

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

Tema 7.
Protocolo de una
Tarjeta Inteligente.

- 1.- Introducción.
- 2.- Nivel Físico.
- 3.- Protocolos de Transmisión.
- 4.- Protocolo de Comunicación.
- 5.- Proceso de Reinicio de la Tarjeta.

(Capítulo 5 del Zoreda)

(Capítulo 6 del RankI)

INTRODUCCIÓN

Planteamiento

- El objetivo de este tema es la descripción del diálogo entre una tarjeta y su terminal.
- Con este fin se presentan las diferentes fases en las que se descompone dicho diálogo,
 - Inicialización de la Tarjeta.
 - Respuesta de la Tarjeta.
 - Selección del Tipo de Protocolo.
 - Diálogo con el Protocolo Seleccionado.
 - Desconexión de la Tarjeta.
- Además resulta fundamental analizar el modo en el que la información fluye desde la tarjeta al terminal y viceversa.
- Siguiendo el modelo de comunicación ISO/OSI se distinguen varias capas, que se caracterizan de modo diferente,
 - Nivel Físico (Nivel 1), que describe el modo en el que los bits se transmiten a través del canal de comunicación.
 - Protocolos de Transmisión (Nivel 2), en el que se indican las estructuras utilizadas en el intercambio de información.
 - Instrucciones (Nivel 7), que describen cual es la estructura de los comandos de la tarjeta y el terminal.
- La relación entre estos niveles es básica para obtener una buena comunicación .

NIVEL FÍSICO

Planteamiento

- Cuando se trata la transmisión de información desde un punto de vista físico, es necesario el estudio de diferentes aspectos.
- Todos estos aspectos se pueden englobar en dos grandes grupos,
 - Transmisión de un bit.
 - Transmisión de un byte.
- Entre los primeros cabe destacar los siguientes aspectos,
 - Niveles de tensión válidos.
 - Interpretación de cada uno de estos niveles.
 - Dimensión de un bit.
 - Detección de un bit.
- Por su parte, los aspectos relacionados con la transmisión de un byte son,
 - Dimensión de un byte de información.
 - Interpretación de los bits de un byte.
 - Separación entre bytes.
- Seguidamente se describen los dos tipos de transmisión, en el que se puede constatar la interconexión existente entre aspectos de los dos grupos.

TRANSMISIÓN DE UN BIT

Niveles de Tensión

- Tanto la lógica binaria como la transmisión de información mediante tensión, sólo soportan dos valores válidos.
 - La lógica binaria acepta los valores 0 y 1.
 - La transmisión mediante tensión soporta los valores 0 y 5 voltios.
- Se puede observar fácilmente que existen dos posibilidades de correlación.
- Lo más común y sencillo es hacer corresponder el 0 lógico con 0 V, y el 1 lógico con 5 V, pero no tiene porque ser ésta la opción elegida.
- Para evitar ambigüedades cuando no se usa la opción anterior, los valores lógicos se suelen denominar del modo siguiente,
 - Z, o marca, es el valor alto.
 - A, o espacio, es el valor bajo.
- A partir de esta definición, se presentan las dos opciones posibles como sigue,
 - Convención Directa, si $Z = 5\text{ V} / 1\text{ lógico}$.
 - Convención Inversa, si $A = 5\text{ V} / 1\text{ lógico}$.
- El valor utilizado en una comunicación se debe definir antes de iniciarse la comunicación.
- Es por ello, que su valor aparece en el primer byte de información transmitido entre la tarjeta y el terminal.

TRANSMISIÓN DE UN BIT

Dimensión

- La Unidad de Transmisión Elemental, o t_{eu} , mide el tiempo necesario para transmitir un bit a través del canal de comunicación.
- Su valor se relaciona con la Frecuencia de la señal de reloj que el terminal suministra a la tarjeta.
- Los valores más comunes son 3.5712 y 4.9152 MHz, que corresponden con los osciladores más habituales y por tanto más baratos.
- Este valor es modificado por un Divisor a través del cual es posible fijar la velocidad de la transmisión de información, cuyo valor habitual es 9600 bits/s.
- Este valor no puede ser demasiado bajo, ya que indica el número de ciclos que requiere el sistema operativo de la tarjeta para recibir y transmitir información.
- Sin la inclusión de unidades de uso específico, la reducción de este divisor requiere un código mayor, reduciendo el espacio de memoria útil en la tarjeta.
- La inclusión de estas unidades permite un incremento significativo de la velocidad de transmisión hasta un valor de 111.6 kbit/s.
- Este valor se puede considerar que es la cota máxima a la que pueden actuar las tarjetas en la transmisión de información.

