);

});

#### Salvataggio accessi

L’endpoint che salva gli accessi alla sala server, /api/access, ma prima di salvare direttamente i dati che ha ricevuto, controlla i dati ricevuti e verifica se l’utente che eseguito l’accesso si trova ancora nel LDAP. Se questo non è il caso viene eliminato il recordi del badge di questo utente, e l’accesso viene marcato come non autorizzato. Altrimenti esso viene salvato con utente, data, motivo e se è autorizzato.

api.post("/access", authenticateToken, async (req, res) => {

  try {

    const { name, motive, authorized, timestamp } = req.body;

    const ldapUsers = await fetchLdapUsers(["CN=Docenti", "CN=Sistemisti"]);

    if (timestamp && !isNaN(Date.parse(timestamp))) {

      if (!ldapUsers.some(user => user.username[0] === name)) {

        logger.info("User no more in LDAP in /api/access");

        logger.info("Removing user from link badge in /api/access");

        await prisma.badge\_link.deleteMany({

          where: { user: name },

        });

        await prisma.access.create({

          data: {

            timestamp: new Date(timestamp),

            name: "",

            motive: "",

            authorized: false

          },

        });

        createNotifications("ACCESS", 0, timestamp);

        return res.status(403).json({ message: "User not in LDAP" });

      }

      await prisma.access.create({

        data: {

          timestamp: new Date(timestamp),

          name: name || "",

          motive: motive || "",

          authorized,

        },

      });

      logger.info("Access data saved successfully in /api/access");

      if (!authorized) {

        createNotifications("ACCESS", 0, timestamp);

      }

      return res.status(201).json({ message: "Access data saved successfully" });

    } else {

      logger.error("Wrong data sended to /api/access");

    }

    return res.status(500).json({ message: "Invalid access data." });

  } catch (error) {

    …

  }

});

### Container

Dopo aver sviluppato l’intero applicativo web e averlo testato, ho deciso di fare il deploy tramite container, perciò ho creato un container per il DB, uno per il frontend e uno per il backend. Non ho dovuto cambiare niente nel codice dato che le tre parti erano già separate tra di loro durante lo sviluppo. Per il container database è possibile utilizzare una distribuzione Docker di MySQL di base, invece per il frontend e il backend devo utilizzare dei Dockerfile per creare dei container personalizzati.

Il Dockerfile del backend è piuttosto semplice, in quanto prende la distribuzione Docker di node 22.14 e copia dentro i miei file di progetto, dopodiché installa le dipendenze necessarie e istanzia l’ORM Prisma e in seguito dichiara la porta su cui viene esposto il servizio (3000). Come ultimo esegue la migrazione nel database e poi fa partire il server node:

FROM node:22.14

WORKDIR /app

COPY package.json package-lock.json ./

RUN npm install

COPY . .

RUN npx prisma generate

EXPOSE 3000

CMD npx prisma migrate deploy && node app.js

Invece per il frontend ci sono un paio di passaggi in più, anche qui si parte dalla stessa distribuzione di base e si copiano i file del progetto e si installano le dipendenze. Dopodiché forzo una variabile di ambiente direttamente nel Dockerfile, cosa che normalmente non si fa, perché si potrebbero assegnare dal docker-compose, ma in questo caso è necessario perché pe far funzionar il frontend devo generare dei file e la variabile d’ambiente deve essere impostata prima che vengano compilati. Dopodiché installo apache web server e rimpiazzo i file di configurazioni di default con quelli creati da me. Prima di avviare apache espongo la porta 80 sui cui è accessibile la dashboard:

FROM node:22.14 AS build

WORKDIR /app

COPY package.json package-lock.json ./

RUN npm install

COPY . .

ENV VITE\_BASE\_URL\_API="http://watchtower-api.caprover.samt.local:3333"

RUN npm run build

FROM httpd:latest

COPY --from=build /app/dist/ /usr/local/apache2/htdocs/

COPY public/new-apache.conf /usr/local/apache2/conf/httpd.conf

COPY public/.htaccess /usr/local/apache2/htdocs/

EXPOSE 80

CMD ["httpd", "-D", "FOREGROUND"]

Per combinare il tutto viene usato il file docker-compose, nel quale vengono indicate tutte le variabili d’ambiente, le dipendenze dei container tra di loro, la rete su cui inserire i Docker e molto altro.

