v. 5, n. 7, 2025

Journal of
Engineering
Research

SAFELAB: A TECHNOLOGICAL PROPOSAL TO IMPROVE SAFETY THROUGH GAS DETECTION IN EDUCATIONAL LABORATORIES

Acceptance date: 18/08/2025
Date of submission: 11/07/2025

Caritina Ávila López
National Technological Institute of Mexico/
Aguascalientes Technological Institute
Aguascalientes – Mexico
https://orcid.org/0009-0008-5538-4095

Marco Antonio Hernández-Vargas
National Technological Institute of Mexico/
Aguascalientes Technological Institute
Aguascalientes, Mexico
https://orcid.org/0000-0002-8146-9307

José Alejandro-Gutiérrez Rodríguez
Student at the National Technological
Institute of Mexico/Technological Institute of
Aguascalientes
Aguascalientes, Mexico

Fernando Robles Casillas
National Technological Institute of Mexico/
Technological Institute of Aguascalientes
Aguascalientes, Mexico
https://orcid.org/0000-0002-0769-440X

María Magdalena-Becerra López
National Technological Institute of Mexico/
Technological Institute of Aguascalientes
Aguascalientes, Mexico

DOI https://doi.org/10.22533/at.ed.317572517077

Alfonso-Recio Hernández
National Technological Institute of Mexico/
Technological Institute of Aguascalientes
Aguascalientes, Mexico

Rocío-García Obregón
National Technological Institute of Mexico/
Technological Institute of Aguascalientes
Aguascalientes – Mexico

Javier Mascorro Pantoja
National Technological Institute of Mexico/
Technological Institute of Aguascalientes
Aguascalientes, Mexico

Mónica Lucia-Vera Medina
Student at the National Technological
Institute of Mexico/Technological Institute of
Aguascalientes
Aguascalientes, Mexico

Abstract: Chemical engineering students at the National Technological Institute of Mexico, Aguascalientes Technological Institute Campus, particularly those who do internships in the Industrial Analysis laboratory, face an opportunity to incorporate Information and Communication Technologies (ICT) to strengthen safety in experimental environments. In response to this need, **SAFELAB** was developed**,** a Comprehensive Real-Time Monitoring System based on a scalable software architecture, whose objective is to significantly improve safety conditions through the early detection of toxic gases and the implementation of preventive and corrective measures. The project was organized in three stages: (1) analysis of the gases used in the laboratory to determine their hazardousness and select the appropriate sensors; (2) design and implementation of an Internet of Things (IoT) prototype to monitor air quality in real time; and (3) development of a mobile application capable of issuing immediate alerts in case of dangerous concentrations. The results were satisfactory: the system demonstrated its ability to identify the presence of harmful gases and issue effective notifications to the user via their mobile device. The proposal represents a scalable, economical, and functional technological solution for educational laboratories that handle hazardous substances.

Keywords: Internet of Things, harmful gas detection, sensors, chemical reagents, information and communication technologies.

INTRODUCTION

Higher education has undergone a significant transformation in recent decades, driven by advances in information and communication technologies (ICT) and the Internet of Things (IoT). This evolution has impacted not only teaching methods, but also practical training environments, such as scientific laboratories, where technological integration offers advantages in terms of efficiency, accuracy, and safety. In particular, chemistry laboratories—where potentially hazardous substances are handled—require the implementation of technologies that ensure safe conditions for students and teachers.

The main objective of this research project is to improve safety in the chemistry laboratories of the Aguascalientes Institute of Technology, especially those used by chemical engineering students. To this end, a Real-Time Monitoring System based on a Scalable Software Architecture (SAFELAB) was designed and implemented, which combines low-cost hardware (such as sensors connected to Arduino boards) with cloud software (Firebase), allowing the detection of dangerous gases and generating immediate alerts through a mobile application.

This article describes the design, implementation, and validation of the SAFELAB system. The results section presents the graphs obtained during controlled tests, which verified the effectiveness of the system in detecting gas releases and generating timely alerts. Finally, conclusions are presented and the implications of this technological solution in educational and industrial safety contexts are discussed.