TRANSMISIÓN DE UN BIT

Detección

- Dado que la mayoría de tarjetas no poseen una unidad específica para la transmisión de la información, su interpretación suele realizarse mediante soluciones software.
- Estas soluciones incluyen una serie de técnicas que permiten la detección correcta de un bit.
- La primera de estas técnicas permite un cierto error en la temporización de las señales de los bits de un byte.
- Este error se cifra en ± 0.2 etu, por lo que en la realidad, únicamente una señal de tamaño 0.6 etu es utilizada en la detección.
- También resulta interesante prevenir posibles imperfecciones en la señal, como puede ser la superposición de una señal de ruido.
- Para ello, la captura del bit correspondiente no debe realizarse una única vez, sino que se realizan lecturas consecutivas que permiten reducir la aparición de una mala detección.
- Lógicamente, estas lecturas deben distribuirse homogéneamente a través de la dimensión válida del bit, cuyo tamaño es 0.6 etu.
- La más habitual es realizar tres lecturas, con una distancia de 0.15 etu entre ellas.
- No se necesita la utilización de un número mayor de lecturas, ya que la transmisión entre la tarjeta y el terminal es bastante buena.

TRANSMISIÓN DE UN BYTE

Descripción

- La transmisión entre una tarjeta inteligente y su terminal suele realizarse de modo asíncrono, por lo que resulta necesaria la inclusión de bits de sincronización.
- Inicialmente la línea aparece a nivel Z, durante un tiempo no determinado.
- Un byte se inicia con la aparición de un flanco que pasa a la línea al estado A durante un tiempo igual a un etu .
- Posteriormente se envían los 8 bits que forman el byte, que se realiza de acuerdo al siguiente criterio,
 - Convención Directa, se envía en primer lugar el bit menos significativo del byte.
 - Convención Inversa, en la que se transmite el bit más significativo en primer lugar.
- A continuación aparece un bit de paridad que permite que el número de valores lógicos 1 sea par, que permite cierto control de errores.
- Para finalizar la comunicación de un byte se transmiten uno o dos bits de parada a nivel Z.
- Este proceso se repite para cada uno de los bytes que se deseen transmitir.
- Es importante destacar, que la acumulación de los errores de temporización de los bits que componen el byte, no deben superar la cota establecida de $0.2\ etu$.

PROTOCOLOS DE TRANSMISIÓN

Planteamiento

- El diálogo que se establece entre el terminal y el tarjeta se ajusta al modelo Cliente-Servidor, donde la tarjeta es el cliente y el terminal es el servidor.
- Es decir, el terminal solicita la ejecución de cierta instrucción, y la tarjeta le responde con el resultado de dicha instrucción.
- La información que fluye entre la tarjeta y el terminal posee una estructura que se ajusta a una serie de protocolos de transmisión.
- Estos protocolos se pueden englobar en dos grandes grupos,
 - Síncronos, que son comunes en las tarjetas de memoria.
 - Asíncronos, utilizados en las tarjetas con microprocesador.
- Existe una gran variedad de los primeros, cada uno para un tipo de tarjeta concreto, aunque existen algunos que se están convirtiendo en estándares de facto.
- Los protocolos asíncronos se nombran como T=x, donde x es un número entre 0 y 15.
- En la actualidad se ha definido cuales son las características de 5 de ellos, aunque sólo se ha publicado la definición de 3 de éstos.
- También aparece un protocolo que puede ser definido de modo diferente en cada país.

PROTOCOLOS SÍNCRONOS

Planteamiento

- Cuando un terminal desea acceder a la información que aparece en una tarjeta, sólo debe especificar su dirección de memoria.
- Así pues, las tarjetas de memoria se pueden entender como un dispositivo periférico que se conecta al terminal, que puede poseer zonas de memoria protegidas.
- Dada la simplicidad de la comunicación, la división en capas, definida en el estándar OSI, no tiene aplicación en este ámbito.
- La idea es utilizar un protocolo que sea sencillo y rápido, aunque esto da lugar a métodos que son muy dependientes de los circuitos de las tarjetas, y por lo tanto muy diversos.
- La simplicidad llega hasta el extremo de no incluir técnicas de detección de errores, como la inclusión de bits de paridad.
- Este hecho se basa en la baja probabilidad de aparición de los errores, ya que la frecuencia suministrada a la tarjeta también es baja, entre 10 y 100 kHz.
- La velocidad de transmisión de la información también se relaciona con la frecuencia que se le suministra a la tarjeta.
- En la actualidad sólo se ha estandarizado el contenido del ATR de estas tarjetas.
- Por esta razón, los terminales deben diseñarse con una gran versatilidad.

