

NUEVAS TECNOLOGÍAS
APLICADAS A LA GESTIÓN (E66)
5º INGENIERÍA EN INFORMÁTICA

Tema 4.

**Estructura Interna de
una Tarjeta Inteligente.**

- 1.- Introducción.
- 2.- Interface con la Unidad de Lectura/Escritura.
 - 2.1.- Tarjetas con Contactos.
 - 2.2.- Tarjetas sin Contactos.
- 3.- Tipos de Microprocesadores.
- 4.- Tipos de Memoria.
- 5.- Hardware Adicional.

(Capítulo 4 del Zoreda)

(Capítulo 3 del RankI)

INTRODUCCIÓN

Planteamiento

- Una tarjeta inteligente se puede considerar como un ordenador personal, aunque un tanto especial.
- Dicha afirmación se basa en el hecho que posee todos los elementos típicos de un ordenador personal.
- En primer lugar presenta un interface con el exterior, a través de unos elementos pasivos, que en este caso aparecen en la unidad de lectura/escritura.
- También aparecen un conjunto de elementos necesarios para el procesamiento de datos, como es el procesador y la memoria.
- Y además posee una serie de elementos que facilitan la labor del sistema, como el circuito de reloj, los circuitos de protección, etc.
- Todos estos elementos son gestionados por un sistema operativo, que en este caso se suele denominar Mascara.
- Sobre ésta es posible desarrollar pequeñas aplicaciones que explotan las características del hardware y las habilidades del sistema operativo.
- En este tema se describen los elementos físicos que componen una tarjeta inteligente, así como la funcionalidad de cada uno de ellos.

INTERF. EN TARJETAS CON CONTACTOS

Planteamiento

- En este tipo de tarjetas, el diálogo se realiza a través de la matriz de contactos situada en la superficie de la tarjeta.
- La posición y las dimensiones de esta matriz de contactos aparecen definidos en el estándar ISO 7816/2.
- La matriz está compuesta de 8 contactos, con una estructura espacial de 4x2.
- Los contactos se nombran como Cx, donde x se enumera de 1 a 8, de arriba a abajo y de izquierda a derecha.
- La dimensión mínima que debe tener un contacto es 1.7 mm x 2 mm.
- Los contactos se fabrican de cobre recubierto de una fina capa de oro o de una aleación de paladio y plata.
- La matriz de contactos se pueden fijar sobre un soporte de fibra de vidrio, en el que también se fija, pero en su reverso, el circuito integrado.
- La conexión entre los contactos y el circuito se realiza a través de cables extremadamente finos de oro o aluminio.
- La unión entre estos cables y los elementos a conectar se puede realizar mediante el uso de ondas ultrasónicas o mediante la aplicación de calor y presión.

INTERF. EN TARJETAS CON CONTACTOS

Funcionalidad de los contactos

- Seguidamente se describe la definición de los contactos de una tarjeta inteligente.
- C1 (Vcc). Este contacto suministra la tensión y la intensidad necesaria para el funcionamiento del circuito integrado de la tarjeta.
- C2 (RST). Este contacto es el encargado de transmitir la señal de reset a la tarjeta, que inicia su diálogo con el terminal.
- C3 (CLK). Aporta la frecuencia que marca la transmisión del ATR y el funcionamiento del procesador.
- C5 (GND). A través de este contacto se aporta la señal de tierra utilizada como referencia para el resto de señales transmitidas.
- C6 (Vpp). Aporta el voltaje e intensidad que requiere la memoria EEPROM para su grabado y borrado.
- C7 (I/O). Sobre este contacto se produce la transmisión de información entre la tarjeta y el terminal.
- Los contactos C4 y C8 no tienen asignada una tarea específica, pudiéndose optar por,
 - No incluir estos contactos en las tarjetas, en cuyo caso la tarjeta sólo posee 6 contactos.
 - Utilizar estos contactos para otros usos, en los que se incluye la definición de otro contacto de I/O.

