FACULTAD
DE INGENIERIA
Universidad de Buenos Aires

CARRERA DE ESPECIALIZACIÓN EN
INTERNET DE LAS COSAS

MEMORIA DEL TRABAJO FINAL

Sistema de gestión de alertas y tareas de procesos de planta - Control de acceso

Autor:
Lionel Gutierrez

Director:
Gustavo Ramoscelli (UNS)

Jurados:
José Alamos (pertenencia)
Leandro Lanzieri Rodriguez (pertenencia)
Leopoldo Zimperz (pertenencia)

Este trabajo fue realizado en la ciudad de Villa Mercedes,
entre marzo de 2020 y marzo de 2021.

Resumen

La presente memoria describe el diseño e implementación de un sistema de control de acceso de personal de terceros a una locación industrial. El sistema garantiza que solo aquellas personas que tienen en regla los requisitos legales y médicos solicitados accedan, evitando que la empresa sea responsable ante posibles accidentes o incidentes de dicho personal. El trabajo desarrollado es la primera etapa de un proyecto integral de gestión de alertas y procesos para la empresa Tenaris Metalmecánica, sobre el cual se agregarán a futuro nuevos casos de uso.

Para la elaboración del trabajo se aplicaron conocimientos adquiridos a lo largo de la carrera, principalmente los referidos a gestión de proyectos, desarrollo de aplicaciones web y multiplataforma, protocolos de Internet y seguridad en IoT. Además, se integraron tecnologías de base de datos relacionales y no relacionales y se aplicaron varias técnicas de testing.

Agradecimientos

AGREGAR AGRADECIMIENTO

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción general

Poner párrafo introductorio.

1.1. Estado del arte

Introducción, propósito y estado del arte de IoT y solución propuesta.

1.1.1. Tecnología IoT

Introducción a las soluciones IoT, posibilidades que brinda para sensado y control de diferentes procesos, ventajas de la tecnología (economía, simplicidad).

1.1.2. Control de acceso

Sistemas de control de acceso que existen en el mercado. Diferencias con el sistema propuesto (valor agregado de la propuesta contra soluciones existentes).

1.2. Motivación

Razones por el cual se desea desarrollar el sistema. Justificaciones. Necesidad del cliente.

1.3. Objetivos y alcance

Objetivos y alcance del trabajo.

Capítulo 2

Introducción específica

Poner párrafo introductorio.

2.1. Protocolos de comunicación

Descripción de los protocolo de comunicación (Wi-Fi/HTTP) utilizados para IoT.

2.1.1. Tecnología de comunicación Wi-Fi

Descripción de tecnología Wi-Fi.

2.1.2. Protoclo HTTP

Descripción de protocolo HTTP.

2.2. Componentes de Hardware utilizado

Descripción de los componentes de hardware utilizados: ESP32, lector de tarjetas, cerradura electrónica.

2.2.1. Módulo ESP32

Descripción del módulo.

2.2.2. Módulo RFID RC522

Descripción del módulo.

2.2.3. Cerradura electrónica

Descripción de cerradura.

2.3. Tecnologías de Software aplicadas

Descripción de las tecnologías de software utilizadas.

2.3.1. Node.JS

2.3.2. Ionic

2.3.3. PostgreSQL

2.3.4. MongoDB

2.3.5. Docker

2.3.6. Postman

2.4. Software de control de versiones

Descripción del software de control de versiones.

2.4.1. GitFlow

Descripción de la herramienta.

2.5. Requerimientos

Requerimientos del proyecto, tanto funcionales, no funcionales, de documentación y de validación. Enumeración de los mismos.

2.5.1. Requerimientos funcionales

2.5.2. Requerimientos no funcionales

2.5.3. Requerimientos de documentación

2.5.4. Requerimientos de validación

Capítulo 3

Diseño e implementación

Poner párrafo introductorio.

3.1. Arquitectura del sistema/módulos

Arquitectura del sistema. Separación en módulos/subsistemas. Protocolos de comunicación entre los módulos y escalabilidad.

3.2. Detalle de módulos de Hardware

Detalle de los módulos del sistema y protocolos utilizados para la comunicación entre los mismos.

3.2.1. Módulo sensor

Detalle de implementación del módulo de sensado/ingreso.

3.2.2. Módulo actuador

Detalle de implementación del módulo de actuación.