PROTOCOLOS SÍNCRONOS

Protocolo Telefónico

- Para mostrar el funcionamiento de este tipo de protocolo, se describe el de las tarjetas que incluyen el chip SLE 4403 de Siemens
- Este chip permite el acceso directo de los bits de su memoria, y las operaciones se realizan mediante la utilización de tres canales,
 - Canal Bidireccional, que es utilizado por la tarjeta y por el terminal para el intercambio de información.
 - Canal de Reloj, emitido por el terminal, que marca el ritmo de la transmisión de los datos.
 - Canal de Control, en el que el terminal indica la operación a realizar.
- La correcta utilización de los canales permite implementar las operaciones necesarias.
- El acceso a los datos se relaciona con el valor de un Registro de Dirección que indica cual es la dirección a la que se desea acceder.
- Su valor es inicializado a cero cuando se activa la tarjeta, y puede ser reinicializado mediante la ejecución de una instrucción específica.
- Otras operaciones son
 - Lectura de Datos e Incremento del Registro de Dirección.
 - Escritura de Datos.
 - Borrado de la Memoria

PROTOCOLOS SÍNCRONOS

Bus I²C

- A diferencia del protocolo anterior, en este bus no hace falta la aparición de un canal de control, ya que la información contenida en el canal bidireccional define la operación.
- Es por ello, que este bus se compone de sólo dos cables, al cual pueden estar conectados varios dispositivos.
- En un momento determinado, sólo uno de ellos puede controlar el diálogo, mientras que el resto escuchan.
- En este ámbito sólo aparecen dos elementos en la comunicación, el terminal que actúa como servidor y la tarjeta como el cliente.
- La transmisión se inicia mediante una señal de inicio y finaliza mediante una señal de parada, ambas suministradas por el terminal.
- Con posterioridad, se realiza un intercambio de información basada en mensajes cuyo tamaño es de un byte.
- Cada uno de estos mensajes deben verificarse mediante la transmisión de un reconocimiento, cuyo tamaño coincide con un ciclo de reloj.
- El primer byte transmitido indica la operación a realizar, lectura o escritura, y la dirección lógica de la tarjeta en el bus.
- Su utilización en el ámbito de las tarjetas se ha extendido en los últimos tiempos.

PROTOCOLO T = 0

Planteamiento y Nivel Físico

- Este protocolo fue utilizado en Francia en las primeras fases del desarrollo de las tarjetas inteligentes, debido a su sencillez y ocupación mínima de memoria.
- La unidad mínima de información transmitida en este protocolo es el byte, sobre el cual se pueden aplicar las técnicas de detección de errores descrita en el nivel físico.
- Así, si se detecta un error en la transmisión de un byte, sólo este byte se debe retransmitir.
- El receptor indica esta situación al emisor, modificando el valor del primer bit de parada antes de su finalización, llevando a nivel A la línea durante un *etu*.
- El uso de unidades específicas puede ser problemático, ya que tratan el *etu* de modo indivisible.
- La separación entre los bytes transmitidos se define a través de dos valores,
 - Tiempo de Guarda, que indica el retardo adicional que requiere la tarjeta para procesar un byte enviado desde el terminal.
 - Tiempo de Espera, como la separación máxima entre dos bytes consecutivos.
- El tiempo de guarda permite aumentar el número de los bits de parada.
- El valor de estos dos tiempos es definido en el ATR de la tarjeta.