## Microcontrollore

Per la parte di IoT (Internet of Things), ho optato per una soluzione basata su M5Stack, più precisamente un microcontrollore CoreS3 combinato con dei NanoC6 per tramettere i dati dai sensori al backend che poi salva i dati nel database.

Ho programmato i microcontrollori in Python, con le necessarie librerie per interagire con l’hardware. Questo viene reso molto più facile dalla piattaforma uiflow.m5stack.com, un IDE online sviluppata appositamente per M5Stack, con cui è possibile eseguire codice e scaricare i file sui microcontrollori.

Per poter utilizzare i vari microcontrollori è necessario installare il firmware adatto, io l’ho fatto con M5burner, un applicativo che permette di scegliere il firmware giusto per ogni prodotto m5Stack e “bruciarlo” sul dispositivo.

|  |
| --- |
| 12 M5burner esempio firmware per CoreS3 |

### CoreS3

Il microcontrollore M5Stack CoreS3 è il controller principale della mia implementazione, infatti è colui che manda i dati al backend e colui che riceve i dati dai sensori e gestisce i LED. Ad esso sono collegati fisicamente un LED e il sensore del CO2, i quali vengono perciò controllati completamente da esso. Tutti gli altri sensori/input sono collegati a dei NanoC6, che mandano a loro volta i dati al CoreS3.

Grazie a questo protocollo di comunicazione wireless, che consente una trasmissione veloce ed efficiente dei dati tra dispositivi senza la necessità di una rete Wi-Fi. Perciò i NanoC6 possono inviare i dati al CoreS3 con poca latenza e un basso consumo energetico, cosa che lo rende una buona tecnologia per il mio caso d’uso.

|  |
| --- |
| M5Stack CoreS3 ESP32S3 Kit di Sviluppo IoT  13 M5Stack CoreS3 |

#### Schermate utente

Ho implementato una serie di schermate da visualizzare sul CoreS3, in modo da dare un feedback visivo all’utente di cosa sta facendo oppure di cosa deve fare per continuare il processo di accesso. Una volta eseguita la procedura d’accesso, viene visualizzata una schermata con informazioni utili, come temperatura, umidità e co2. Di seguito si trovano tutte queste e la logica di come si passa da una all’altra..

|  |
| --- |
| 14 Schermate CoreS3 |

### NanoC6

I microcontrollori M5Stack NanoC6 sono delle versioni in miniatura del CoreS3, con meno funzionalità, perciò questi hanno il compito di raccogliere i dati dai sensori o dagli input e trasmetterli al CoreS3, oppure di ricevere dati da esso e decidere in base a questi se accendere un LED o se aspettarsi un input dalla tastiera.

|  |
| --- |
| M5Stack M5STACK M5NanoC6 Scheda di sviluppo IoT ESP32-C6 WiFi-6 Matte Three  Zigbee RISC-V 160 MHz : Amazon.it: Videogiochi  15 M5Stack NanoC6 |

### Architettura implementata

Mentre ho imparato ad usare le componenti M5Stack, mi sono accorto che gli hub che ho comandato non sono adatti al mio caso d’uso, in quanto ripetono semplicemente il segnale in entrata e non è possibile gestire le porte. Per questo motivo ho dovuto modificare la mia architettura dei sensori e microcontrollori. Dopo una ricerca approfondita sugli hub disponibili (in realtà degli switch, ma la nomenclatura di M5Stack li chiama così) ho scoperto che non esistono di tipo misto, perciò che combina I2C (porta A, rossa) e generic I/O (porta B, nera), in modo da collegare sia un LED che un sensore alla stesa porta di un NanoC6. Per questo motivo, e per non fare un’altra comanda, ho deciso di modificare l’architettura in modo da non utilizzare più hub ma collegare direttamente un LED e un sensore al CoreS3 e collegare gli altri componenti direttamente ad un NanoC6. Da questo cambiamento risulta il seguente schema.