3.3. Detalle de módulos de Software

3.3.1. Módulo de Backend

Detalle de implementación backend del sistema. Explicar por un lado la API Rest del sistema y el detalle de implementación del middleware de autenticación (API de autenticación).

3.3.2. Módulo de Frontend

Detalle de implementación frontend del sistema.

3.4. Interfaz con sistema de documentación

Detalle de interfaz con sistema de documentación. Mock implementado para testeo integral del sistema.

Capítulo 4

Ensayos y Resultados

Poner párrafo introductorio.

4.1. Detalle de pruebas realizadas

Detalle de las pruebas realizadas, herramientas utilizadas para el testing. módulos mockeados.

4.2. Pruebas unitarias

Detalle de pruebas unitarias realizadas sobre los diferentes módulos del sistema.

4.2.1. Testing del módulo sensor

Detalles de pruebas del módulo sensor.

4.2.2. Testing del módulo actuador

Detalle de pruebas del módulo actuador.

4.2.3. Testing del módulo de Backend

Detalle de pruebas del backend del sistema. Esto incluye la API Rest expuesta por el mismo y la API de autenticación.

4.3. Pruebas de sistema

Detalle de prueba integral y de sistema.

4.4. Pruebas de aceptación

Pruebas de aceptación con cliente.

4.4.1. Descripción y detalles de prueba de ingreso habilitado

Detalle de la prueba con ingreso OK de usuario, ejemplo de caso de uso completo del sistema.

4.4.2. Descripción y detalles de prueba de ingreso inhabilitado

Detalle de la prueba con ingreso NO OK de usuario, ejemplo de caso de uso completo del sistema.

Capítulo 5

Conclusiones

5.1. Resultados obtenidos

Se logró cumplir el alcance y objetivo del proyecto. En primer lugar, se implementó el sistema de control solicitado, incluyendo los módulos de sensado y actuación y la aplicación web de gestión de control y alertas. En segundo lugar, se sentaron las bases para el agregado de futuros casos de uso, para lo cual se hizo un diseño modular. Esto permitirá al sistema el sensado de datos de nuevos procesos de planta, según el requerimiento 1.1, especificado en la sección 2.5.

Adicionalmente, se pudo incorporar al sistema un módulo para gestionar la autenticación y autorización de los usuarios y el acceso a la API Rest del Backend del sistema de modo seguro. Esto posibilitó cumplir con el requerimiento 1.6, que fue agregado al trabajo durante su desarrollo. Este requerimiento permite independizar al sistema desarrollado del sistema de autenticación de la empresa y lograr una mayor portabilidad, lo que da la posibilidad a futuro de expandir el mismo a otras empresas.

Finalmente, el trabajo cumplió con el requerimiento de lograr una gestión efectiva de los terceros con un control rígido para su acceso, al sistematizar la gestión del acondicionamiento de la documentación. Si bien existen otros sistemas de control de ingreso en el mercado, se logró agregar valor mediante la comunicación del sistema en cuestión con el sistema de control de documentación de terceros y con los procesos de alerta y gestión implementados. El trabajo realizado habilita una gestión proactiva, rápida y ordenada de los terceros, de forma de actuar inmediatamente ante problemas de ingresos. Las ventajas obtenidas incluyen:

- Reducir tiempo para la gestión.
- Evitar atrasos en ingresos por falta de ajustes en la documentación.
- Evitar problemas legales ante incidentes del personal externo.
- Evitar el uso de papel y herramientas des-centralizadas para el control y gestión de los terceros por parte de cada sector de la empresa.

Si bien todavía el sistema no se implementó en operativo, con las pruebas realizadas y analizando los ingresos de personal en los últimos dos años, se prevé evitar un 5 % de ingresos incorrectos o con problemas, y reducir los tiempos ante inconvenientes con la documentación en unas 10 horas hombre/mes.

En la tabla 5.1 se muestra la comparación entre el sistema implementado y soluciones similares del mercado, en la que se puede apreciar el diferencial del sistema desarrollado.

TABLA 5.1. Comparación contra otras soluciones similares del mercado.