INTERF. EN TARJETAS CON CONTACTOS

Valores de Tensión

- Inicialmente se utilizaban circuitos TTL en los que se requería una tensión de 5 V.
- Hoy en día se utilizan otro tipo de tecnología, como MOS y CMOS, que no requieren esta tensión pero que pueden funcionar con ella.
- Por su parte, las tarjetas GSM sólo requieren 3 V por lo que deben incluir un conversor en los teléfonos que realice este cambio de tensión.
- En un futuro, las tarjetas inteligentes funcionarán en un rango de tensión de 3 a 5 V, por lo que se evitarán problemas como la inserción de una tarjeta en un lector con tensión no adecuada.
- Esta hecho no tiene ninguna influencia sobre el funcionamiento de los elementos del circuito integrado.
 - Este rango de tensión va a ser obligatorio para todos los procesadores
 - Resulta muy complejo integrar memorias EEPROM con este rango de tensión, aunque ya se han desarrollado.

INTERF. EN TARJETAS CON CONTACTOS

Valores de Intensidad

- El consumo del circuito integrado de la tarjeta depende en gran medida de la frecuencia de funcionamiento, y en menor medida de la temperatura.
- La intensidad máxima de funcionamiento varía en función del estándar que se analice.
 - El estándar ISO 7816/3 especifica un valor máximo de 200 mA.
 - Por su parte el estándar GSM 11.11, sólo admite hasta 10 mA.
- Estos valores se pretenden revisar a la baja.
- La mayoría de circuitos no requieren un nivel de 200 mA para su funcionamiento pero estos consumos pueden llegar a aparecer ciertos picos de consumo muy cortos.
- Para evitar su influencia, se puede poner un condensador que resuelva el problema.
- Algunas tarjetas presentan un modo de ahorro de energía en el que,
 - El procesador pasa a un estado de consumo mínimo.
 - La RAM y la circuitería asociada a I/O permanecen activos.
 - El resto de circuitos se desconectan.
- De este modo se produce un ahorro de energía, de gran utilidad en teléfonos móviles.

INTERF. EN TARJETAS CON CONTACTOS

Programación de la EEPROM

- La tecnología disponible en los primeros años de las tarjetas inteligentes, manejaba una memoria EEPROM que requería una tensión e intensidad externas.
- Por esta razón, se incluyó un contacto por el cual se suministraran los valores requeridos.
- Este contacto podía presentar dos estados diferentes,
 - Activo, en el que suministra la intensidad y la tensión necesaria para la programación de la EEPROM.
 - Inactivo, en la que se aportan unos valores mas bajos de intensidad y tensión.
- El estado de este contacto era controlado por la propia tarjeta a través de la información que envía a través de I/O.
- En la actualidad se integra tanto la EEPROM como el generador que aporta las tensiones e intensidad necesarias para su programación.
- Por esta razón, este contacto resulta inútil en la mayoría de los casos, aunque debe de seguir manteniéndose por compatibilidad.

INTERF. EN TARJETAS CON CONTACTOS

Señal de Reloj

- En las primeras tarjetas inteligentes podía aparecer un circuito de generación de reloj, por lo que la señal recibida por la tarjeta no era utilizada para el funcionamiento general de la tarjeta.
- Su uso se centraba en la fase de inicialización de la tarjeta, es decir, cuando se enviaba la señal de reset y se respondía con el ATR.
- El resto de las operaciones se ajustaba a la frecuencia especificada en el ATR.
- Este planteamiento se sigue manteniendo en la actualidad, aunque las tarjetas ya no suelen tener circuito de reloj interno.
- La señal de reloj definitiva se utiliza en dos aspectos,
 - La transmisión de datos a través de I/O
 - Frecuencia del procesador.
- En el segundo de los casos, no es necesario que el procesador actúe exactamente a la señal de reloj transmitida, sino que es posible modificarla.
- Así, algunos de los procesadores incluye un multiplicador de la señal de reloj, con el objeto de aumentar la velocidad del procesador.
- Habitualmente se utiliza un multiplicador de 2.