|  |
| --- |
| 16 Architettura M5Stack implementata |

### Registrazione badge

Per registrare meglio gli accessi nella sala server, è necessario sapere chi è entrato e quando. L’informazione di chi è entrato viene recuperata tramite il badge della scuola, sul quale è salvata una stringa esadecimale univoca. Essa deve però essere associata ad un nome utente per generare del valore aggiuntivo, perciò risulta necessario salvare questo link tra badge e utente nel database. Questo processo viene spiegato nello schema sottostante, infatti un utente docente o sistemista, quando accede alla dashboard, riceve un codice di registrazione, con il quale si deve recare nella sala server e immetterlo nella tastiera e posizionare il badge sul sensore RFID. Quando un utente immette dei valori dalla tastiera e mette il badge sul sensore, il CoreS3 manda una richiesta al backend per capire se questo utente ha già effettuato il link tra badge e username. Se questo è il caso viene registrato come accesso, altrimenti viene effettuato il link nel database e viene registrato automaticamente un accesso con motivo di registrazione badge.

|  |
| --- |
| 17 Schema funzionamento badge |

|  |
| --- |
| 18 Interfaccia registrazione badge, con istruzioni |

### Accesso

Una delle principali funzionalità è quella di monitorare gli accessi alla sala server. Per fare ciò viene utilizzata una combinazione di sensori (PIR, RFID e MiniKB). Il sensore di movimento a infrarossi (PIR) percepisce un movimento di una persona che entra dalla porta, e da questo momento essa ha 60 secondi di tempo per appoggiare il proprio badge sul lettore RFID e inserire il motivo della loro presenza tramite la mini tastiera (1: Maintenance, 2: Inspection, 3: Testing, 4: Emergency, tutti gli altri tasti: Other) e premere invio per confermare. Con questo l’accesso è stato registrato come autorizzato, con il motivo, il nome dell’utente e il timestamp nel database. Se dopo 60 secondi queste azioni non sono avvenute, il sistema registra un accesso non autorizzato. Quando l’utente intende uscire, deve premere il tasto “e”, per dire al microcontrollore che l’utente ora sta uscendo. Dopodiché potrà essere registrato un nuovo accesso.

### Comunicazione wireless

Per fare comunicare i microcontrollori NanoC6 con il microcontrollore CoreS3, ho optato per il protocollo ESPnow, creato da Espressif, che permette di fare delle comunicazioni point to point (unicast) tramite i mac address dei dispositivi. Inoltre è molto interessante per IoT a causa del suo basso consumo di energia e di una bassa latenza. Inoltre ha il vantaggio che non dipende da una connessione Wi-Fi, che potrebbe non essere disponibile a causa di problemi tecnici, e perciò anche la comunicazione dei microcontrollori andrebbe a cadere.

Invece la comunicazione del CoreS3 con il backend dell’applicativo, tramite API REST, viene eseguita tramite il Wi-Fi della rete nera, più preciso BLACKNET-DEVICES.

### Sensori

Per poter implementare le funzionalità richieste, sono necessari alcuni sensori e input per rilevare i dati necessari nella sala server. Di seguito sono elencati i sensori M5Stack utilizzati, con i dati interessanti per il mio progetto che rilevano:

* ENV III 🡪 dati di temperatura e umidità
* PIR 🡪 rileva raggi infrarossi riflessi dagli umani, sensore di movimento
* RGB LED 🡪 3 led configurabili con tutti i colori rgb
* RFID 🡪 rileva le informazioni del badge
* CardKeyBoard 🡪 mini tastiera per inserire codice di registrazione badge e inserimento motivo acceso
* Tvoc/eCo2 🡪 valore del co2 nell’aria

### Montaggio sistema

Di seguito viene riportato come e perché sono stati montati i componenti hardware nella sala server.