PROTOCOLO T = 0

Estructura del Mensaje

- En este protocolo el terminal envía un mensaje en el que solicita a la tarjeta la ejecución de una determinada operación.
- El mensaje enviado por el terminal se divide en dos partes bien diferenciadas,
 - Bloque de Cabecera que incluye el código de la instrucción a realizar y sus parámetros.
 - Un Bloque de Datos, que es opcional, en donde se envían los datos requeridos.
- De un modo más concreto, la cabecera se compone de los siguientes 5 bytes,
 - CLA e INS, que codifican la clase y el código de la instrucción a ejecutar. El valor de CLA nunca puede ser igual a FF.
 - P1 y P2 incluyen los parámetros necesarios para completar la instrucción.
 - P3 indican el número de datos a transmitir entre el terminal y la tarjeta o viceversa.
- El sentido de la transmisión influye en el modo de interpretar el valor P3 igual a 0,
 - Si los datos fluyen del terminal, se indica que no existen datos a transmitir.
 - En caso contrario, se deben enviar 256 bytes.

PROTOCOLO T = 0

Byte de Proceso

- La transmisión de cada uno de los bloques se realiza de modo separada, y entre ellas la tarjeta debe transmitir un Byte de Proceso.
- Las diferentes acciones se codifican del modo siguiente,
 - NULL = 60, reinicia el tiempo de espera, lo que incrementa el tiempo de proceso de la tarjeta.
 - ACK, indica que la cabecera se ha recibido correctamente y el modo de transmitir el bloque de datos.
 - SW1 = 6X ó 9Y, donde X es distinto de 0, aparece cuando el terminal no debe transmitir el bloque de datos.
- El valor de ACK se relaciona con el valor de INS, aunque con las siguientes modificaciones,
 - Si la instrucción requiere una activación del valor del contacto Vpp, se incrementa en 1 el valor de INS.
 - Independientemente de este comentario, si la tarjeta desea recibir los bytes de modo individual se envía el valor negado.
- Cuando se desea enviar el bloque de datos de modo individual, cada uno de ellos debe ser respondido por un byte de proceso.
- La tarjeta puede recibir los primeros bytes de modo individual, y posteriormente recibir el resto del mensaje.

PROTOCOLO T = 0

Respuesta de la Tarjeta

- Si la tarjeta debe responder con un conjunto de bytes, como respuesta a una solicitud del terminal, esta se produce a continuación del bloque de cabecera.
- La comunicación finaliza cuando la tarjeta envía los bytes SW1-SW2, cuyo significado es,
 - SW1, indica si la instrucción es correcta, es decir, si la clase, el código y los parámetros son correctos.
 - SW2, indica complementa el valor de SW1.
- Cuando no aparece ningún error, el valor de este par es 90-00.

Problemas del Protocolo

- El problema básico de este protocolo es la interrupción de la comunicación por parte de la tarjeta.
- Este hecho se puede producir por un problema en ésta, o bien por la pérdida de un byte en la comunicación desde el terminal.
- Cuando el terminal detecta esta situación, ya que se alcanza el tiempo de guarda, debe reiniciar la tarjeta y la comunicación.
- Otro problema es la imposibilidad de detectar más de un error en un byte, por la utilización del bit de paridad.

PROTOCOLO T = 1

Planteamiento

- La unidad mínima de información de este protocolo es el bloque de datos, compuesto por una secuencia de bytes.
- Estos bytes son enviados mediante la técnica descrita en el nivel físico, plasmando la división definida en el estándar ISO/OSI.
- Dado que la seguridad en la transmisión de mensajes requiere tanto la separación como la cooperación de los distintos niveles, la seguridad de este protocolo es muy alta.
- Así, es posible transferir en el nivel físico datos cifrados en un nivel superior.
- Por lo que respecta al intercambio de bloques dentro del protocolo,
 - El primer bloque de datos es transmitido por el terminal.
 - El segundo bloque lo envía la tarjeta.
 - El resto de los bloques son enviados, alternativamente, por el terminal y la tarjeta.
- El protocolo es capaz de enviar mensajes de cualquier tamaño, aunque el tamaño máximo de un bloque está limitado.
- La técnica empleada es el encadenamiento de bloques, cuya unión genera el mensaje completo.