THEORETICAL BACKGROUND

Emerging technologies in educational environments. The development of emerging technologies has profoundly transformed educational processes in recent decades. These technologies, still in the process of consolidation, have a high disruptive potential by introducing new forms of interaction, automation, and access to knowledge. According to Crawford et al. (2024), emerging technologies are "technological innovations with the potential to change teaching and learning methods, but which are not yet fully integrated" (p. 4).

In contexts where a combination of theory and experimentation is required, such as chemical engineering, emerging technologies can enhance both the safety and effectiveness of practices.

The Internet of Things (IoT) and its application in laboratories. One of the emerging technologies with the greatest impact in recent years is the Internet of Things (IoT), which allows physical objects to be interconnected through sensors, microcontrollers, and communication networks. In the educational and scientific fields, its application in laboratories offers notable advantages: real-time environmental monitoring, automated alerts, data collection for analysis, and remote control of devices. According to UNIR (2023), "the IoT is based on the digitization of information sensed by devices that transmit it to the cloud for processing and automated response."

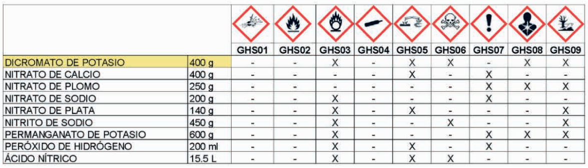
Safety in chemical laboratories and gas monitoring. Chemical laboratories are potentially hazardous environments due to the use of toxic, flammable, or volatile substances. Therefore, the implementation of environmental monitoring systems is an urgent necessity, not only to comply with safety regulations, but also to safeguard the integrity of students, teachers, and technical staff. Andersen (2025) points out that "the incorporation of gas detection systems is an essential preventive measure in academic laboratories that use hazardous chemicals" (p. 9).

Hazardous compounds can be classified into several categories, including flammable gases (such as methane or hydrogen), non-flammable but asphyxiating gases (such as carbon dioxide), and toxic gases (such as ammonia or chlorine). The presence of these compounds in high concentrations can cause anything from mild irritation to lethal effects.

METHODOLOGY

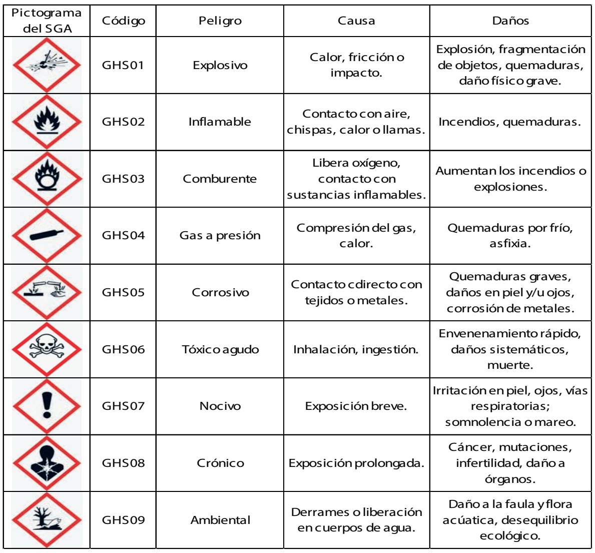
The development of the system was structured in several stages. First, the gases frequently used in the Industrial Analysis laboratory were identified, which allowed the selection of suitable sensors for monitoring. Subsequently, the prototype was designed and integrated with IoT connectivity, and a mobile application was programmed to send real-time notifications to the teacher's device in the event of a leak. This automated solution significantly reduces emergency response times, centralizes risk management, and optimizes institutional safety protocols.

Initial diagnosis and sensor selection. Information was gathered through interviews with teachers and direct observation, which allowed us to identify the most commonly used and highest-risk compounds, such as ammonia (NH_3), sulfur dioxide (SO_2), chlorine (Cl_2), methane (CH_4), and carbon monoxide (CO). Based on this, MQ-type sensors (models MQ-2, MQ-9, MQ-135, MQ-136, MQ-137, and MQ-138) compatible with these compounds were selected. The following tables show some of the reagents used in the Industrial Laboratory along with the risks associated with their use.



