

# Sistemas Embebidos

1 - tema 3

VHDL: suele caer un contador  
- (reloj y reset imparten)

1 - tema 4/5

- no hacer dos process  
diferentes que modifiquen  
el mismo registro.

1 - tema 6

VHDL <sup>(nodos)</sup>, Memoria

1 - presentaciones

---

---

---

---

# Tema 1: Sistemas empotrados: ámbitos de aplicación y flujo de diseño

## • ¿Qué es un sistema empotrado?

Es un sistema que realiza una función específica aunque hay algunos dispositivos empotrados que pueden realizar varias funciones.

## • Características y ámbitos de aplicación de los SE

Características:

- Conurrencia: los componentes del sistema funcionan simultáneamente.
- Fiabilidad y seguridad.
- Eficiencia (respuesta rápida).
- Interacción con disp. físicos no convencionales: sensores, actuadores, conversores.
- Bajo consumo, peso, precio y tamaño

Ambitos de aplicación:

- Automación: control temperatura, sistema de frenado, ...
- Electrónica de consumo: TV, PDAs, DVDs, electrodomésticos, ...
- Control industrial: robots, sistemas de control -manufacturación-
- Medicina: monitores cardíacos, prótesis, ...
- Redes: routers, hubs, gateways, ...
- Oficina: fax, fotocopiadoras, ...

## • Flujo de diseño:

### 1. Crear la arquitectura

- Concepto
  - Análisis de requerimientos
  - Creación arquitectura considerando todos los recursos y los requerimientos
- |                             |
|-----------------------------|
| - Tecnología disponible     |
| - Limitaciones precio final |
| - Velocidad                 |

## Arquitectura de un SE

Se trata de una abstracción del sistema, donde se presentan un conjunto de elementos hw y sw que interactúan. Todo el hw reside en una tarjeta llamada PWB/PCB (Printed Wiring/Circuit Board).

- La CPU: Unidad Central de Proceso (Unidad de Control, Banco de registros, Unidad aritmético-logica, Buses internos).

Tipos: CISC, RISC, DSPs, microprocesadores, microcontroladores

- Memoria: donde se encuentran todos los datos e instrucciones que se van a utilizar durante programa. Organización jerárquica basada en la localización espacial y temporal de datos:

Cache (más rápido pero limitado), RAM y ROM (memoria principal), discos y otros medios.

MMU (Unidad de Gestión de Memoria): traduce dir. lógicas en físicas, gestiona seguridad y controla acceso.

- Buses y Entrada/Salida del procesador: los SE interactúan con el entorno mediante:

- Dispositivos convencionales: teclados, ratones.

- Dispositivos especializados: sensores y actuadores.

Los métodos de conexión pueden ser cableados (puertos serie y paralelo) e inalámbricos (bluetooth, infrarrojos)

- Protocolos y transferencia de datos:

- Conexiones serie: uno de los protocolos serie más conocidos es el RS232, utilizado tanto para transferencia síncrona (con reloj) como asíncrona (bits de inicio/parada).

- Conexiones paralelas: transfieren varios bits simultáneamente (IEEE1284 para impresoras), también incluyen buffers para mejorar la gestión de datos.

- Transferencias de datos:
  - DMA (Acceso Directo a Memoria), minimiza la intervención del procesador.
  - Interrupciones: eventos que permiten al procesador responder a dispositivos externos.

## Tema 2: Microprocesadores, microcontroladores y procesadores de señal digital.

### • Introducción:

El procesador es el dispositivo central de control de un SE. Puede haber además varios procesadores esclavos. La complejidad y arquitectura del maestro determina si se clasifica como microprocesador o microcontrolador o DSPs (Procesadores de señal).

### • Modelos de Arquitectura ISA:

#### CARACTERÍSTICAS:

1. Operaciones: matemáticas y lógicas, desplaz. y rotaciones, Load/Store, saltos, ...

2. Operandos: 8 bits, 16 bits, 32 bits, ...

#### 3. Almacenamiento:

- Organización de la memoria: el rango de direcciones disponible para un procesador puede ser:

- Lineal: las localizaciones se representan de forma incremental  $0 \dots 2^{(N-1)}$  donde N = num bits dir.

- Segmentado: la memoria se divide en segmentos. La dirección viene determinada por un n° de segmento + offset, también hay que ver como se guardan los datos en memoria:

- Big-endian: el bit/byte más significativo va primero (ej. 68000, Sparc).

- Little-endian: el bit/byte menos significativo va primero (ej. x86)

#### 4. Modos de direccionamiento:

- Arquitectura Load/Store: sólo se permiten operaciones de procesamiento de datos en registros (ej. Power PC).

- Arquitectura Registro/Memoria: se pueden realizar operaciones tanto en registros como en mem.

#### 5. Interrupciones y excepciones:

Son mecanismos para parar y modificar el flujo de un programa.

#### EVOLUCIÓN:

- Acumuladores de 8 bits: limitados por su capacidad de acceso a memoria (Intel 8080).

- Procesadores de 16/32/64 bits: amplían las capacidades de cálculo y direccionamiento, mejoran el rendimiento introduciendo Segmentación y jerarquías de memoria.