PROTOCOLO T = 1

Estructura de los Bloques

- Un bloque está compuesta por tres campos,
 - Prologo, contiene datos referentes al control de la comunicación.
 - Información, en el que aparecen los datos que se desean transmitir.
 - Epílogo, cuya información permite realizar la detección de errores en la transmisión.
- El prólogo tiene un tamaño de tres bytes, cuyo nombre y significado es el siguiente,
 - Dirección de Nodo o NAD, que indica la dirección del origen y del destino, así como el estado del contacto Vpp.
 - Byte de Control de Protocolo o PCB, que permite identificar cual es el tipo del bloque.
 - Longitud, cuyos valores válidos son de 0 a 254, asociada al campo de información.
- El tamaño del epílogo depende del tipo de detección de error utilizada,
 - Un byte, cuando se utiliza la Comprobación de Redundancia Longitudinal o LRC, en el que se calcula la XOR de todos los bytes.
 - Dos bytes si se utiliza la Comprobación de Redundancia Cíclica o CRC, que utiliza el polinomio $x^{16} + x^{12} + x^5 + 1$.
- Normalmente se utiliza el primero por su sencillez y su menor tamaño.

PROTOCOLO T = 1

Tipos de Bloques

- El valor del PCB permite definir tres tipos de bloques diferentes,
 - Bloques de Información, donde aparecen los datos que forman el mensaje a transmitir.
 - Bloques de Respuesta, que indican si la recepción de un bloque ha sido correcta.
 - Bloques de Supervisión, a través de los cuales es posible controlar la comunicación y la modificación de la longitud máxima.
- Los dos primeros tipos incluyen en el PCB el denominado Número de Secuencia de Envío o N(S), cuyo manejo es el siguiente,
 - Su valor en los bloques de información es independiente en el terminal y la tarjeta, aunque en ambos su valor inicial es 0.
 - Se incrementa, en módulo 2, después del envío correcto de un bloque de información.
 - Un bloque de respuesta tiene un valor de N(S) igual al del bloque de información recibido, si aparece un error de transmisión.
- Además los bloques de información contienen un bit en el PCB que indica si el bloque es un bloque intermedio en la transmisión de un mensaje.

PROTOCOLO T = 1

Parámetros del Protocolo

- La longitud máxima del campo de información aparece definida por los parámetros,
 - Tamaño del Campo de Información para el Terminal o IFSD, cuyo valor inicial es 32.
 - Tamaño del Campo de Información para la Tarjeta o IFSC, cuyo valor inicial se define en el ATR.
- El valor inicial de estos parámetros puede ser modificado mediante bloques de supervisión.
- Por lo que respecta a la temporización de los bloques, se definen los siguientes parámetros,
 - Tiempo de Espera de Carácter o CWT, indica el tiempo máximo permitido entre el flanco de inicio de dos bytes del mismo bloque.
 - Tiempo de Espera de Bloques o BWT, es el tiempo máximo que puede transcurrir entre el inicio del último byte de un bloque y el inicio del primer byte del siguiente bloque.
 - Tiempo de Guarda de Bloque o BGT, marca el tiempo mínimo permitido entre los flancos de inicio de dos caracteres consecutivos enviados en direcciones opuestas.
- El valor de los dos primeros es definido en el ATR de la tarjeta, mientras que el último tiene un valor fijo de 22 etus.
- La utilización de bloques de supervisión puede aumentar el valor de BWT.

PROTOCOLO T = 1

Control de Errores

- Un error en la comunicación se puede producir por diferentes razones,
 - La detección de un error de paridad en uno o más bytes del mensaje.
 - La detección de un error en el valor del campo epílogo.
 - La pérdida de un mensaje en la línea.
- La detección y el procesamiento de errores en este protocolo se descompone en tres fases, que aportan un nivel de efectividad muy alta.
- En la primera fase, el emisor reenvía el bloque erróneo si,
 - Recibe un bloque de reconocimiento que le indica la existencia de un error.
 - Pasado un tiempo mayor de BWT no recibe ningún bloque.
- Si esta fase no es satisfactoria, el terminal envía un bloque de supervisión de resincronización a la tarjeta, que reinicia la comunicación al estado posterior al procesamiento del ATR.
- Como último recurso, el terminal reinicia la tarjeta, debiendo repetir todos los diálogos establecidos entre el terminal y la tarjeta.
- Después de tres intentos fallidos de reinicio de la tarjeta, el terminal la desactiva y la expulsa, indicando al usuario el mal funcionamiento de la tarjeta.