INTERF. EN TARJETAS CON CONTACTOS

Transmisión de Datos

- La transmisión de los datos se realiza a través de I/O mediante un método de comunicación half-duplex y bidireccional.
- Por tanto, existe dos modos de funcionamiento
 - Transmisión: Emisión Tarjeta -> Terminal.
 - Recepción: Emisión Terminal -> Tarjeta.
- Tanto la tarjeta como el terminal poseen dos niveles de tensión para indicar que ellos están preparados para enviar o recibir.
- Cuando ninguno de ellos desea enviar, la línea pasa a nivel alto.
- Si alguno de ellos desea transmitir, la línea pasa a nivel bajo indicando esta circunstancia.
- Este comportamiento está controlado por la circuitería asociada a la línea que incluye una resistencia de pull-up.
- Mediante esta resistencia se evita que el envío de dos señales a nivel alto, con su consumo de intensidad asociado, genere algún problema en los circuitos de la tarjeta o del terminal.

INTERF. EN TARJETAS SIN CONTACTOS

Planteamiento

- El terminal debe de enviar y recibir información de la tarjeta para que esta funcione de un modo adecuado.
- Tensión.
- Señal de Reloj.
- Datos desde la Tarjeta.
- Datos a la Tarjeta.
- Cuando no existen contactos resulta necesario habilitar algún modo alternativo para realizar esta transferencia de información.
- Se han desarrollado diferentes técnicas con diferentes propiedades, incluso algunos de ellas de uso exclusivo.
- Las más comunes son:
 - Transmisión por Microondas.
 - Transmisión Óptica.
 - Acoplado Capacitivo.
 - Acoplado Inductivo.
- Las dos últimas son las más habituales en este ámbito, debido al formato de las tarjetas, por lo que se han definido como estándares.
- Y de éstas dos, la última puede ser utilizada para la transmisión de la tensión y de los datos.

INTERF. EN TARJETAS SIN CONTACTOS

Consumo y Distancia de Funcionamiento

- El consumo de una tarjeta sin contactos define su rango de funcionamiento, es decir, cuál es la distancia máxima a la que puede funcionar.
- Las tarjetas asociadas al control de acceso a una zona reservada, sólo realizan operaciones de lectura de información.
- Esta operación sólo consume décimas de μW , y por tanto pueden actuar hasta a un metro de distancia.
- Si una tarjeta debe soportar operaciones de escritura de información, su consumo puede llegar a $100 \mu\text{W}$, por lo que su distancia se limita a tan sólo 10 cm.
- Por último, las tarjetas con microprocesador requieren un consumo de 100 mW , por lo que la distancia de funcionamiento se reduce a unos pocos milímetros.
- Independientemente de la distancia máxima de funcionamiento, todas las tarjetas basadas en el acoplamiento por inducción se basan en las propiedades electromagnéticas de las bobinas.
- La única diferencia aparece en la frecuencia de la corriente portadora, que varía entre 100-300 kHz y llega hasta algunos MHz.
- Por su parte, el acoplamiento capacitivo se basa en las características capacitivas de dos superficies próximas.

INTERF. EN TARJETAS SIN CONTACTOS

Acoplamiento Inductivo

- La transmisión de información se produce a través de las propiedades electromagnéticas de las bobinas.
- De un modo esquemático se puede enunciar del modo siguiente,
 - En el terminal y en la tarjeta aparecen una o más bobinas.
 - Cuando aparece una corriente eléctrica en la bobina del terminal se produce un campo magnético.
 - Éste genera una diferencia de potencial en la bobina de la tarjeta.
 - Si la bobina aparece en un circuito cerrado, se genera una corriente eléctrica que da lugar a un nuevo campo magnético.
 - La intensidad de este campo magnético puede ser modificado, al cambiar el diseño del circuito cerrado de la tarjeta.
 - El terminal puede detectar las variaciones de este campo magnético en su bobina, ya que también es influenciada por la bobina de la tarjeta.
- Habitualmente la corriente que circula en la bobina es alterna, y su frecuencia se denomina frecuencia portadora.
- La transmisión de información puede ser diferente en la tarjeta y en el terminal, siendo habitual el modulado de la fase.