## TIPOS DE PROCESADORES

- CISC (Complex Instruction Set Computing): Intel 80x86, Motorola 68000. Posee instrucciones complejas para reducir la cantidad de código.
- RISC (Reduced Instruction Set Computing): ARM, PowerPC. Posee instrucciones simples y rápidas, favoreciendo ciclos más predecibles.
- Modelos de paralelismo a nivel de instrucción:
  - SIMD (Single Instruction Multiple Data): una instrucción opera sobre múltiples datos. Impresoras, escáneres.
  - Superescalar: ejecución de múltiples instrucciones en un solo ciclo.
  - VLIW (Very Long Instruction Word): múltiples instrucciones en un ciclo a través de varios componentes funcionales.

## • Modelos ISA específicos para aplicaciones:

Modelo controlador: diseñado para tareas simples, como el manejo de audio o video. Procesadores en tarjetas analógicas de TV.

Modelo camino de datos: es un procesador cuyo propósito es realizar periódicamente computaciones fijas sobre conjuntos de datos diferentes. Teléfono digital

Modelo FSMD (Finite State Machine with Data path): es la combinación de los dos anteriores, cuando no se requieren manipulaciones complejas y hay que realizar repetidamente computaciones fijas en conjuntos distintos de datos.

Modelo Máquina Virtual de Java (JVM): basado en el estándar de la máquina virtual de Java. ej: 80/100

## • Diseño de un procesador:

El diseño de un procesador determina su rendimiento y flexibilidad para aplicaciones empotradas.

- El modelo de arquitectura Harvard permite incrementar la cantidad de datos procesados por unidad de tiempo, por eso suele utilizarse en modelos ISA basados en datapath, como los DSPs, donde se hacen instrucciones fijas sobre diferentes conjuntos de datos. Básicamente tiene la memoria separada para datos e instrucciones, mejorando el rendimiento. Ej: DSPs, ARM9.
- El modelo de arquitectura von Neumann comparte memoria para datos e instrucciones. Ej: ARM7 y x86.

Componentes principales: registros (almacenan datos temporales para operaciones rápidas), la unidad de control (CU, gestiona el flujo de datos y las instrucciones) y una ALU (ejecuta op. matemáticas y lógicas).

## Interfaz de E/S:

- Dispositivos conectados al procesador para E/S de datos: Redes y comunicaciones, Entrada (teclado, ratón, control remoto), gráficos (LEDs, monitores) y almacenamiento (discos, cintas).
- Interfaz entre controlador y master:
  - Master inicializa y monitoriza el controlador.
  - Master realiza peticiones de E/S, mediante instrucciones o la memoria.
  - Dispositivo E/S contacta con CPU (instrucciones)
  - Intercambio de datos (transferencia programada, DMA).

## Rendimiento del procesador:

El rendimiento se evalúa mediante diferentes métricas.

- Tasa de transferencia (throughput-CPU): es la cantidad de trabajo que realiza la CPU en un periodo determinado, medida en MB/s o MIPS.
- Ciclos por instrucción (CPI): influye directamente en el tiempo de ejecución de un programa, el reloj de la CPU suele ser más rápido que el del sistema.  $T_{ejec} = n^{\circ} \text{ instr.} \cdot CPI \cdot \text{periodo\_reloj}$

Cuando se conocen los tiempos de ejecución de un programa en dos arquitecturas A y B, se define el speedup como:  $\text{speedup}_{B/A} = \frac{T_{ejecA}}{T_{ejecB}}$

Latencia y fiabilidad:

- MTBF (Mean Time Between Failures)
- MTTA (Mean Time To Recover)

## Raspberry Pi

**Definición y Uso:** La **Raspberry Pi** es una computadora de placa única (SBC) de bajo costo y tamaño reducido, diseñada inicialmente para fomentar la enseñanza de ciencias de la computación.

Ideal para proyectos de **IoT** y **sistemas embebidos** gracias a su bajo consumo y capacidad de interactuar con sensores y dispositivos externos.

### **Modelos Destacados**

**Raspberry Pi 1, 2 y 3:** ofrecen un balance de potencia y consumo, el modelo 3 introdujo la conectividad WiFi y Bluetooth.

**Raspberry Pi 4:** versión mucho más potente, opciones de hasta 8 GB de RAM, soporte para USB 3.0 y doble salida 4K.

**Raspberry Pi Zero y Zero W:** modelos ultracompactos y más económicos; el modelo W incluye conectividad WiFi y Bluetooth.

**Raspberry Pi 5 (2023):** Procesador ARM Cortex-A76, soporte para SSD y mejoras gráficas (4K y 8K).

La Raspberry Pi utiliza principalmente un sistema operativo basado en Linux, llamado Raspberry Pi OS (anteriormente conocido como Raspbian).

**Raspberry Pi OS Lite:** Una versión sin entorno gráfico, ideal para proyectos de servidor o IoT donde la interfaz de usuario no es necesaria.

**Raspberry Pi OS Desktop:** Versión estándar con entorno gráfico, similar a otros sistemas de escritorio Linux. Ideal para quienes buscan un uso más cotidiano de la Pi.

**Raspberry Pi OS Full:** Incluye todas las herramientas de desarrollo y aplicaciones preinstaladas (como LibreOffice, herramientas de programación y software educativo), siendo perfecta para la educación.

### **Aplicaciones**

Control de dispositivos domésticos (luces, electrodomésticos). Monitorización de invernaderos o estaciones meteorológicas. Cámaras de seguridad y servidores ligeros.