# Test

## Protocollo di test

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-001  REQ-001 | **Nome:** | Verifica installazione sensori e componenti |
| **Descrizione:** | Verificare che tutti i sensori, cavi e controller siano montati correttamente nella sala server. | | |
| **Prerequisiti:** | Recarsi nella sala server. | | |
| **Procedura:** | 1. Controllare la presenza di tutti i componenti hardware richiesti. 2. Verificare il corretto montaggio dei sensori, cavi e controller nella sala server. | | |
| **Risultati attesi:** | Tutti i componenti sono installati correttamente e funzionanti. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-002  REQ-004 | **Nome:** | Accesso Dashboard docente/sistemista |
| **Descrizione:** | Accedere alla dashboard di watchtower come docente o sistemista, perciò un utente con permessi elevati. | | |
| **Prerequisiti:** | - | | |
| **Procedura:** | 1. Aprire <http://watchtower.caprover.samt.local/login> 2. Effettuare il login con username: sistemista1 e password: Password&1 | | |
| **Risultati attesi:** | Login effettuato, nella navbar ci sono le tab per accessi e notifiche e in basso a sinistra sotto all’utente si vede la scritta “docente” rispettivamente “sistemista”. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-003  REQ-004 | **Nome:** | Accesso Dashboard allievo |
| **Descrizione:** | Accedere alla dashboard di watchtower come allievo, perciò un utente con permessi ridotti. | | |
| **Prerequisiti:** | - | | |
| **Procedura:** | 1. Aprire <http://watchtower.caprover.samt.local/login> 2. Effettuare il login con username: allievo2 e password: Password&1 | | |
| **Risultati attesi:** | Login effettuato, nella navbar ci sono solo i tab per navigare ai grafici di temperatura, co2 e umidità e in basso a sinistra sotto all’utente si vede la scritta “allievo”. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-004  REQ-004 | **Nome:** | Dashboard grafici temperatura ultima ora |
| **Descrizione:** | Visualizzare i dati dell’ultima ora in un grafico riguardo alla temperatura (o co2 o umidità). | | |
| **Prerequisiti:** | Avere effettuato l’accesso. | | |
| **Procedura:** | 1. Navigare alla pagina di temperatura (/temperature) | | |
| **Risultati attesi:** | Si vede un grafico con i dati di temperatura dell’ultima ora, sempre con 5 minuti di distacco. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-005  REQ-004 | **Nome:** | Dashboard grafici temperatura ultimo giorno |
| **Descrizione:** | Visualizzare i dati dell’ultima ora in un grafico riguardo alla temperatura (o co2 o umidità). | | |
| **Prerequisiti:** | Avere effettuato l’accesso. | | |
| **Procedura:** | 1. Navigare alla pagina di temperatura (/temperature) 2. Cambiare grafico in last day | | |
| **Risultati attesi:** | Si vede un grafico con i dati di temperatura delle ultime 24 ore. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-006  REQ-004 | **Nome:** | Dashboard grafici temperatura ultima settimana |
| **Descrizione:** | Visualizzare i dati dell’ultima ora in un grafico riguardo alla temperatura (o co2 o umidità). | | |
| **Prerequisiti:** | Avere effettuato l’accesso. | | |
| **Procedura:** | 1. Navigare alla pagina di temperatura (/temperature) 2. Cambiare grafico in last week | | |
| **Risultati attesi:** | Si vede un grafico con i dati di temperatura massima di ogni giorno negli scorsi sette giorni. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-007  REQ-004 | **Nome:** | Dashboard grafico accessi |
| **Descrizione:** | Visualizzare il numero di accessi alla sala server. | | |
| **Prerequisiti:** | Avere effettuato l’accesso come docente/sistemista e avere effettuato un accesso fisico alla sala server da quando il sistema di monitoraggio è in uso. | | |
| **Procedura:** | 1. Navigare alla pagina degli accessi (/access) | | |
| **Risultati attesi:** | Si vede un grafico con i dati degli accessi nell’ultima settimana, divisi in autorizzati e non. Sotto a questo grafico si vedono inoltre gli ultimi 10 accessi effettuati, con nome, data e motivazione. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-008  REQ-004 | **Nome:** | Dashboard notifiche |
| **Descrizione:** | Visualizzare le notifiche generate dall’applicativo in base ai dati ricevuti dal microcontrollore. | | |
| **Prerequisiti:** | Avere effettuato l’accesso come docente/sistemista e generare un’anomalia nei dati, per esempio effettuare un accesso non autorizzato. | | |
| **Procedura:** | 1. Navigare alla pagina delle notifiche (/notifications) | | |
| **Risultati attesi:** | Si vede una lista di notifiche, divise per categoria e per gravità. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-009  REQ-004 | **Nome:** | Dashboard impostare limite notifiche |
| **Descrizione:** | Modificare i valori di soglia per le notifiche. | | |
| **Prerequisiti:** | Avere effettuato l’accesso come docente/sistemista e recarsi nella pagina delle notifiche. | | |