INTERF. EN TARJETAS SIN CONTACTOS

Estándares ISO

- El estándar ISO 10536 caracteriza a las tarjetas con circuitos integrados y sin contactos, que funcionan a una distancia muy corta.
- En la actualidad están definidas las partes,
 - 1 Características Físicas.
 - 2 Dimensiones y Localización de Áreas de Acoplamiento.
 - 3 Señales Electrónicas y Funcionamiento del Reset.
 - 4 ATR y Protocolos de Transmisión.
- El contenido de este estándar se puede resumir como sigue,
 - Externamente una tarjeta sin contactos se parece a una tarjeta con contactos, en la que también es posible incluir contactos.
 - Se habilita la posibilidad del acoplamiento inductivo y del capacitivo.
 - Por tanto, los lectores y las tarjetas pueden soportar ambos tipos de comunicación.
- Por su parte, el estándar relativo a las tarjetas de mayor distancia, ISO 14443, todavía se encuentra en periodo de desarrollo.
- Es por ello que se supone que el mercado definirá cual será el estándar a seguir.

TIPOS DE MICROPROCESADORES

Planteamiento

- Los microprocesadores utilizados en el ámbito de las tarjetas inteligentes son ordenadores completos, con su procesador, memoria y un interface con el mundo exterior.
- Existen diferentes tipos de memoria, ROM, RAM y EEPROM, cada una con una funcionalidad distinta.
- Por su parte el circuito de E/S suele ser una unidad específica que el procesador puede direccionar como una posición de memoria.
- Algunos fabricantes incluyen otras unidades que facilitan la tarea del procesador, como coprocesadores.
- Estos microprocesadores deben cumplir una serie de características básicas,
 - Coste de Fabricación Mínimo, eliminando los elementos que no son necesarios.
 - Funcionalidad, que requiere la inclusión de los elementos necesarios.
 - Seguridad, con lo que se incluyen todos los elementos necesarios para posibilitar un buen nivel de seguridad activo y pasivo.
 - Minimización del Tamaño del Chip, evitando su ruptura por cualquier agresión externa.
 - Disponibilidad Reducida, para eliminar la posibilidad de un duplicado del chip.

TIPOS DE PROCESADORES

Planteamiento

- La elección del procesador a utilizar es uno de las decisiones más importantes.
- La Fiabilidad del procesador es uno de los aspectos a considerar.
- Es por ello que se suelen utilizar procesadores bien conocidos y que han sido probados en diferentes ámbitos.
- De este modo, el proceso de fabricación y el funcionamiento del procesador resultan muy seguros.
- También facilita el desarrollo de los sistemas operativos, ya que sus programadores poseen librerías ajustados a los procesadores.
- La Velocidad de Proceso también debe ser considerada, aunque en este caso no se requiera una gran velocidad de proceso.
- Otra consideración es la Capacidad de la Tarjeta, que suele estar entre 8 Kb y 30 Kb.
- Ambas consideraciones aconsejan el uso de procesadores de 8 bits, en los que se incluyen un bus de direcciones de 16 bits.
- El conjunto de instrucciones suele ser del tipo CISC, y coincidente con el del Motorola 6805 o el del Intel 8051.
- En algún caso puede utilizarse una arquitectura RISC de 16 bits, como el Hitachi H8.

TIPOS DE MEMORIAS

Planteamiento

- Como en un ordenador, una tarjeta inteligente requiere diferentes tipos de memoria para almacenar datos con propiedades distintas,
 - Memoria de Consulta, en la que información sólo puede ser consultada.
 - Memoria de Almacenamiento Variable, que contienen los datos que se modifican.
 - Memoria Volátil, en la que se almacenan los datos intermedios.
- Para el primer tipo de memoria suele utilizarse la memoria ROM, cuyo contenido se imprime en el proceso de fabricación.
- Para el segundo tipo, existe una gran variedad de memorias,
 - EPROM, utilizada en los primeros tiempos.
 - EEPROM, cuyo uso es el más extendido.
 - Flash-EEPROM y FRAM, que son las opciones de futuro en este ámbito.
- La memoria volátil se construye con RAM, que puede ser Estática o Dinámica.
 - Inicialmente se utilizó la DRAM debido a su sencillez.
 - En la actualidad se utiliza SRAM, ya que no requiere refresco, por lo que se puede eliminar la señal de reloj.