**Ventajas:** Económica, versátil, y respaldada por una comunidad activa.

**Desafíos:** Mayor consumo energético que microcontroladores como Arduino. Menor resistencia en entornos extremos.

### MRAM (Magnetoresistive RAM)

**Definición:** La **MRAM** es una memoria no volátil que almacena datos mediante propiedades magnéticas en lugar de cargas eléctricas, ofreciendo alta velocidad y durabilidad.

#### Funcionamiento

**Lectura:** Mide la resistencia en una unión túnel magnética (consiste en dos capas de material ferromagnético separadas por una capa aislante). Cuando las capas magnéticas están alineadas entre sí, se atraen, por lo que hay menor resistencia y se interpreta como "1", y al haber mayor resistencia, como "0".

**Escritura:** Una corriente eléctrica altera la orientación magnética de las capas, cambiando el estado almacenado.

#### Ventajas

**No volatilidad:** Conserva datos al apagarse.

**Alta velocidad:** Similar a la SRAM, pero es no volátil.

**Bajo consumo de energía:** ideal para dispositivos dependientes de baterías.

**Durabilidad:** Resistente a millones de ciclos de escritura.

#### Desventajas

**Costo elevado:** Más cara que otras memorias, como la SDRAM.

**Escalabilidad:** Baja densidad, lo cual hace que sean más grandes y tengan menor capacidad.

**Interferencias magnéticas:** Aunque son poco comunes, afectan su fiabilidad en entornos con mucho ruido electromagnético.

#### Aplicaciones

Caché en procesadores por su rapidez.

IoT y sistemas embebidos: sensores, satélites, y dispositivos médicos.

#### Futuro

Empresas como Samsung e Intel están invirtiendo en el desarrollo de MRAM para mejorar su capacidad y costo, destacándola como una memoria clave para aplicaciones avanzadas y sostenibles.

### Solid State Drive (SSD)

**Definición:** Los **SSD** son dispositivos de almacenamiento que usan memoria no volátil (Flash NAND) para leer y escribir datos sin partes mecánicas, a diferencia de los HDD.

#### Funcionamiento

**Escritura:** se aplica una diferencia de voltaje entre la entrada y la salida, después, si se quiere escribir, se aplicará un voltaje positivo desde la puerta de control que atraerá a los electrones hacia la puerta flotante, donde se almacenan los electrones hasta por 10 años. Para eliminar el dato, se aplica un voltaje negativo.

**Lectura:** Si en la salida se pueden leer electrones, significa que la puerta flotante está vacía, por lo que se almacena un 0. Si la puerta flotante está llena, los electrones de la puerta repelen los electrones procedentes de la fuente, para que no se puedan leer electrones a la salida, lo que significa que se almacena un 1.

## Tipos de Tecnología

**SLC (1 bit por celda):** Alta velocidad y durabilidad, pero costosa.

**MLC/TLC (2-3 bits por celda):** Balance entre costo y rendimiento.

**QLC (4 bits por celda):** Más capacidad pero menor durabilidad y velocidad.

## Comparación SSD vs HDD

**SSD:** Rápido, ideal para sistemas operativos y gaming, pero más caro por GB.

**HDD:** Económico, adecuado para almacenamiento masivo (archivos multimedia y copias de seguridad).

## RAM DDR4

**Introducción:** Tecnología de memoria RAM introducida en 2000, usada inicialmente con procesadores AMD Athlon e Intel Pentium 4. La DDR4 (Double Data Rate 4) sincroniza lectura/escritura al reloj con accesos en ambos flancos.

**Características:** Tamaño por módulo: 8-64 GB, velocidades de 2400-3200 MHz, consumo máximo de 5 W. Zócalo de 288 pines (más que DDR3) y menor grosor.

**Comparativa DDR4 vs DDR3:** DDR4 ofrece mayor velocidad, menor voltaje (1.2V), mayor capacidad por módulo y mejor eficiencia.

**Vulnerabilidad Rowhammer:** Accesos repetidos a filas pueden cambiar bits, afectando la estabilidad de los datos.

**Optimización y Overclocking:** Beneficios en multitarea y juegos, pero con riesgos de estabilidad y garantía.

**Mercado y futuro:** Marcas principales como Corsair y Kingston; se prevé el avance hacia DDR5 con mayor capacidad y eficiencia.

## Memorias Flash

Creada como evolución de las memorias EEPROM, con dos tipos principales: NOR y NAND.

**Arquitectura NOR:** Transistores conectados en paralelo permiten lecturas rápidas, pero su fabricación es más costosa.

- Lectura: Se activan los transistores de los que se quieren leer, si el transistor tiene carga en su puerta flotante quiere decir que tiene almacenado un '0' en caso contrario un '1'

- Escritura: Se deben borrar los datos aplicando un alto voltaje para dejar la puerta flotante sin carga dejando las celdas con un '1' mediante el efecto túnel de Fowler-Nordheim (dañando el óxido de la puerta flotante y por tanto reduciendo la vida útil de la flash).

**Arquitectura NAND:** Celdas en serie, optimizadas para almacenamiento masivo pero con acceso más lento y desgaste por escritura/borrado.