| **Procedura:** | 1. Premere sul pulsante delle impostazioni. 2. Modificare un qualche valore. 3. Salvare. | | |
| **Risultati attesi:** | Se si preme nuovamente sul pulsante, il nuovo valore è stato salvato e ora le notifiche verranno generato in base a questo nuovo dato. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-010  REQ-004 | **Nome:** | Registrazione badge |
| **Descrizione:** | Associare il proprio badge scolastico al proprio utente. | | |
| **Prerequisiti:** | Avere effettuato l’accesso come docente/sistemista e avere il badge scolastico. | | |
| **Procedura:** | 1. Premere sulla card nella home in cui viene richiesto di eseguire un’azione con il badge. 2. Memorizzare il numero scritto. 3. Recarsi in sala server e mettere il badge sul lettore RFID. 4. Inserire il codice memorizzato tramite la tastiera 5. Uscire | | |
| **Risultati attesi:** | Se si torna sull’applicativo e si fa un refresh, la card dovrebbe essere scomparsa e l’utente è collegato al proprio badge. Inoltre sulla schermata del microcontrollore appare un messaggio di successo di associazione tra badge e utente. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-011  REQ-004 | **Nome:** | Dashboard risolvi notifiche |
| **Descrizione:** | Marcare una notifica come risolta, così che non si più visualizzata. | | |
| **Prerequisiti:** | Avere effettuato l’accesso come docente/sistemista e avere una notifica nella pagina. | | |
| **Procedura:** | 1. Navigare alla pagina delle notifiche (/notifications) 2. Premere su una notifica 3. Premere Resolved 4. Confermare | | |
| **Risultati attesi:** | La notifica non è più visibile. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-012  REQ-004 | **Nome:** | Dashboard risolvi tutte notifiche |
| **Descrizione:** | Marcare tette le proprie notifiche come risolte, così che non vengono più visualizzate. | | |
| **Prerequisiti:** | Avere effettuato l’accesso come docente/sistemista e avere almeno una notifica nella pagina. | | |
| **Procedura:** | 1. Navigare alla pagina delle notifiche (/notifications) 2. Premere su Resolve All 3. Confermare | | |
| **Risultati attesi:** | Non ci sono più notifiche nella pagina. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-013  REQ-005 | **Nome:** | Email di notifica |
| **Descrizione:** | Quando viene generato una notifica di livello alto, viene inviata una notifica email a docenti e sistemisti. | | |
| **Prerequisiti:** | Avere un utente con email nel LDAP. | | |
| **Procedura:** | 1. Generare un’allerta di livello alto (accesso non autorizzato) 2. Andare nella propria casella postale. | | |
| **Risultati attesi:** | C’è un’email inviata da WatchTower di allerta | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-014  REQ-002 | **Nome:** | Raccolta temperatura e umidità |
| **Descrizione:** | Il sensore ENV III raccoglie i dati ambientali ogni 5 minuti e li trasmette al microcontrollore, che li mostra e li manda al backend. | | |
| **Prerequisiti:** | Avere i sensori e microcontrollori montati e accesi, aver effettuato l’acceso tramite badge e tastiera. | | |
| **Procedura:** | 1. Apettare finchè il microcontrollore mostri I dati di temperature e umidità. | | |
| **Risultati attesi:** | Temperatura e umidità mostrati sullo schermo. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-015  REQ-002 | **Nome:** | Raccolta valore Co2 e accensione LED |
| **Descrizione:** | Il sensore di Co2 raccoglie i dati rilevanti e ogni 5 minuti e li trasmette al microcontrollore, che li mostra e li manda al backend e accende un LED in base al valore. | | |
| **Prerequisiti:** | Avere i sensori e microcontrollori montati e accesi, aver effettuato l’acceso tramite badge e tastiera. | | |
| **Procedura:** | 1. Apettare finchè il microcontrollore mostri il dato di co2 e accenda il LED. | | |
| **Risultati attesi:** | LED acceso (verde, arancione o roso) e valore Co2 scritto sullo schermo. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-016  REQ-002 | **Nome:** | Rilevamento accesso consentito |
| **Descrizione:** | Il sistema registra gli accessi consentiti alla sala server, con nome, motivo e data. | | |
| **Prerequisiti:** | Avere i sensori e microcontrollori montati e accesi. | | |
| **Procedura:** | 1. Entrare in sala server 2. Posizionare il badge sul sensore RFID 3. Immettere il motivo di accesso tramite la tastiera (istruzioni sullo schermetto) | | |
| **Risultati attesi:** | Schermata di successo e registrazione accesso. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case:**  **Riferimento**: | TC-017  REQ-002 | **Nome:** | Rilevamento accesso non consentito |
| **Descrizione:** | Il sistema registra gli accessi non consentiti alla sala server con la data dell’avvenimento. | | |
| **Prerequisiti:** | Avere i sensori e microcontrollori montati e accesi. | | |
| **Procedura:** | 1. Entrare in sala server 2. Aspettare un minute finché lo schermo mostra il fallimento di autenticazione | | |
| **Risultati attesi:** | Schermata di fallimento e registrazione accesso. | | |