		GHS01	GHS02	GHS03	GHS04	GHS05	GHS06	GHS07	GHS08	GHS09
DICROMATO DE POTASIO	400 g	-	-	X	-	X	X	-	X	X
NITRATO DE CALCIO	400 g	-	-	-	-	X	-	X	-	-
NITRATO DE PLOMO	250 g	-	-	-	-	-	-	X	X	X
NITRATO DE SODIO	200 g	-	-	X	-	-	-	X	-	-
NITRATO DE PLATA	140 g	-	-	X	-	X	-	-	-	X
NITRITO DE SODIO	450 g	-	-	X	-	-	X	-	-	X
PERMANGANATO DE POTASIO	600 g	-	-	X	-	-	-	X	X	X
PERÓXIDO DE HIDRÓGENO	200 ml	-	-	X	-	X	-	X	-	-
ÁCIDO NÍTRICO	15.5 L	-	-	X	-	X	X	-	-	-

Table 1. Some reagents used in the Industrial Analysis Laboratory.



Pictograma del SGA	Código	Peligro	Causa	Daños
	GHS01	Explosivo	Calor, fricción o impacto.	Explosión, fragmentación de objetos, quemaduras, daño físico grave.
	GHS02	Inflamable	Contacto con aire, chispas, calor o llamas.	Incendios, quemaduras.
	GHS03	Comburente	Libera oxígeno, contacto con sustancias inflamables.	Aumentan los incendios o explosiones.
	GHS04	Gas a presión	Compresión del gas, calor.	Quemaduras por frío, asfixia.
	GHS05	Corrosivo	Contacto cdirecto con tejidos o metales.	Quemaduras graves, daños en piel y/u ojos, corrosión de metales.
	GHS06	Tóxico agudo	Inhalación, ingestión.	Envenenamiento rápido, daños sistemáticos, muerte.
	GHS07	Nocivo	Exposición breve.	Irritación en piel, ojos, vías respiratorias; somnolencia o mareo.
	GHS08	Crónico	Exposición prolongada.	Cáncer, mutaciones, infertilidad, daño a órganos.
	GHS09	Ambiental	Derrames o liberación en cuerpos de agua.	Daño a la faula y flora acúatica, desequilibrio ecológico.

Table 2. Description of damage caused by the reagents used.

Prototype design and implementation. The system was designed with ESP32 microcontrollers connected to MQ sensors, mounted on a 3D-printed base with PETG filament to ensure ventilation and thermal resistance. The firmware, developed in C++, integrated automatic Wi-Fi connection, password authentication, and false positive detection through redundant scanning (, 2022). The system architecture included *firmware* for sensor reading and data transmission; *backend* with Next.js and PostgreSQL for report and user management; *WebSocket server* in Node.js for real-time communication; *web application* (Next.js) for administrative monitoring; and a *mobile application* (React Native) for alerts to operational personnel. The following figure shows the system architecture indicating all the elements mentioned above.

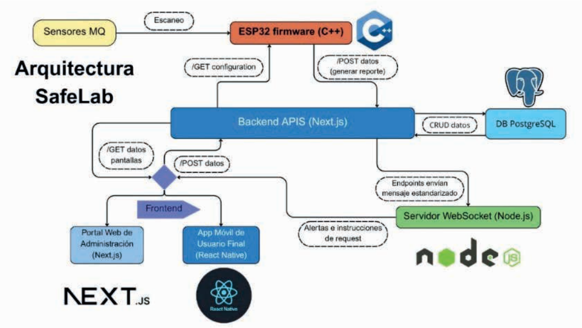

Arquitectura SafeLab
Sensores MQ
Escaneo
ESP32 firmware (C++)
/GET configuration
/POST datos (generar reporte)
Backend APIS (Next.js)
CRUD datos
DB PostgreSQL
/GET datos pantallas
/POST datos
Endpoints envían mensaje estandarizado
Frontend
Servidor WebSocket (Node.js)
Alertas e instrucciones de request
Portal Web de Administración (Next.js)
App Móvil de Usuario Final (React Native)
NEXT.JS
React Native
node JS

Figure 1. SAFELAB System Architecture.