- Lectura: se mide la corriente en una celda objetivo mientras las demás celdas del string se colocan en estado de "paso".

- Escritura: antes de escribir, las celdas deben borrarse aplicando un alto voltaje, lo que desgasta la memoria con el tiempo. Al escribir un '0', se aplica tensión entre el drenador y la puerta de control de la celda. Al escribir un '1', se mantiene el resultado del borrado.

## Comparativa NOR vs NAND:

**NOR:** Mayor velocidad de lectura/escritura y fiabilidad; ideal para firmware y sistemas embebidos.

**NAND:** Mayor capacidad y menor costo; utilizada en SSD, pendrives y tarjetas SD.

**Tipos de NAND:** SLC, MLC, TLC y QLC, que varían en resistencia, capacidad y precio.

**Tecnología 3D NAND:** Incrementa la densidad al apilar celdas verticalmente, mejorando rendimiento y durabilidad.

# Tema 4: Buses industriales

## • Protocolos

Los buses industriales son los encargados de conectar los componentes de un sistema empotrado. Actúan como conductores de señales que transmiten datos, direcciones y control (reloj, petición, reconocimiento). Tipos:

- Bus del sistema o principal: conecta memoria principal y la caché al master. Cortos y rápidos.
- Backplane: conectan memoria, master y E/S en un única bus. Son rápidos.
- Bus de expansión: resto de componentes. Suelen ser estandares (USB, PCI). Permiten interrupciones.

Otra clasificación:

- Expandibles: permiten añadir dispositivos dinámicamente. USB, IDE.
- No expandibles: configuraciones fijas con dispositivos predeterminados

## • Protocolos de arbitraje:

Roles:

- Maestro: son los dispositivos que pueden iniciar una transacción. Si sólo hay un maestro no es necesario ningún protocolo de arbitraje.

- Esclavo: son los dispositivos que sólo acceden al bus como respuesta a una solicitud del maestro.
- Árbitro: hw que determina bajo qué circunstancia un maestro puede conseguir el control del bus.

Esquemas de arbitraje:

- Central paralelo dinámico: usa señales de prioridad para asignar el bus, puede emplear colas FIFO para las solicitudes.
- Central serie: dispositivos conectados en cascada, y cada uno evalúa su derecho a usar el bus en orden.
- Distribuido: no existe árbitro central. Hay prioridades predefinidas que determinan quién accede al bus.

## • Protocolos de comunicación (Handshake)

Define cómo maestro y esclavo/s coordinan sus operaciones. Esquema de tiempo:

- Bus sincrónico: se transmite bto el reloj, las transacciones ocurren en las flancas del reloj (subida o bajada). Solo funcionan para distancias cortas y frecuencias bajas.
- Bus asíncrono: la señal del reloj no se transmite, utilizan "request" y "acknowledge" para comunicarse, permiten distancias mayores.

## • Protocolo básico:

- El maestro pide una transacción de lectura o escritura a un esclavo.
- El esclavo responde enviando un ACK.

Si se piden datos de memoria o de un controlador E/S, si la dir. es válida, se envía el dato, puede usarse el modo rotaga (burst).

## Comunicación Serie:

En los SE, la comunicación serie utiliza un único canal para transferir datos bit a bit. Transferencias:

- Síncronas: se coordina mediante un reloj. Ej: SPI (Serial Peripheral Interface).
- Asíncrona: incluye bits de inicio START y parada STOP. Puede añadirse un bit par o impar para detectar errores. UART.

Bus I2C: diseñado para conectar procesadores y periféricos con interfaces específicas.

Arquitectura maestro/esclavo :

- Cada dispositivo tiene una dirección única de 7 o 10 bits que se usa para identificarlo. Transferencias se organizan en las siguientes etapas:
  - Idle: SDA = SCL = H . SDA (Serial Data Line), SCL (Serial Clock Line) , H (High) , L (Low).
  - Start: SDA H/L y SCL=H indica comienzo.
  - Address: el master envía la dirección y el modo transferencia (7+1 bit). El esclavo responde con un Ack .
  - Transferencia datos: se transmite un byte del emisor al receptor + ACK del receptor al transmisor.
  - Stop: SDA L/H con SCL=H.

## Comunicación paralela: PCI

La comunicación paralela tiene varios canales para transferir múltiples bits simultáneamente. PCI:

- Bus síncrono de alta velocidad: frecuencia → 33-66 MHz y ancho de banda → 32-64 bits, máx.  $528 \text{ MB/s}$
- Proceso de arbitraje:
  1. El iniciador solicita acceso al bus (REQ#).
  2. El árbitro concede el acceso (GNT#).
  3. El inicializador realiza la transacción (lectura o escritura).

## Rendimiento del bus:

El rendimiento de un bus depende del ancho de banda y Split transaction.

- Ancho de banda: cantidad de datos que el bus puede transmitir por unidad de tiempo, depende de:
  - Diseño físico: longitud, nº líneas, dispositivos soportados. Más corto = menos dispositivos, más líneas datos, + rápido
  - Protocolo: cuanto más sencillo más ancho de banda, los burst aumentan ancho de banda pero tb latencia.
- Split transaction: divide las transferencias en etapas para que otros dispositivos usen el bus mientras el handshake.