Característica	Sistema	Pronext KY800	Samsung H505
Log de ingresos	Si	Si	No
Interfaz a sistemas externos	Si	No	No
Gestión integral de accesos	Si	No	No
Máximo usuarios	Indefinido	500	30
Conectividad/Protocolos	Wi-Fi	Bluetooth	No
Doble factor autenticación	No	No	Si
Tarjetas RFID	Si	Si	Si
Alerta de acceso	Si	Si	Si
Acceso con huella	No	Si	No

Cabe destacar la importancia de los conocimientos obtenidos a lo largo de la carrera. En primer lugar, fueron muy importantes los aportes de la asignatura de gestión de proyectos. Una buena gestión de proyectos fue fundamental, tanto para lograr una planificación clara que actúe como guía a lo largo de todo el desarrollo, como para minimizar riesgos. En lo particular del trabajo, luego del comienzo del desarrollo se agregó un nuevo requerimiento al mismo. Teniendo el diagrama de Gantt [1] armado, y en función del nuevo requerimiento y el avance real al momento de la solicitud, se pudo estimar el esfuerzo necesario y determinar que se podía incluir en el plan, dado que los plazos eran suficientes para poder cumplir con la fecha de finalización. Sin una gestión de proyectos clara, es muy probable que este nuevo requerimiento haya sido rechazado.

Adicionalmente, los conocimientos en desarrollo de aplicaciones multiplataforma permitieron plantear una solución que sea *web responsive* y que a futuro se puede implementar en un entorno mobile con mínimo esfuerzo. También se abre la posibilidad de implementar el sistema en la nube.

Por último, es importante mencionar que no se cumplió ninguno de los riesgos identificados durante la planificación, con lo cual no fue necesario aplicar el plan de mitigación. No obstante, el análisis y planificación temprana de los riesgos fue fundamental para hacer un seguimiento periódico, evitando que los mismos sucedan. Sin una correcta gestión y planificación, varios de los riesgos se podrían haber vuelto severos, impactando en los tiempos y recursos necesarios para completar el trabajo a término.

5.2. Trabajo futuro

Para la continuidad y mejora de este trabajo se plantean dos líneas de acción.

En primer lugar, una línea de mejora del trabajo actual dentro de la que se incluyen:

- Realizar mejoras en seguridad:

    - Agregar comunicación HTTPS entre los diferentes módulos del sistema. De este modo, se asegura que la información viaje encriptada y se evitan ataques del tipo *man in the middle*. Esto permitirá migrar el sistema a la nube, donde las comunicaciones viajan entren varios sistemas abiertos, a través de Internet, y no quedan confinados al ámbito de una red interna o Intranet de una empresa.
    - Agregar un segundo factor de autenticación al sistema. Con el objetivo de evitar que ante pérdidas o robos de la tarjeta RFID de ingreso o duplicación de la misma un atacante pueda ingresar a planta, se plantea la posibilidad de agregar un teclado matricial de forma de requerir además de la tarjeta una clave numérica durante el proceso de ingreso.

- Automatizar tareas de configuración: se analiza implementar una aplicación para poder configurar las acciones del sistema ante las diferentes variantes de entradas (ingreso correcto, ingreso de usuario inactivo, ingreso con documentación vencida). Actualmente esta información se guarda y administra en una base de datos no relacional, por parte del personal de sistemas, que permite definir para cada tipo y valor de entrada un conjunto de acciones de salidas (tareas de control, alertas, emails). Se evalúa desarrollar una aplicación para que el usuario pueda configurar estas salidas y generar diferentes tipos de acción, independizándose del área de sistemas.
- Realizar una prueba de implementación en la nube: utilizar la nube de Azure para probar y asegurar el escalamiento de la solución. Esto permitirá incluir nuevas locaciones o plantas industriales al trabajo, ya sea dentro de la empresa actual o para ser implementado en nuevas empresas.

En segundo lugar, en el marco del proyecto integral de gestión de alertas y procesos, el objetivo es incorporar nuevos procesos y casos de uso al sistema. De hecho, ya fue solicitado un primer caso de uso por parte del laboratorio de metrología de la empresa. El mismo implica el control de temperatura y humedad de dicho laboratorio, para asegurar que ambas variables se encuentren dentro de los límites requeridos y generar alertas en caso de desvíos para poder actuar en consecuencia, manual o automáticamente.

Bibliografía

[1] Wikipedia. *Diagrama de Gantt*. https://es.wikipedia.org/wiki/Diagrama_de_Gantt. Oct. de 2020. (Visitado 07-03-2021).