Integration and interface development. Two interfaces were developed: a web interface for system administration, data visualization, and configuration; and a mobile interface for receiving real-time notifications. Both were connected to the backend through REST endpoints and to the WebSocket server to ensure immediate updates and low latency (Johnson, 2024).

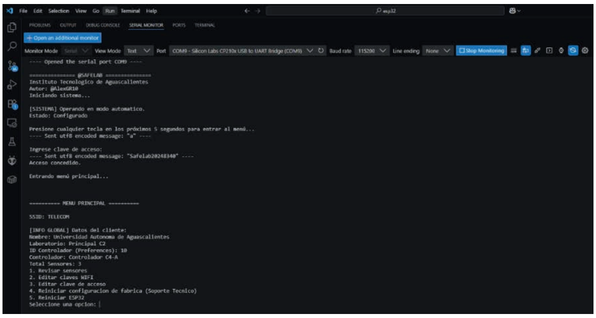
Functional testing. Controlled tests were carried out with real and simulated gases. The system demonstrated effectiveness in leak detection, automatic report generation, and sending alerts to web and mobile applications. The integration between sensors, firmware, database, and cloud services was successfully validated, confirming the functionality of the system under real laboratory conditions.

RESULTS

The main finding of this research was the technical validation of the SAFELAB system, which proved to be an effective and scalable solution for environmental monitoring in chemical laboratories through the use of Information and Communication Technologies (ICT). The system successfully integrated multiple components: gas sensors, ESP32 microcontrollers, a backend server- , a relational database, a web application, a mobile application, and a real-time communication server based on WebSocket.

The architecture allowed real-time data generated by the sensors to be captured, transmitted, stored, and visualized. This data was processed locally by the microcontrollers and sent to the backend for recording and consultation through the user interfaces. The web application provided administrators with access to alerts, historical reports, sensor status, and technical configurations, while the mobile application offered operational users immediate access to notifications and relevant events.

Microcontroller (ESP32) access and configuration test. In order to validate the security and accessibility of the system, direct tests were performed on the ESP32 microcontroller console interface. These tests included access verification using a **"superpassword,"** designed as a recovery mechanism in case of lost credentials or during initial device configuration (see Figure 2).


File Edit Selection View Go Run Terminal Help
esp32
PROBLEMS OUTPUT DEBUG CONSOLE SERIAL MONITOR PORTS TERMINAL
+ Open an additional monitor
Stop Monitoring

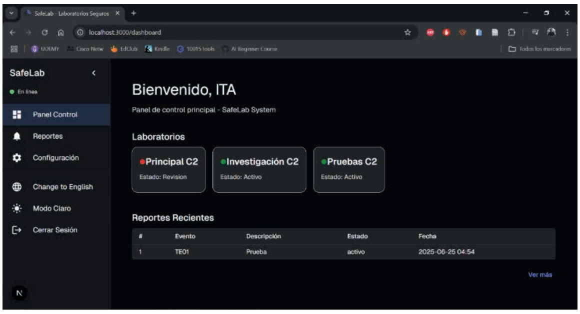
Monitor Mode Serial
View Mode Text
Port COM9 - Silicon Labs CP210x USB to UART Bridge (COM9)
Baud rate 115200
Line ending None

```
---- Opened the serial port COM9 ----

=============== @SAFELAB ===============
Instituto Tecnologico de Aguascalientes
Autor: @AlexGR10
Iniciando sistema...

[SISTEMA] Operando en modo automatico.
Estado: Configurado

Presione cualquier tecla en los próximos 5 segundos para entrar al menú...
---- Sent utf8 encoded message: "a" ----

Ingrese clave de acceso:
---- Sent utf8 encoded message: "Safelab20248340" ----
Acceso concedido.

Entrando menú principal...



---------- MENU PRINCIPAL ----------

SSID: TELECOM

[INFO GLOBAL] Datos del cliente:
Nombre: Universidad Autonoma de Aguascalientes
Laboratorio: Principal C2
ID Controlador (Preferences): 10
Controlador: Controlador C4-A
Total Sensores: 3
1. Revisar sensores
2. Editar claves WIFI
3. Editar clave de acceso
4. Reiniciar configuracion de fabrica (Soporte Tecnico)
5. Reiniciar ESP32
Seleccione una opcion: |
```

Figure 2. Access to the system using a "superpassword."