PROTOCOLO T = 1

Transmisión de Mensajes

- Si los mensajes a transmitir son de un tamaño menor que el permitido por el valor IFSD, o el IFSC, el terminal y la tarjeta envían bloques de modo alternativo.
- Los emisores de un bloque de información han de recibir un bloque en el que se indique si el bloque que han enviado se ha recibido de un modo correcto,
 - Si reciben otro bloque de información, la transmisión de su bloque ha sido correcta.
 - El valor de N(S) de un bloque de respuesta indica cómo se ha recibido el bloque.
- Cuando es necesario enviar un mensaje con un tamaño mayor que el permitido se debe dividir en bloques de un tamaño menor que el fijado.
- El posterior encadenamiento de estos bloques se realiza del modo siguiente,
 - El emisor envía el primer bloque con el valor de N(S) correspondiente y con M igual a 1.
 - Cuando lo recibe el receptor responde con un bloque de respuesta, cuyo valor de N(S) indica si ha aparecido un error.
 - El último bloque se marca por un valor de M igual a 0, y se transmite como el bloque de un mensaje compuesto por un único bloque.

- En cualquiera de los casos, la aparición de un bloque de supervisión indica la existencia de algún tipo de problema en la transmisión.

PROTOCOLOS DE COMUNICACIÓN

Planteamiento

- El intercambio de información entre el terminal y la tarjeta se realiza mediante la utilización de un protocolo de comunicación.
- La instrucción es enviada por el terminal a la tarjeta, que debe responder al primero con el resultado de su ejecución.
- Los protocolos de transmisión interpretan la instrucción y la respuesta como un elemento completo que deben transmitir.
- El protocolo de transmisión utilizado debe ser transparente, lo que ha influido en la definición del protocolo de comunicación, ya que debe permitir la transmisión de bytes y de bloques.

Estructura Básica

- Tanto la instrucción como la respuesta tienen una estructura muy similar a la descrita como estructura de mensaje del protocolo T = 0.
- En la instrucción aparece una cabecera, en donde aparece la instrucción a ejecutar y sus parámetros, y un cuerpo donde se sitúan los datos a transmitir.
- La estructura de la respuesta es equivalente a la del protocolo T = 0, un cuerpo donde van los datos y un fin de comunicación compuesto por los bytes SW1 y SW2.
- La diferencia aparece en el modo de indicar el número de bytes a transmitir.

PROTOCOLOS DE COMUNICACIÓN

Estructura de la Instrucción

- La instrucción se divide en dos partes que se denominan Cabecera y Cuerpo.
- La cabecera es obligatoria, y se compone de,
 - CLA, o clase, cuyo valor indica el sistema de seguridad y conjunto de códigos.
 - INS, o código de la Instrucción.
 - P1 y P2, que incluyen los parámetros de la instrucción a ejecutar.
- El cuerpo es opcional, y está compuesta de las tres campos siguientes,
 - Lc, o Longitud de los Datos de Salida.
 - Campo de Datos.
 - Le, o Longitud de los Datos de Entrada.
- La estructura del cuerpo varía en función de la instrucción a ejecutar, apareciendo cuatro posibles combinaciones.
- Los campos Lc y Le pueden tener un tamaño de 1, cuando su valor es menor de 255, ó de 3 bytes, si su valor es mayor de 255.
- Cuando ocupa 3 bytes, el primer byte siempre tiene el valor FF, y los dos bytes restantes incluyen el valor del campo.
- Cuando Le tiene un valor de 00, indica que su valor es igual al máximo permitido por la instrucción ejecutada.

PROTOCOLOS DE COMUNICACIÓN

Estructura de la Respuesta

- La respuesta se compone de un Cuerpo y una Cola.
- El cuerpo es opcional, e incluye los bytes que son enviados desde la tarjeta al terminal, y cuyo tamaño coincide con el valor Le de la instrucción asociada.
- La cola se compone de los bytes SW1-SW2 a través de los cuales, la tarjeta indica al terminal si la instrucción se ha ejecutado de un modo correcto.
- Estos códigos se pueden clasificar en cuatro tipos diferentes,
 - La ejecución se ha completado,
 - de un modo satisfactorio.
 - pero se avisa de una posible ejecución incorrecta.
 - Se ha interrumpido la ejecución,
 - por la aparición de un error .
 - ya que la instrucción no es válida .
- De los cuatro grupos descritos, el más amplio es el último, ya que incluye todos los posibles errores de análisis de la instrucción,
 - Valor de CLA o INS incorrectos.
 - Número o valor de P1 y P2 inadecuado.
 - Test de seguridad no satisfecho.