## Ejemplos:

### Universal Serial Bus (USB):

Es un bus de comunicación para conectar el PC a varios periféricos. El ancho de banda se configura para cada dispositivo. La topología es como un árbol con el host como raíz. La raíz ejecuta un driver de controlador USB que controla los dispositivos conectados al bus. Soporte plug-and-play para conexión/desconexión dinámica. Comunicación mediante endpoints (unidireccionales) agrupados en interfaces.

Protocolos: half-duplex (full-duplex para 3.0) donde los datos se pasan a través de una interfaz de dos cables.

Al conectar un dispositivo se produce un attach event

Clasificación: - Almacenamiento: discos duros, memoria flash. - Interfaz humano: ratón, teclado. - Hub: para extensión.

- Comunicaciones: tarjetas de red, modems.

Tipos de transferencia: control (todo dispositivo debe tener un endpoint), interrupciones (para datos de baja freq.),

bulk (grandes datos como impresora) e isoácronas (periódicas y continuas como video/audio).

### Bus NFC:

Definición y funcionamiento: es una tecnología de comunicación inalámbrica que permite la transferencia de datos entre dos dispositivos, usa comunicación activa (estos dispositivos inicien la comunicación y procesen los datos, como aplicaciones de móvil) y pasiva (no requieren de alimentación propia, como las etiquetas NFC).

#### Modos de trabajo:

- Lector/escritor: el elemento activo lee o escribe en la etiqueta pasiva.
- Emulación de tarjeta: un dispositivo emula una tarjeta inteligente, como en los pagos sin contacto.
- Peer-to-peer: dos dispositivos NFC pueden intercambiar información de manera bidireccional.

Un dispositivo NFC consta de varias partes:

- Chip NFC. Cerebro del sistema NFC. Gestiona la comunicación, flujo y procesado de las señales.
- Antena NFC. Se encarga de la recepción y transmisión de las ondas de radiofrecuencia para la recepción y envío de datos.
- Memoria. Almacena información, como un identificador único o datos específicos del lector NFC.

Los datos se organizan en un formato de estandarizado como NDEF (NFC Data Exchange Format), este permite que diferentes dispositivos y aplicaciones comprendan el contenido del mensaje.

Aplicaciones: Pagos móviles y sin contacto. Tarjetas de transporte público. Control de acceso en hoteles y oficinas. Publicidad interactiva mediante etiquetas NFC.

Ventajas: fácil de usar, bajo consumo de energía, alta seguridad, rápida transferencia de dato.

Desventajas: corto alcance, transferencia y disponibilidad limitada, costos adicionales en infraestructura.

## **BLUETOOTH:**

Definición y funcionamiento: es una tecnología de comunicación inalámbrica de corto alcance (10-30 metros) diseñada para redes personales (WPAN). Utiliza ondas de radio en la banda de frecuencia ISM (Industrial, Científica y Médica) de 2.4 GHz.

Forma redes llamadas piconet, donde un dispositivo actúa como maestro y los demás como esclavos.

### Proceso de Conexión

Descubrimiento: los dispositivos se anuncian en canales específicos.

Emparejamiento: intercambio de claves y establecimiento de enlaces seguros.

Sincronización: coordinación de intervalos de conexión y saltos de frecuencia.

Transferencia de datos: envío en paquetes con detección y corrección de errores.

### Aplicaciones

- Dispositivos de entrada/salida: ratones, teclados, controles de juegos.
- Audio: auriculares y altavoces inalámbricos.
- Wearables: pulseras, relojes inteligentes.
- Automóviles: manos libres, transmisión de música.
- Seguimiento: etiquetas y localización de objetos perdidos.

Ventajas: Bajo consumo de energía. Fácil de usar y ampliamente compatible.

Desventajas: Limitado a 10-30 metros de alcance. Velocidad de transferencia inferior a tecnologías como WiFi.

## **WIFI:**

Definición y funcionamiento: es una tecnología inalámbrica basada en los estándares IEEE 802.11, utilizada principalmente para redes de área local (WLAN). Opera en bandas de frecuencia de 2.4 GHz, 5 GHz y 6 GHz (WiFi 6E).

### Protocolos asociados:

**IEEE 802.11a:** Banda de 5 GHz, velocidades de hasta 54 Mbps.

**IEEE 802.11ac:** Banda de 5 GHz, velocidades de hasta 6.9 Gbps.

**IEEE 802.11ax (WiFi 6):** Uso eficiente de canales y soporte para múltiples dispositivos. Velocidades de hasta 9.6 Gbps.

### Aplicaciones

Redes domésticas y empresariales para acceso a Internet.

IoT (Internet of Things): sensores, cámaras de seguridad.

Streaming de video y contenido HD.

Ventajas: Alta velocidad de transferencia (hasta 9.6 Gbps). Alcance de hasta 100 metros en condiciones ideales.

Desventajas: Mayor consumo energético comparado con Bluetooth y NFC. Vulnerabilidad a interferencias en bandas saturadas.

## BUS CAN (Controller Area Network):

**Descripción:** Protocolo de comunicación desarrollado por Bosch en los años 80 para conectar módulos electrónicos de forma eficiente y confiable, sin necesidad de un controlador central.

### Características:

Comunicación basada en mensajes.

Tipología descentralizada y tolerante al ruido.

Alta fiabilidad y optimización del ancho de banda.