Subsequently, the **sensor menu** was navigated, which dynamically retrieved the information stored in the database, correctly displaying the identifiers assigned to the microcontroller according to the corresponding laboratory. This menu demonstrated that the system automatically recognized the specific configuration of the environment where it was installed.

Integration test between ESP32 and the backend. To validate the correct communication between the ESP32 microcontroller and the backend, controlled data was sent via HTTP POST requests. It was verified that the data was received without errors, that the corresponding reports were automatically generated , and that they were recorded in full in the relational database (see Figure 3).



Bienvenido, ITA

Panel de control principal - SafeLab System

Laboratorios

Principal C2
Estado: Revision

Investigación C2
Estado: Activo

Pruebas C2
Estado: Activo

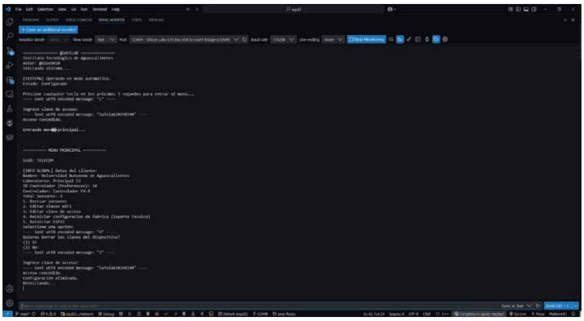
Reportes Recientes

#	Evento	Descripción	Estado	Fecha
1	TE01	Prueba	activo	2025-06-25 04:54

Figure 3. SAFELAB main control panel.

Configuration recovery test from the backend. An essential feature of the SAFELAB system is the ability of the ESP32 microcontroller to dynamically recover its configuration from the backend using HTTP GET requests. In this test, it was verified that, when sending its unique identifier (MAC address), the device correctly received parameters such as the number of assigned sensors and the corresponding thresholds, thus ensuring automatic and contextualized assignment according to the laboratory to which it belongs.

Initially, the ESP32 was linked to the customer's laboratory "UAA", with sensors identified as 56, 57, and 58 (assigned to the controller with ID 10). To validate the dynamic configuration update, the device was reset to factory defaults (Figure 4) and reconfigured with a new ID corresponding to the customer "ITA."

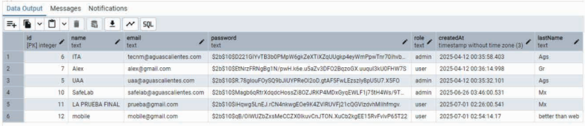


```
--------------- @SAFELAB ---------------
Instituto Tecnologico de Aguascalientes
Autor: @Aleo0R10
Iniciando sistema...

[SISTEMA] Operando en modo automatico.
Estado: Configurado

Presione cualquier tecla en los proximos 5 segundos para entrar al menú...
---- Sent utf8 encoded message: "c" ----

Ingrese clave de acceso:
---- Sent utf8 encoded message: "Safelab20240340" ----
Acceso concedido.

Entrando men��principal...


---------- MENU PRINCIPAL ----------

SSID: TELECOM

[INFO GLOBAL] Datos del cliente:
Nombre: Universidad Autonoma de Aguascalientes
Laboratorio: Principal C2
ID Controlador (Preferences): 10
Controlador: Controlador C4-A
Total Sensores: 3
1. Revisar sensores
2. Editar claves WIFI
3. Editar clave de acceso
4. Reiniciar configuracion de fabrica (Soporte Tecnico)
5. Reiniciar ESP32
Seleccione una opcion:
---- Sent utf8 encoded message: "4" ----
Quieres borrar las claves del dispositivo?
(1) Si
(2) No:
---- Sent utf8 encoded message: "1" ----

Ingrese clave de acceso:
---- Sent utf8 encoded message: "Safelab20240340" ----
Acceso concedido.
Configuración eliminada.
Reiniciando...
```

Figure 4. Resetting the ESP32 to factory settings.

Real-time communication tests using WebSocket. One of the key components of the SAFELAB system was the WebSocket server, designed to send real-time notifications to authorized users, according to the laboratory to which they belong. To validate its operation, events were simulated from different laboratories (ITA and UAA), checking that alerts were only delivered to users connected to the "room" corresponding to their institution.