## Risultati test

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Case** | **Risultato** | **Data** | **Stato** |
| TC-001 |  |  |  |
| TC-002 | Premere su Log In, per passare alla schermata di home.  Utente del gruppo sistemista: | 20.03.2025 | Passato |
| TC-003 | Premere su Log In, per passare alla schermata di home.  Utente del gruppo allievi: | 20.03.2025 | Passato |
| TC-004 |  | 20.03.2025 | Passato |
| TC-005 |  | 20.03.2025 | Passato |
| TC-006 |  | 20.03.2025 | Passato |
| TC-007 | Grafico:    Tabella: | 20.03.2025 | Passato |
| TC-008 |  | 20.03.2025 | Passato |
| TC-009 | Premere il pulsante settings e modificare un valore.    Salvare. | 20.03.2025 | Passato |
| TC-010 | Premere sulla seguente card:    Prendere il codice dal dialog:    Appoggiare il badge sul sensore:  C:\Users\tom.schillerwein\Downloads\1000017329.jpg  Viene mostrata la seguente schermata sul microcontrollore:  C:\Users\tom.schillerwein\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\otp_screen.jpeg  Inserire il codice e premere invio, ora vien mostrata la seguente schermata:  C:\Users\tom.schillerwein\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\TempState\ShareServiceTempFolder\success_screen.jpeg  Anche nell’applicativo la card con il codice è scomparsa. | 20.03.2025 | Passato |
| TC-011 | Premere Resolved. La notifica è rimossa dalla lista. | 20.03.2025 | Passato |
| TC-012 | Premere Resolve All e confermare.  Tutte le notifiche sono rimosse. | 20.03.2025 | Passato |
| TC-013 | Dopo aver generato un accesso non autorizzato, ho ricevuto la seguente email: | 20.03.2025 | Passato |
| TC-014 | C:\Users\tom.schillerwein\Downloads\20250320_113141.jpg  Sensore Co2  Valore Co2  Led Co2 | 20.03.2025 | Passato |
| TC-015 | C:\Users\tom.schillerwein\Downloads\20250320_113258.jpg  Sensore ENV III  Valori temperatura e umidità | 20.03.2025 | Passato |
| TC-016 | Entrare nella sala server.  C:\Users\tom.schillerwein\Downloads\20250320_114316.jpg  Sensore PIR (movimento)  Sensore RFID  Mini Tastiera  Posizionare il badge sul sensore.  C:\Users\tom.schillerwein\Downloads\20250320_114323.jpg  Inserire il motivo.  C:\Users\tom.schillerwein\Downloads\20250320_114444.jpg  Accesso eseguito con successo. | 20.03.2025 | Passato |
| TC-017 | Entrare in sala server.  C:\Users\tom.schillerwein\Downloads\20250320_114316.jpg  Dopo 1 minuto:  C:\Users\tom.schillerwein\Downloads\20250320_114523.jpg  Accesso non autorizzato rilevato. | 20.03.2025 | Passato |

## Mancanze/limitazioni conosciute

Descrizione con motivazione di eventuali elementi mancanti o non completamente implementati, al di fuori dei test case. Non devono essere riportati gli errori e i problemi riscontrati e poi risolti durante il progetto.

# Consuntivo

Consuntivo del tempo di lavoro effettivo e considerazioni riguardo le differenze rispetto alla pianificazione (cap. 1.7) (ad esempio Gantt consuntivo).

