Comparativa de Componentes de Hardware: Decisiones Eficientes y Confiables

La selección del hardware es tan crucial como la del software. Para nuestro prototipo, optamos por componentes que ofrecen un equilibrio perfecto entre fiabilidad, bajo costo, amplia documentación y facilidad de integración.

1. Detección de Presencia: Sensor Ultrasónico HC-SR04 vs. Sensor Infrarrojo (PIR) / Barrera Láser

Característica	**Nuestra Elección: Sensor Ultrasónico HC-SR04**	**Alternativa: Sensor Infrarrojo Pasivo (PIR)**	**Alternativa: Barrera Láser/Infrarroja**
Tipo de Detección	Mide la distancia exacta enviando un pulso de sonido y midiendo el tiempo de rebote.	Detecta movimiento a través de cambios en la radiación infrarroja (calor corporal). No mide distancia.	Detecta la interrupción de un haz de luz entre un emisor y un receptor.
Precisión y Control	Alta precisión. Nos permite definir un umbral exacto (ej. 30 cm) para activar el sistema. Es clave para la lógica anti-tailgating.	Menos preciso. Puede tener falsos positivos por cambios de temperatura o ser menos sensible si la persona se mueve muy lento. No informa sobre la proximidad.	Muy fiable para cruce, pero requiere dos componentes (emisor/receptor) y una alineación cuidadosa, lo que complica la instalación física.
Costo y Simplicidad	Extremadamente económico y simple. Requiere solo 4 pines y su librería es muy sencilla.	También económico, pero su lógica de detección es menos granular.	Ligeramente más costoso y complejo de instalar físicamente que un solo sensor ultrasónico.

¿Por qué nuestra elección es mejor para este proyecto?
El HC-SR04 no solo nos dice "si hay alguien", sino "a qué distancia está". Esta información de distancia es fundamental para la inteligencia de nuestra máquina de estados. Nos permite:

1. Activar el sistema solo cuando una persona está intencionadamente cerca, ignorando a quienes solo pasan de lejos.
2. Implementar una lógica anti-tailgating robusta al poder confirmar que el espacio entre los dos sensores está libre antes de cerrar la puerta.

Un sensor PIR no nos daría esta granularidad, y una barrera láser, aunque efectiva, es más compleja de instalar y no nos informa de la llegada inicial de una persona (solo del cruce). El HC-SR04 es la solución más completa y rentable.

---

2. Identificación Primaria: Lector RFID MFRC522 vs. Teclado Numérico / Lector de Huella Dactilar

Característica	Nuestra Elección: Lector RFID MFRC522	Alternativa: Teclado Numérico	Alternativa: Lector de Huella Dactilar
Velocidad y Comodidad	Extremadamente rápido y sin contacto. El usuario solo necesita acercar una tarjeta o llavero.	Lento y propenso a errores. El usuario debe recordar y teclear un PIN, lo cual es más lento y puede ser observado por otros (shoulder surfing).	Rápido, pero puede fallar con dedos sucios, mojados o con heridas.
Seguridad de la Credencial	Seguro. Cada tarjeta tiene un UID único que no puede ser fácilmente clonado (en el nivel básico). Es más seguro que un PIN que puede ser compartido o robado.	Baja seguridad. Los PINs se pueden olvidar, compartir, adivinar o robar visualmente.	Alta seguridad. La huella es única para cada individuo.
Costo e Integración	Muy bajo costo y excelente soporte para Arduino con librerías maduras. Se integra fácilmente vía SPI.	También de bajo costo, pero requiere manejar una matriz de botones, lo que consume más pines y complejidad de código.	Significativamente más costoso y con librerías que pueden ser más complejas de integrar.

¿Por qué nuestra elección es mejor para este proyecto?
El MFRC522 representa el punto óptimo entre seguridad, costo y conveniencia. Ofrece una mejora de seguridad masiva sobre un PIN, ya que la credencial es física. Aunque un lector de huellas es más seguro, su costo es prohibitivo para un prototipo de esta escala y su fiabilidad puede ser un problema en ciertos entornos. El RFID nos permite implementar un sistema de credenciales único y robusto, que es la base perfecta sobre la cual construir factores de autenticación adicionales como el QR o el reconocimiento facial, logrando la "Seguridad Multifactorial" que es uno de los pilares de nuestro diseño.