First, the association between users, roles, and clients was verified. By consulting the *Client* and *UserClient* tables, it was confirmed that the user with ID 5 was linked to the client "UAA" (ID 6), while the user with ID 6 belonged to "ITA" (ID 5). This assignment was key to correctly segmenting the reception of events (Figure 5).



	id [PK] integer	name text	email text	password text	role text	createdAt timestamp without time zone (3)	lastName text
1	6	ITA	tecnm@aguascalientes.com	$2b$10$D221GIYvTB3b0PMpW6gkZeXTiXZqUUgkp4eyWmPpwTnr70ihvb...	admin	2025-04-12 00:35:58.403	Ags
2	7	Alex	alex@gmail.com	$2b$10$EtNrzFRNgBg1N/pwH.k6e.u5aZv3DFO2BqzoGX.uuqul3kU0FHW7S	user	2025-04-12 00:36:14.998	Gr
3	5	UAA	uaa@aguascalientes.com	$2b$10$R.78glouFOySQ9bJiUYPReOl2oD.gtAF5FwLEzszly8pU5U7.X5FO	admin	2025-04-12 00:35:32.101	Ags
4	10	SafeLab	safelab@aguascalientes.com	$2b$10$Magb6qRtrXdqdcHossZi8OZJRKP4MDxGyqEWLF1j75tH4Ws/9T...	admin	2025-06-26 03:46:00.531	Mx
5	11	LA PRUEBA FINAL	prueba@gmail.com	$2b$10$iHqwg5LnEJ.rCN4nkwgEOe9K4ZViRUVFj21cQGVlzdvhMlihfmgv.	user	2025-07-01 02:26:00.541	Mx
6	12	mobile	mobile@gmail.com	$2b$10$qB/GIWUZbZxsMeCCZX0IkuvCnJTON.XuCb2kgEE15RvFvlvP65T22	user	2025-07-01 02:54:14.17	better than web

Figure 5. Users registered in the system.

To facilitate testing, reports were simulated from the backend using Postman, without the need to recompile the ESP32 firmware. In the first case, the web interface was logged into as user "UAA" and a change was generated in the status of sensor 56, which went from "high" to "normal." The WebSocket server recognized the connection and automatically assigned the user to the corresponding room (room 6), successfully sending the notification in real time.

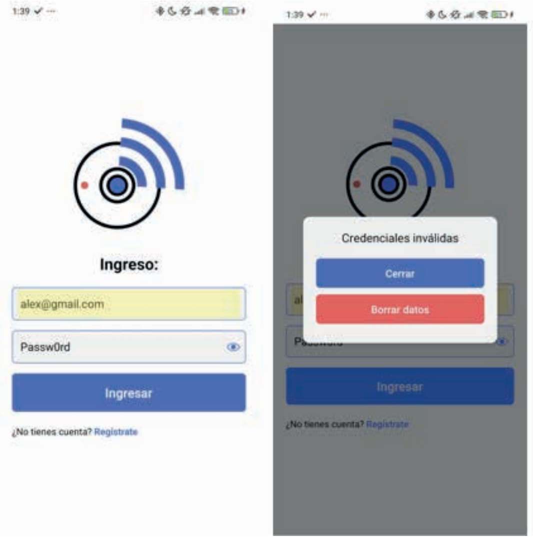
The test was then repeated with the session started as user “ITA.” Although the system recorded the same report in the database, no alert was displayed on this user’s interface, demonstrating the effectiveness of client segmentation. Finally, upon returning to the “UAA” user account, it was verified that both reports from sensor 56 were correctly recorded and visible on their dashboard.

These tests confirmed **low latency**, the correct association of users with notification rooms, and the integrity of the real-time communication system, which are essential elements for ensuring a timely response to critical events in the laboratory.

Mobile application testing. In order to validate the functionality of the mobile application, tests were carried out focusing on login, real-time notification reception, and sensor status display. These tests were performed by operational users (students), who successfully accessed the platform using their previously registered credentials.