# Conclusioni

Quali sono le implicazioni della mia soluzione? Che impatto avrà? Cambierà il mondo? È un successo importante? È solo un’aggiunta marginale o è semplicemente servita per scoprire che questo percorso è stato una perdita di tempo? I risultati ottenuti sono generali, facilmente generalizzabili o sono specifici di un caso particolare? ecc.

## Sviluppi futuri

Migliorie o estensioni che possono essere sviluppate sul prodotto.

## Considerazioni personali

Cosa ho imparato in questo progetto? ecc.

# Glossario

|  |  |
| --- | --- |
| **Termine** | **Descrizione** |
| LDAP | **Lightweight Directory Access Protocol** : **protocollo** di rete per l'accesso e la gestione di directory distribuite su una rete. Viene utilizzato principalmente per autenticare utenti e gestire informazioni in organizzazioni, come liste di utenti, gruppi e permessi. |
| JWT | **JSON Web Token**: standard web per lo scambio di dati definito dalla RFC 7519 proposto nel 2015. |
| Vue JS | **Vue.js:** un framework JavaScript open-source per la costruzione di interfacce utente e applicazioni web |
| Tailwind CSS | **Tailwind CSS:** framework CSS open source usato per applicare velocemnte uno stile alle pagine HTML. |
| Shadcn Vue | **Shadcn Vue**: libreria di componenti grafici che utilizza vue e Tailwind per creare componenti grafici accattivanti. |
| Node.js | **Node.js**: Ambiente di runtime JavaScript, progettato per eseguire codice JavaScript lato server in modo asincrono e ad alte prestazioni. |
| Express | **Express**: Framework web minimalista per Node.js che semplifica la creazione di API e applicazioni web, fornendo un sistema di routing e middleware flessibile. |
| API | **Application Programming Interface**: insieme di strumenti e procedure che consentono a diversi software di comunicare tra loro. |
| I²C | **Inter Integrated Circuit**: sistema di comunicazione seriale bifilare utilizzato tra [circuiti integrati](https://it.wikipedia.org/wiki/Circuito_integrato). Il classico bus I²C è composto da almeno un master ed uno slave. |

# Bibliografia

## Bibliografia per articoli di riviste:

1. Cognome e nome (o iniziali) dell’autore o degli autori, o nome dell’organizzazione,
2. Titolo dell’articolo (tra virgolette),
3. Titolo della rivista (in italico),
4. Anno e numero
5. Pagina iniziale dell’articolo.

## Bibliografia per libri

1. Cognome e nome (o iniziali) dell’autore o degli autori, o nome dell’organizzazione,
2. Titolo del libro (in italico),
3. ev. Numero di edizione,
4. Nome dell’editore,
5. Anno di pubblicazione,
6. ISBN.

## Sitografia

1. URL del sito (se troppo lungo solo dominio, evt completo nel diario),
2. Eventuale titolo della pagina (in italico),
3. Data di consultazione (GG-MM-AAAA).

**Esempio:**

* http://standards.ieee.org/guides/style/section7.html, *IEEE Standards Style Manual*, 07-06-2008.

# Allegati

* Diari di lavoro
* Applicativo
* Quaderno dei compiti
* Abstract
* Gantt
* Use Case
* …

# Indice delle Figure

[1 Use Case 6](#_Toc192430133)

[2 Diagramma di Gantt preventivo 6](#_Toc192430134)

[3 Schema Microcontrollore e Sensori 8](#_Toc192430135)

[4 Architettura sistema 8](#_Toc192430136)

[5 Diagramma ER 9](#_Toc192430137)

[6 Struttura interfacce 9](#_Toc192430138)

[7 Protocollo LDAP 10](#_Toc192430139)

[8 Struttura cartelle frontend 12](#_Toc192430140)

[9 Pagina Home 13](#_Toc192430141)

[10 Pagina Temperatura 13](#_Toc192430142)

[11 Struttura cartelle backend 14](#_Toc192430143)

[12 M5burner esempio firmware per CoreS3 16](#_Toc192430144)

[13 M5Stack CoreS3 17](#_Toc192430145)

[14 M5Stack NanoC6 17](#_Toc192430146)

[15 Architettura M5Stack implementata 18](#_Toc192430147)

[16 Schema funzionamento badge 19](#_Toc192430148)

[17 Interfaccia registrazione badge, con istruzioni 19](#_Toc192430149)