---

3. Control de Protocolo: Interruptores Físicos vs. Configuración por Software (GUI)

Característica	Nuestra Elección: Interruptores Físicos	Alternativa: Configuración por Software (GUI)	¿Por qué nuestra elección es mejor para este proyecto?
Seguridad y Acceso al Control	Seguridad física. Solo alguien con acceso físico a la caja del sistema puede cambiar el modo de operación. Esto previene cambios de protocolo no autorizados remotamente.	Conveniente, pero vulnerable. Si alguien obtiene acceso a la PC de administración, podría degradar la seguridad del sistema (ej. cambiar de "RFID+Facial" a "Solo RFID").	Para un sistema de seguridad, tener un control físico tangible añade una capa de seguridad real. Un administrador puede estar seguro de que el protocolo que él estableció con los interruptores no puede ser alterado por un ataque de software. Es una decisión de diseño que prioriza la robustez.
Fiabilidad y Simplicidad	Extremadamente fiable y simple. Un interruptor está ON o OFF. El estado es	Depende de la comunicación constante y correcta entre la GUI y	La simplicidad de leer un estado HIGH/LOW de un pin es inherentemente más

	inequívoco y no depende de que el software esté corriendo o de la comunicación.	la máquina de estados. Un fallo en la comunicación podría impedir el cambio.	robusta que un complejo sistema de comandos de software. Para el botón de emergencia (E), esta fiabilidad es absolutamente crítica.
Feedback Inmediato	Visual y táctil. El administrador puede ver y sentir el estado del sistema directamente en el hardware.	Puramente visual en una pantalla.	Los interruptores físicos proporcionan una certeza que una interfaz de software no puede igualar, especialmente en situaciones críticas.

¿Por qué nuestra elección es mejor para este proyecto?
El uso de interruptores físicos no es una solución "anticuada", sino una decisión de diseño deliberada que prioriza la seguridad y la fiabilidad. Para funciones críticas como la selección del protocolo de seguridad y, sobre todo, la activación del modo de emergencia, la simplicidad y robustez de un interruptor físico superan con creces la conveniencia de una configuración puramente por software, alineándose con las mejores prácticas de los sistemas de control industrial y de seguridad.

---

4. Feedback al Usuario: LEDs Verde/Rojo vs. Pantalla LCD / Zumbador (Buzzer)

Característica	**Nuestra Elección: LEDs Verde y Rojo**	**Alternativa: Pantalla LCD**	**Alternativa: Zumbador (Buzzer)**
Claridad y Universalidad	Lenguaje universal e instantáneo. Verde significa "Adelante/OK", Rojo significa "Detenerse/Error". Es entendido por cualquier persona, sin importar el idioma o la condición.	Requiere que el usuario se detenga a leer un mensaje. Puede ser difícil de ver a distancia o bajo luz solar directa.	Proporciona feedback audible, pero puede ser molesto en un entorno de oficina. Un solo tono no puede comunicar la naturaleza del error (ej. "fuera de horario" vs. "tarjeta desconocida").
Simplicidad y Costo	Costo insignificante y la integración más simple posible (un pin por LED).	Más costoso y requiere una comunicación más compleja (I2C o paralelo), consumiendo más pines y recursos del microcontrolador.	De bajo costo, pero menos informativo que un LED.
Efectividad	Altamente efectivo para comunicar el estado binario más importante: "Acceso Concedido" o "Acceso Denegado".	Útil para mensajes detallados, pero una sobrecarga para una simple confirmación.	Bueno como complemento, pero no como feedback principal.

¿Por qué nuestra elección es mejor para este proyecto?
Para el feedback primario de "éxito" o "fallo", los LEDs son la solución más eficiente, clara y universal. Comunican el resultado de la validación de forma instantánea y sin ambigüedad. Mientras una pantalla LCD podría ser una buena adición futura para mostrar mensajes detallados, para el feedback esencial, la simplicidad y efectividad de un LED rojo y verde son inmejorables, proporcionando una experiencia de usuario fluida y sin fricciones.