### Evolución:

Adoptado por Mercedes-Benz y utilizado en diagnósticos con OBD-II.

Avance hacia CAN FD, que admite tasas de transmisión más rápidas y mensajes más grandes.

### Aplicaciones más allá de la industria automotriz:

Robótica, automatización industrial, maquinaria pesada y navegación marítima.

### Funcionamiento técnico:

Arbitraje para decidir qué nodo transmite.

Sincronización con relojes independientes por nodo.

Uso de tramas simplificadas para solicitar datos entre dispositivos.

**Seguridad:** Vulnerabilidades como "car hacking" al puerto OBD-II.

## BUS SPI (Serial Peripheral Interface):

**Definición:** Protocolo serial síncrono utilizado para comunicación rápida entre microcontroladores y periféricos.

### Componentes:

**Maestro:** Controla la comunicación (señal SCLK).

**Esclavo:** Responde al maestro.

Líneas: SCLK, MOSI, MISO, SS/CS.

**Ventajas:** Alta velocidad, bajo consumo, simplicidad de hardware.

**Desventajas:** Complejidad física con muchos esclavos, alcance limitado.

**Comparaciones:** Más rápido que I<sup>2</sup>C y UART, pero menos flexible. I<sup>2</sup>C incluye direccionamiento; SPI no.

**Aplicaciones:** Controladores de pantalla, sensores, memorias, módulos de comunicación.

**Perspectiva futura:** Uso en tecnologías avanzadas de sistemas embebidos.

## Zigbee (Protocolo para IoT y Redes de Baja Energía):

**Definición:** Tecnología inalámbrica basada en IEEE 802.15.4 para redes de bajo consumo y bajo coste, ideal para IoT.

**Variantes:** Zigbee 1.0, 1.1, 3.0 y ZigbeePro (mejoras en seguridad, escalabilidad y consumo energético).

**Topologías de red:** Estrella, malla y árbol.

**Ventajas:** Bajo consumo y larga duración de batería. Alta escalabilidad (hasta 65,000 nodos). Seguridad avanzada con cifrado AES de 128 bits.

**Aplicaciones:** Domótica, medicina, automatización industrial, redes verdes (parques solares/eólicos).

**Capas del protocolo:** Física, MAC, red, aplicación (APS y ZDO).

**Seguridad:** Claves AES de 128 bits para cifrado y autenticación.

## LoRa (Long Range):

**Descripción:** Tecnología de modulación de espectro (CSS) que permite comunicación de largo alcance y bajo consumo energético, creada por Cycleo (ahora parte de Semtech).

**Características técnicas:**

Funciona en bandas de radiofrecuencia específicas (868 MHz en Europa, 915 MHz en América, 433 MHz en Asia).

Velocidades de 0,3 Kb/s a 50 Kb/s.

Componentes principales: dispositivos finales, puertas de enlace y servidor de red.

**Ventajas:** Bajo consumo de energía, largo alcance, bajo costo y comunicación segura.

**Seguridad:** Utiliza AES-128 para cifrado de mensajes y autenticación de dispositivos.

**Aplicaciones:** Agricultura, monitoreo remoto, ciudades inteligentes y salud.

**Desafíos:** Interferencias, latencias y capacidad limitada para grandes volúmenes de datos.

## RFID (Identificación por Radiofrecuencia):

**Definición:** Tecnología de comunicación inalámbrica que utiliza señales de radio para transferir datos entre un lector y un emisor.

**Tipos de etiquetas:**

**Activas:** Tienen su propia fuente de energía, mayor alcance.

**Pasivas:** Sin fuente de energía, menor alcance.

**Componentes:** Antena y chip con memoria.

**Frecuencias y alcances:** **LF:** 125-134 KHz, alcance de 10 cm. **HF:** 13,56 MHz, alcance de 10-100 cm. **UHF:** 860-960 MHz, alcance de hasta 12 m. **NFC:** 13,56 MHz, alcance de 10-20 cm.

**Ventajas:** Amplio uso comercial, adaptable a distintas aplicaciones (logística, seguridad, control de accesos).

**Historia:** Surgió durante la Segunda Guerra Mundial y se popularizó en los años 70.

## **JTAG (Diagnóstico y Depuración de Sistemas Digitales):**

**Definición:** JTAG es un estándar de interfaz (IEEE 1149.1) utilizado para depuración, pruebas de hardware y programación de circuitos digitales.

### **Funciones principales:**

**Pruebas de hardware:** Detecta problemas de conexión en placas electrónicas sin necesidad de sondas físicas.

**Depuración de software:** Monitorea registros y memoria en tiempo real, aunque puede ralentizar el sistema.

**Programación In-Circuit:** Permite cargar firmware directamente en dispositivos como FPGAs.

**Ventajas:** Eficiencia, facilidad para detectar errores, actualizaciones in situ.

**Desventajas:** Complejidad en el diseño, uso de recursos del sistema y posibles riesgos para el hardware.

**Aplicaciones:** Telecomunicaciones, defensa, medicina, IoT.

**Limitaciones:** Velocidad limitada, difícil de usar en circuitos no diseñados para JTAG, riesgos de seguridad.

# Tema 5 - Periféricos: sensores y actuadores.

## Interfaz digital:

Basados en lógicas TTL y CMOS: - TTL (Transistor-Transistor Logic): Operan con voltajes de 5V. SN7400.