REINICIO DE LA TARJETA

Planteamiento

- Existe una gran variedad de tarjetas en el mercado, por lo que el primer diálogo entre el terminal y la tarjeta es la identificación de ésta última.
- En primer lugar, el terminal activa las señales de tensión, reloj y reinicio que permite la puesta en marcha de la tarjeta.
- Seguidamente, la tarjeta responde con la Respuesta al Reinicio, ATR, que incluye las principales características de comunicación de la tarjeta.
- La estructura y contenido del ATR difiere en las tarjetas síncronas y asíncronas, es decir, sin y con procesador.
- Si la tarjeta es asíncrona, el terminal puede iniciar un diálogo, denominado Selección del Tipo de Protocolo, PTS, que puede llegar a modificar alguno de los valores del ATR.
- Este diálogo se compone de dos mensajes, uno enviado por el terminal y una respuesta enviada por la tarjeta.
- Si el terminal acepta los valores del ATR, o los obtenidos después del PTS, inicia el diálogo directo con la tarjeta.
- En caso contrario, puede reiniciar el proceso varias veces, usualmente tres veces, con el objetivo de obtener valores adecuados.

REINICIO DE UNA TARJETA SÍNCRONA

Planteamiento

- En las tarjetas síncronas, se puede utilizar una frecuencia de transmisión comprendida entre 7 y 50 kHz para la transmisión del ATR.
- El mensaje transmitido por la tarjeta tiene una longitud fija de 32 bits, que se envían mediante la convención directa,
 - En primer lugar se envía b1 y el último que se envía es b8.
 - Se interpreta Z como 1 y A como 0.
- En dicho mensaje aparecen dos campos de 8 bits que son obligatorios,
 - H1, que codifica el tipo de protocolo.
 - H2, incluye parámetros que son necesarios para el tipo de protocolo seleccionado.
- El contenido del resto del mensaje no está normalizado. por lo que cada tarjeta puede incluir información diferente.
- De modo genérico, aparece información de tipo histórico, como el número de serie de la tarjeta.

REINICIO DE UNA TARJETA ASÍNCRONA

Estructura Básica

- La longitud máxima de un ATR es 33 bytes, que se descompone en las siguientes partes,
 - TS, o Byte de Inicio, que es obligatorio.
 - T0, o Byte de Formato, que es obligatorio.
 - Caracteres de Interface, con un número máximo de 15, todos ellos opcionales.
 - Caracteres de Históricos, con un número máximo de 15, todos ellos opcionales.
 - TCK, o Byte de Reconocimiento, que resulta obligatorio en algún caso.

Significado de TS

- Mediante la utilización de este carácter se define cual es el valor inicial de t_{et} .
- Para ello se divide por tres el tiempo entre los dos primeros flancos de bajada,
 - Si la tarjeta tiene reloj interno vale $1/9600$ s.
 - Sino su valor es $372/f_i$ s, siendo f_i $[1,5]$ MHz la frecuencia de reloj aportada por el terminal.
- Además, se define el valor de la convención utilizada en el nivel físico de comunicación.
- Los valores posibles de este byte son,
 - Convención Directa, ZZAZZZAA o 3B.
 - Convención Inversa, ZZAAAAAA o 3F.

REINICIO DE UNA TARJETA ASÍNCRONA

Significado de T0 y de los Car. Interface

- Este byte marca la estructura del resto del ATR, indicando el número de caracteres históricos y la existencia de los caracteres de interface.
- Para comprender su relación con la existencia de los caracteres de interface, es necesario especificar que éstos aparecen en grupos de cuatro bytes que se nombran [TA_i, TB_i, TC_i, TD_i].
- Dividendo T0 en los dos valores hexadecimales que forman un byte, se obtiene que,
 - El valor menos significativo indica el número de caracteres históricos incluidos en el ATR.
 - Por su parte, el valor más significativo indica la existencia del primero de los grupos de los caracteres de interface,
 - El bit más significativo se asocia con TD1.
 - El menos significativo con TA1.
- Los caracteres TD_i tienen una estructura similar, conteniendo un protocolo de transmisión, T, y la existencia de los caracteres de interface necesarios para su parametrización.
 - T aparece como el valor hexadecimal menos significativo.
 - El valor más significativo indica la existencia del (i+1)-ésimo grupo de los caracteres de interface.
- El orden de los protocolos de transmisión indica su prioridad, debiendo ser el primero el T = 0 si éste fuera soportado por la tarjeta.