Initially, system security was verified through attempts to access the system with invalid passwords, which were correctly rejected by the authentication system (Figure 6). Next, the main panel of the application was successfully accessed using valid credentials, and the connection of the mobile device to the WebSocket server was confirmed, enabling the reception of real-time events.

An external simulation (via Postman) was used to generate a new report associated with customer ID 5. The mobile application, being correctly linked to that customer, automatically received the notification and updated its interface with the new event detected, thus validating the correct functioning of the communication channel and the synchronization of data with the system database.



1:39

Ingreso:

alex@gmail.com

Passw0rd

¿No tienes cuenta? Regístrate

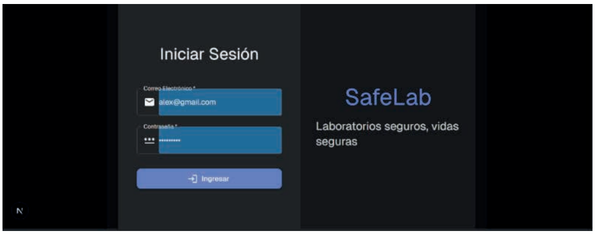
Credenciales inválidas

Figure 6. Mobile application login screen.

These tests confirmed that the mobile app not only allows secure and personalized access, but also fulfills its main objective: to provide operational users with a reliable tool for receiving security alerts immediately.

Authentication and security tests. Specific tests were carried out to verify the robustness of the JWT token-based authentication system and role-based access control. The objective was to ensure that only authorized users can access the routes and functionalities that correspond to them, both on the web platform and in the mobile application.

First, an attempt to access the web administration panel was simulated using a user without administrator privileges. The system correctly detected the user’s role and denied access to that section, redirecting them outside the restricted environment (Figure 7).



Iniciar Sesión

Correo Electrónico *: alex@gmail.com

Contraseña *: ••••••••••

SafeLab

Laboratorios seguros, vidas seguras

Figure 7. Access attempt with an unauthorized user.

Next, different scenarios were tested with **expired or revoked tokens**. When a token was manually revoked in the database, the system identified the access attempt as soon as a new request was made, automatically redirecting the user to the login page and preventing access to protected routes, such as / reports. This same behavior was confirmed by the backend console, which logged the invalid requests and handled them appropriately with HTTP status codes (401 Unauthorized).

Similarly, these tests were replicated in the mobile application. Once the corresponding token was revoked, the backend rejected requests to restricted resources and forced the user to be redirected to the /logout route, thus validating that the system responds consistently and securely to invalid sessions in mobile environments as well.

These tests confirmed that the system effectively implements an authentication policy based on security standards, with route protection, real-time token validation, and role-based access segmentation, ensuring a reliable environment for both operational users and administrators.

Comprehensive functional test (end-to-end). In order to validate the complete functionality of the system under real conditions, a comprehensive test was carried out in the Industrial Analysis laboratory. This test simulated an authentic risk scenario, in which a harmful gas was released in a controlled manner, allowing the behavior of the system to be observed throughout its entire operational flow.

Benzene, one of the chemicals present in the laboratory, was selected as the test substance. After preparing the area under the appropriate safety measures, sensor ID 55 was deliberately exposed to the gas. As a result, the sensor gradually increased its readings until it reached the configured threshold, which automatically triggered the generation of a new report from the controller (Figure 8).

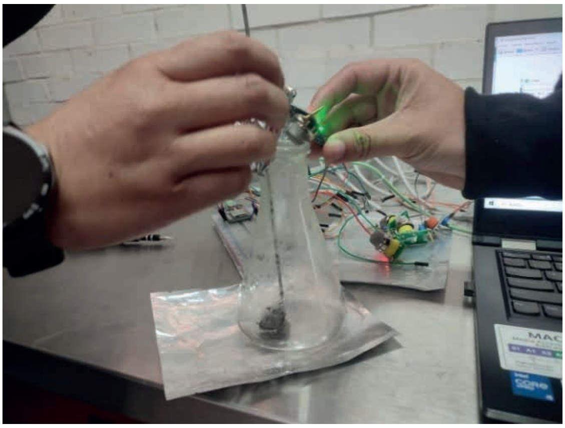


Figure 8. Successful gas leak test.