- CMOS (Complementary Metal-Oxide-Semiconductor): Operan a 1'5V - 3'3V. 74HC (alta velocidad) y 74HCT (compatibles TTL)

Protección de entradas digitales: los diodos ESD (Electro Static Discharge) suelen usarse para proteger descargas electrostáticas, evitando daños a circuitos sensibles, entradas de 3'3V.

Expansión de entradas y salidas digitales: - Entradas: 74257 (multiplexor 2 a 1) para expandir líneas de entrada.

- Salidas: 74HC259 (latch direccionable de 8 bits) y 74HC574 (flip-flop octal).

- Salidas de alta corriente: utilizarán transistores BJT para manejar mayores cargas.

## Interfaz analógico:

Sensores: son dispositivos fundamentales que convierten fenómenos físicos o químicos en señales eléctricas interpretables. Estas señales son procesadas por sistemas empotrados para monitorear, analizar y controlar diversos entornos.

- Sensor de aceleración: Tecnología MEMS (microelectromechanical System), detecta cambios de posición mediante una pequeña masa central; también basados en condensadores. LSM303D (3D accelerometer and 3D magnetometer module), se comunica con protocolo SPI o I2C.

- Giroscopio: sirven para medir la velocidad angular, es útil para detectar rotaciones. Consiste en un volante que, montado sobre un eje, es capaz de rotar libremente en cualquier dirección. Tipos:

· Mecánico: usan rotores internos que giran a alta velocidad, y cuando el giroscopio cambia su orientación, el rotor mantiene su posición, proporcionando información sobre la dirección del cambio. Usado en barcos y aviones para la navegación. Componentes: bastidor, eje de giro, cardán y el rotor.

· Fibra óptica: usa el efecto Sagnac, se divide un haz de luz y se envía por fibras ópticas enrolladas en direcciones opuestas.

· Láser: usa el efecto Sagnac, tiene una cavidad cerrada con espejos en los vértices, un láser se genera y se divide en dos haces desplazados en direcciones opuestas.

· MEMS: funcionan mediante la detección de la fuerza de Coriolis, cuando el dispositivo rota, se genera una fuerza detectada por los sensores MEMS.

Aplicaciones: estabilización de drones, juegos (Wii), y orientación de satélites.

- Sensor de proximidad: capaz de detectar la presencia o la distancia de objetos cercanos sin necesidad de contacto físico, hay distintos tipos de sensores de proximidad:
  - Capacitivos: miden la capacidad de un objeto de almacenar carga eléctrica.
  - Inductivas: utilizan un campo electromagnético que cambia al detectar metales cercanos.
  - Infrarrojos: detectan objetos mediante la reflexión de luz infrarroja.
  - Láseres: utilizan un haz de luz láser para medir distancias.
  - Ultrasónicos: emiten ondas de sonido de alta frecuencia y miden el tiempo que tarda la onda en rebatir.
  - ToF: miden el tiempo de vuelo de un haz de láser reflejado. Ej: sensores ToF con precisión milimétrica.

Se suelen usar para el estacionamiento en automóviles, teléfonos móviles y seguridad industrial.

- Sensor de humo: es un dispositivo diseñado para detectar la presencia de humo en el aire, se componen de un detector, un procesador y un sistema de alerta. El detector identifica la presencia de humo, el procesador analiza la señal y el sistema de alerta emite un aviso sonoro o luminoso ante una emergencia. Hay dos tipos: iónicos (basadas en dos placas internas que funcionan junto a un material radioactivo, cuando detectan partículas de combustión, se activa un circuito eléctrico que a su vez activa las dos placas para proceder al envío de una señal de alerta) y ópticas (responden a cambios en la luz utilizando un emisor de luz y un fotosensor, estos cambios son provocados por el humo).

- Sensor de presión: es un dispositivo capaz de medir la presión de gases o líquidos. Se comunica a través de la interfaz I2C. Ejemplo: BMP180, monitoriza presión (30 - 110 KPa) y temperatura, usado para medir la altitud y el nivel del agua.

Actuadores: convierten una señal digital en un estímulo físico. Tipos:

- De control industrial: sistemas neumáticos, movimiento.
- Ópticos: leds, lcd, display.
- Motores: corriente continua (movimiento continuo basado en señales), motor paso a paso (rotaciones discretas por señales escalonadas) y servomotores (sistema de lazo cerrado usado en discos duros y robótica).
- Acústicos: altavoz, zumbador.

Conversores A/D y D/A: transforman señales analógicas en digitales y viceversa:

- A/D → métodos: flash, aproximaciones sucesivas
- D/A → reconstrucción de señales mediante filtrado e interpolación.

PWM (Pulse Width Modulation): técnica para controlar la potencia entregada a actuadores.

Procesamiento de señal: se refiere a la manipulación de señales dig./analog. para extraer información útil.

Operaciones comunes: filtrado (elimina ruido o señales no deseadas), compresión (reduce la cantidad de datos necesarios para representar la señal) y análisis espectral (examina las frecuencias presentes en una señal).

Todas las señales periódicas pueden representarse como una suma de funciones coseno de diferentes amplitudes y frecuencias.