TIPOS DE MEMORIAS

Características

- Resulta de gran interés analizar las diferentes memorias de almacenamiento no volátil que aparecen en el mercado.
- La memoria EPROM sólo puede ser borrado mediante la interacción de rayos ultravioletas, por lo que su uso en tarjetas inteligentes no es interesantes.
- La memoria EEPROM es la más utilizada en la actualidad, aunque presenta una serie de inconvenientes que deben considerarse,
 - Su programación, tanto escritura como borrado, requiere una tensión de 17 v.
 - Para alcanzar esta tensión, se debe incluir un circuito específico, denominado Bomba de Carga o Charge Pump.
 - Su coste suele ser bastante alto.
 - El ciclo de escritura suele ser de 3-10 ms.
- Por su parte la memoria Flash-EEPROM, con una tecnología similar EEPROM, pero,
 - La tensión de programación es 12 v.
 - El ciclo de escritura es de 10 μ s.
- La FRAM es la memoria más moderna, con una tensión de programación de 5 v y un ciclo de escritura de 100 ns.
- Pero requiere cierto refresco, lo que impide su introducción en este ámbito.

OTRAS UNIDADES

Coprocesadores

- Los algoritmos de cifrado de información mediante clave pública requieren el cálculo de exponenciales y el cálculo del módulo de grandes números.
- El coste de estos algoritmos suele ser bastante alto por lo que se utilizan circuitos específicos.
- Estos circuitos manejan palabras de 140 bits, y pueden mejorar, hasta 6 veces, la velocidad de un PC.
- Cuando se requiere realizar una operación de este tipo, el procesador ordena su desarrollo al coprocesador, y espera a que este termine.

Generador de Números Aleatorios

- Los procesos de autenticación requieren la generación de un número aleatorio real, que no sea pseudo-aleatorio.
- Dicho número no debe ser predecible desde el exterior, por lo que no debe relacionarse con ninguna de las informaciones recibidas por la tarjeta, como la tensión o la temperatura.
- Su valor se suele construir a través de varios estados lógicos del procesador, como el contenido de los registros.
- El valor obtenido se introduce en un registro de desplazamiento en bucle cerrado, a partir del cual es posible generar los números aleatorios.

OTRAS UNIDADES

Detección de Errores en la EEPROM

- El límite de la vida de la tarjeta se asocia con el de la memoria EEPROM que contiene.
- Con el objeto de aumentar al máximo su ciclo de vida, se pueden incluir algoritmos para la detección y corrección de errores.
- Si se desea un algoritmo realmente efectivo, el tamaño del código puede llegar a ocupar la mitad de la capacidad de la tarjeta.
- Este hecho provoca una dura decisión, entre la capacidad real de la tarjeta y su ciclo de vida.

Transmisión de Datos vía Hardware

- Cuando se desea aumentar la velocidad de transmisión de los datos, no resulta interesante el control vía software, ya que ésta se limita por la velocidad del procesador.
- La mejor alternativa es el diseño de un circuito que posibilite este aumento de la velocidad de transmisión.
- Este circuito, denominado Transmisor Receptor Asíncrono Universal, ocupa una región del chip mayor que el programa almacenado en memoria.
- Este es uno de los problemas básicos de su desarrollo, aunque el aumento en la escala de integración resolverá dichos problemas.

OTRAS UNIDADES

Doblado del Reloj Interno

- Con el paso del tiempo, se requiere una mayor capacidad de procesamiento de las tarjetas.
- Dicho aumento se puede obtener mediante el duplicado de la señal de reloj externa.
- Este aumento permite aumentar la frecuencia de funcionamiento de diferentes unidades, como el procesador, las comunicaciones y los coprocesadores.
- El mayor problema se presenta en el aumento de la corriente que requiere el procesador, sobre todo en terminales cuya alimentación se basa en una batería.

Manejo de la Memoria vía Hardware

- Los últimos sistemas operativos desarrollados para tarjetas inteligentes permiten la inclusión de código ejecutable en su memoria.
- La carga de estos programas es controlado por el sistema de claves de la tarjeta, aunque su posterior ejecución no suele ser controlada.
- Así, estos programas pueden acceder a zonas reservadas y modificar su contenido, pudiendo modificar el valor de las claves.
- Para evitar estos problemas es posible incluir una MMU en la tarjeta, que permite verificar la ejecución de los programas, controlando que accede a las zonas de memoria adecuadas.