REINICIO DE UNA TARJETA ASÍNCRONA

Caracteres de Interface Globales

- El primer grupo de caracteres de interface y parte del segundo grupo se nombran como Caracteres de Interface Globales en los que se definen el nivel físico de la comunicación.
- El valor de etu a utilizar en la comunicación se define en TA1, que incluye la codificación de los siguientes parámetros,
 - El divisor de la frecuencia proporcionada por el terminal, F , y la frecuencia máxima.
 - Un factor de ajuste de la transmisión, D .
- El valor por defecto de TA1 es 11.
- La intensidad y la tensión de programación a utilizar se codifican en los caracteres TB1 y TB2,
 - Si el valor de TB1 es 00 indica que la tensión de programación no es utilizada.
 - En caso contrario, contiene la codificación de la intensidad y el valor de la tensión.
 - Por su parte TB2, especifica la tensión en décimas de voltio, y su valor prevalece sobre el especificado en TB1.
- El valor por defecto de TB1 es 25.
- La dimensión de un byte es $(12+N)$ etu , donde N es el tiempo de guarda contenido en TC1.
- Si $N = 255$ la dimensión de un byte depende del protocolo, 12 etu para $T = 0$ y 11 etu para $T = 1$.
- El valor por defecto de TC1 es 00.

REINICIO DE UNA TARJETA ASÍNCRONA

Caracteres de Interface de Protocolo

- El segundo grupo se asocia al protocolo $T = 0$, que codifica el único parámetro asociado, el tiempo de espera.
- Para ello se utiliza el valor de TC2.
- EL protocolo $T = 1$ se describe en el i -ésimo grupo con $i > 2$, donde se definen los valores,
 - El byte TA_i define IFSC.
 - El byte TB_i codifica BWT y CWT.
 - El bit menos significativo de TC_i indica el tipo de detección de errores utilizado.
- El valor por defecto de estos bytes es, 20 para TA_i , 4D para TB_i y 00 para TC_i .

Caracteres Históricos

- Los estándares no describen el contenido de estos caracteres, por lo que cada fabricante suele utilizarlos de modo diferente.
- Habitualmente incluyen información ASCII, en la que aparece información general.

Caracteres de Reconocimiento

- Cuando se utiliza el protocolo $T = 1$, este byte incluye la XOR de los bytes del ATR, excluyendo el carácter TS.

REINICIO DE UNA TARJETA ASÍNCRONA

Selección del Tipo de Protocolo

- La selección del tipo de protocolo siempre es iniciado por el terminal y debe ser respondido por la tarjeta.
- Este proceso permite modificar alguno de los valores especificados por la tarjeta en su ATR.
- En caso contrario, la comunicación utiliza el primer protocolo especificado en el ATR.
- No se produce si sólo aparece un protocolo y los valores de F y D son los valores por defecto.
- Aparecen dos modos de funcionamiento,
 - Negociable, los valores por defecto de F y D son utilizados hasta completar un PTS.
 - Específico, se utilizan los valores de F y D que aparecen en el ATR.
- La existencia del carácter de protocolo TA2 indica la utilización del último modo, e incluye el protocolo a utilizar.
- Se puede cambiar de uno a otro modo, tal y como se muestra,
 - Negociable a Específico, requiere un PTS completo.
 - Específico a Negociable, se puede realizar mediante la inclusión de una señal de reset.

REINICIO DE UNA TARJETA ASÍNCRONA

Selección del Tipo de Protocolo

- La estructura del PTS es similar a la del ATR,
 - Carácter Inicial o PTSS, que es obligatorio y cuyo valor es FF.
 - Carácter de Formato o PTS0, que también es obligatorio y que tiene una estructura idéntica a los TDi.
 - Caracteres de Parámetros, cuyo existencia depende de PTS0, y que incluyen los valores del ATR a modificar.
 - Carácter de Control o PCK, que siempre aparece siendo su valor igual al XOR de los anteriores bytes.
- Los caracteres de parámetros presentan la siguiente estructura,
 - PTS1 es idéntico a TA1.
 - PTS2 se relaciona con el valor de N.
 - PTS3 no está definido.
- Ante el mensaje enviado por el terminal, la tarjeta debe responder con el mismo mensaje si esta de acuerdo.
- En caso contrario puede no responder, ante lo cual el terminal asume su rechazo y produce una señal de reset.