At the same time, the web application remained on standby for events and reacted in real time when it received the corresponding alert, displaying the new report and updating the monitoring panel immediately.

Simultaneously, a user with an active session in the mobile application also received the notification and was able to view the event information from their device, thus confirming the effective synchronization between the backend, sensors, WebSocket server, and both client interfaces.

This comprehensive test demonstrated that the system satisfactorily fulfills its central objective: to detect the presence of hazardous gases and issue real-time alerts to the appropriate users, strengthening safety protocols in educational environments where chemicals are handled.

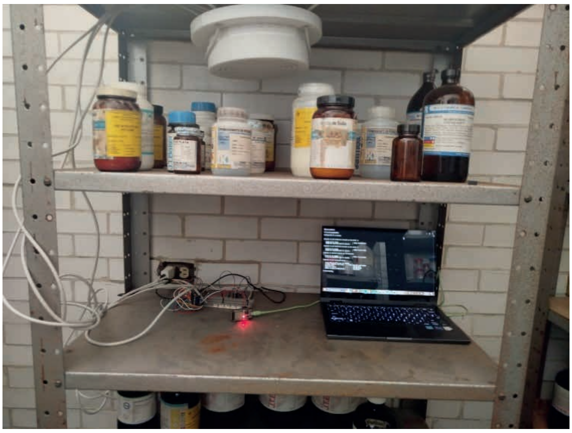


Figure 9. System put into production.

CONCLUSIONS

The implementation of the SAFELAB system proved to be a viable, functional, and scalable solution for improving safety in laboratory environments where potentially hazardous gases are handled. The integration of microcontrollers, specialized sensors, distributed software architecture, and real-time connected applications made it possible to detect the presence of harmful compounds with high accuracy, generating immediate alerts on both mobile and web platforms.

Functional tests validated the correct interoperability between the different components of the system, including secure authentication, data storage, communication via WebSockets, and dynamic configuration recovery. Likewise, it was verified that alerts were sent exclusively to authorized users assigned to the corresponding laboratories, ensuring effective information segmentation.

From a technical and pedagogical point of view, the project demonstrated that the incorporation of technologies such as IoT, ESP32 microcontrollers, MQ sensors, React Native, and relational databases can significantly enhance risk management in academic laboratories, fostering a culture of prevention among chemical engineering students and teachers.

As a future line of work, we propose to scale this system to other academic and industrial spaces, integrate sensors for additional environmental variables (such as temperature, humidity, or pressure), and improve the intelligence system for risk prediction using machine learning algorithms.

REFERENCES

Andersen, L. (2025, junio 9). What is Toxic Gas? https://blog.storemasta.com.au/what-is-toxic-gas

Crawford, J. A., Vallis, C., Yang, J., Fitzgerald, R., O'Dea, C., & Cowling, M. (2024). *Educational Transformation Through Emerging Technologies: Critical*

Johnson, T. (2024, septiembre 11). *Understanding Backend Architecture*. DEV Community. https://dev.to/tomjohnson3/understanding-backend-architecture-ljb

MICRODESYS. (2022). *Microcontrolador Esp32 – Microdesys*. https://microdesys.es/docs/microcontrolador-esp32/

PROMETEC. (2023). *Sensores de gas serie MQ – Prometec*. https://www.prometec.net/sensores-de-gas-serie-mq/

Red Hat. (2025). *¿Qué es el Internet de las cosas—IoT y cómo funciona?* ¿Qué es el Internet de las cosas (IoT)? https://www.redhat.com/es/topics/internet-of-things/what-is-iot

Review of Scientific Impact on Learning. Journal of University Teaching & Learning Practice

SDI, I. (2021, junio 25). *Sensores: Qué son, cómo funcionan, características y tipos*. https://sdindustrial.com.mx/blog/sensores/

Taller de DroneBot. (2021, enero 16). Getting Started with PlatformIO - Better than the Arduino IDE. *DroneBot Workshop*.

UNIR, L. U. E. I. (2023, mayo 17). *¿Qué es la arquitectura IoT y dónde se emplea?* UNIR. https://www.unir.net/revista/ingenieria/arquitectura-iot/https://dronebotworkshop.com/platformio/