# Tema 6 . - Integración, coste y prestaciones

## Introducción: límites en los tiempos de ejecución

El tiempo de ejecución de una instrucción está limitado por los siguientes dos casos:

- Límite inferior: la instrucción funciona sin problemas: hay acierto de cache, los operandos están preparados, no hay conflicto de recursos con otras instrucciones
- Límite superior: va todo mal, no hay acierto de cache, operandos no preparados, conflictos de recursos con otras instrucciones.

WCET y BCET: el tiempo de ejec. se evalúa entre el peor caso (WCET) y el mejor caso (BCET).

## Herramienta de análisis de tiempos de ejecución

- Predicción del comportamiento del procesador: puede ser la cache (capacidad, tamaño de linea, asociatividad, técnica de reemplazo, información sobre aciertos/fallos) o el pipeline (tiempo que pasa una instrucción en él).
- Análisis de caminos: computar un límite superior de todos los tiempos de ejecución de todos los posibles caminos del programa.

Se usan bloques básicos: secuencias de instrucciones en las que el flujo de control entra al principio y sale al final, sin saltos. Ej: lazos, condiciones, funciones. Para cada bloque se estudian los accesos a memoria y su efecto en cache, y un análisis de su ejecución en un pipeline determinado.

## Ánalisis de rendimiento de sistemas distribuidos:

Estos sistemas incluyen componentes hardware que se comunican mediante redes, interactuando con sensores y actuadores que definen la velocidad de operación.

### Métodos:

- Basadas en simulación: se modela el comportamiento dinámico del sistema para analizar interacciones y estimar el rendimiento promedio. Son útiles para estimar el caso de rendimiento medio, pero no para el caso peor.
- Basadas en planificación integral: planifica las comunicaciones como una computación más. Permite mezclar sistemas disparados por eventos con otros por tiempo. El procesamiento y las comunicaciones se dirigen por la ocurrencia de eventos y el paso del tiempo.
- Basados en composición: adecuado para sistemas distribuidos complejos con arquitecturas heterogéneas, concurrencia y eventos múltiples. Se estiman los WCET y BCET bajo diferentes políticas de planificación y patrones de llegada de eventos.

## Consumo en sistemas empotrados:

Modelo de consumo y energía: La disipación de potencia puede ser dinámica (provocada por los cambios de estado  $\rightarrow P \sim C \cdot V_{DD}^2 \cdot f \cdot r$  r: fracción de transistores que conmutan) o estática (entre conmutaciones del circuito debido a las fugas sub-umbrales, aumenta con tecnologías más avanzadas  $\rightarrow P \sim V_{DD} \cdot N_{tran} \cdot K_{design} \cdot I_{leak}$ ). Para poder realizar estimaciones a nivel de sistema son necesarios modelos:

- Modelo a nivel de función e instrucción: analiza cuánto consume cada operación del procesador, útil para optimizar bloques específicos de instrucciones.
- Modelo de microarquitectura: simula el comportamiento del procesador considerando ciclos individuales, jerarquías mem. y otros.
- Modelo de memoria y bus: estima el consumo basado en la configuración de memoria y la freq. de acceso.
- Modelo de batería: relación no lineal entre la corriente extraída y la capacidad disponible:  $C = K / t^\alpha$ , donde  $\alpha$  varía.

Optimizaciones a nivel de aplicación/sistema: Durante el diseño, es necesario obtener una relación consumo/vida de la batería/rendimiento, por ejemplo los sistemas con celdas solares harían la mayor parte del trabajo durante el día. Para ello, existen una serie de estrategias de optimización:

- Escalamiento de frecuencia y voltaje: las reducciones en  $V_{DD}$  disminuyen mucho el consumo dinámico, pero pueden requerir bajar la frecuencia para mantener el funcionamiento estable.
- Escalamiento dinámico de los recursos: inhabilita total o parcialmente los componentes.
- Selección del core del procesador: uso de procesadores especializados como ASIPs (Application-Specific Integration Processors) y DSPs (Digital Signal Processors).
- Selección del subsistema de memoria: reduce el consumo en cachés mediante estrategias como: prefetching (anticipa los datos necesarios para evitar accesos repetidos a memoria externa) y la compresión de código (reducir el tamaño del software para disminuir accesos a memoria). Peores soluciones: grandes caches muy asociativas.

Optimización del interconexión:

- Bus splitting: divide los buses en segmentos para minimizar transferencias innecesarias.
- Bus invert coding: reduce los cambios de estado en los buses para disminuir pérdidas dinámicas.

Seguridad:

- Parámetros de seguridad: confidencialidad, integridad, disponibilidad, autenticación y no repudiable.
- Niveles de implementación de seguridad: físico, hw, fallos del sw y red.
- Tipos de fallos: estáticos o programables.

Restricciones de seguridad: energía (especialmente en sistemas basados en batería, como criptografía) y la capacidad de procesamiento (que sean flexibles, adaptables, pero teniendo en cuenta el coste).

Diseño de Sistemas Empotrados seguros:

- A nivel de diseño: resistencia a manipulación, protección de memoria, protección IP, comunicaciones.
- A nivel de aplicación: identif. de usuario y control de acceso, protección de apps IP, protección frente a virus y código malicioso.

Criptografía en Sistemas Empotrados: es la solución a muchos problemas de seguridad. } Problemas: consume y requiere mucha memoria.  
Soluciones: inst. que consuman y tarden lo mismo.