PROPUESTA DE MODIFICACIÓN DE LA

NAS 830

NORMA ADIF SEÑALIZACIÓN

PROTOCOLO ESTÁNDAR DE ADIF PARA LAS COMUNICACIONES ENTRE CTC Y ENCLAVAMIENTO SCI-CC-A. VERSIÓN 1.0

1ª EDICIÓN: JULIO 2021

CONTROL DE CAMBIOS Y VERSIONES

Revisión		Modificaciones	Puntos Revisados
Nº	Fecha		

EQUIPO REDACTOR

Grupo de Trabajo GT-405. Enclavamientos electrónicos.

Propone:

Grupo de trabajo GT-405
Fecha: 10 de mayo de 2024

ÍNDICE DE CONTENIDOS **PÁGINA**

1.-OBJETO

El presente documento tiene por objeto someter a segunda fase de consulta una modificación a la Norma NAS 830 "PROTOCOLO ESTÁNDAR DE ADIF PARA LAS COMUNICACIONES ENTRE CTC Y ENCLAVAMIENTO SCI-CC-A. VERSIÓN 1.0". 1ª EDICIÓN. JULIO 2021.

Si como resultado de este proceso, finalmente se modificara la norma antedicha, ésta se publicará íntegramente, incluyendo las modificaciones que correspondan, y será codificada como NAS 830_ED1M1.

2.-MODIFICACIONES SOMETIDAS A FASE DE CONSULTA

Las modificaciones realizadas en la Norma son las siguientes:

Modificaciones	Puntos Revisados
MODIFICACIÓN 1. Se incluye párrafo sobre medidas de seguridad adecuadas para cumplir la legislación.	1
MODIFICACIÓN 2. Se añade la definición del estándar empleado para la implementación de RSA y el padding a emplear para la implementación de RSA mediante el estándar PKCS#1 v2.2.	7.2.3
MODIFICACIÓN 3. Se añade aclaración sobre el número de FEC que pueden existir en un CTC.	7.3.4.1, 7.3.4.2
MODIFICACIÓN 4. Se corrige errata sobre la sincronización	8.1
MODIFICACIÓN 5. Se modifica el texto para especificar los valores de los números de secuencia para el modo E-E.	8.2
MODIFICACIÓN 6. Se elimina la duplicidad de definición del parámetro LMR y se corrige error en el ejemplo del final del apartado.	9.4.1
MODIFICACIÓN 7. Se modifica el texto del campo Nº SEC REMOTA IM.	9.6.1, 9.8.1, 9.8.2, 9.8.5, 9.8.6
MODIFICACIÓN 8. Se modifica el texto del campo Nº SEC FEC IM.	9.6.3, 9.7.2, 9.8.3, 9.8.4
MODIFICACIÓN 9. Se incluye el campo LONGITUD en el CAMRC.	9.6.3
MODIFICACIÓN 10. Se corrige error en el campo LONGITUD y se añade valor.	9.8.2, 9.8.3

Modificaciones	Puntos Revisados
MODIFICACIÓN 11. Se modifica el texto para añadir el código de respuesta 0x03 y se amplía el texto del código de rechazo 0x00 en el mensaje de RESPUESTA DE ÓRDENES para aquellos casos en los que el enclavamiento no proporciona información de orden aceptada/rechazada.	9.8.3
MODIFICACIÓN 12. Se especifica que se deben enviar todos los cambios de estado producidos entre petición y petición en modo P-R.	9.7, 11.1
MODIFICACIÓN 13. Se modifican los esquemas caso 1 y caso 2 añadiendo el mensaje de RECONOCIMIENTO DE CAMBIOS DE ESTADO a la recepción de CAMBIOS DE ESTADO, según establece el protocolo.	10.4.3
MODIFICACIÓN 14. Se añade nuevo apartado 11.3 con los caracteres ASCII admitidos en las órdenes.	11.3
MODIFICACIÓN 15. Se reordena la colocación de los capítulos 12, 13 y 14, actualizando la 'Normativa Derogada' y añadiendo párrafos aclaratorios en 'Normativa de referencia'.	12, 13, 14

A continuación se incluye el texto original de la NAS830_ED1 seguido de la modificación propuesta, en cursiva:

2.1.-MODIFICACIÓN 1

Se incluye párrafo sobre medidas de seguridad adecuadas para cumplir la legislación.

Texto original en el capítulo 7.2.3:

1.-OBJETO

El objeto de este documento es definir el Protocolo Estándar de Adif para las comunicaciones de mando y control entre CTC y enclavamiento "SCI-CC-A" basado en TCP/IP.

Mediante este protocolo se pretende normalizar en toda la red el formato de la comunicación entre CTC y enclavamiento, independientemente de la tecnología de ambos, eliminando equipamientos intermedios con función de adaptadores de protocolos.

Texto propuesto:

1.-OBJETO

El objeto de este documento es definir el Protocolo Estándar de Adif para las comunicaciones de mando y control entre CTC y enclavamiento "SCI-CC-A" basado en TCP/IP.

Mediante este protocolo se pretende normalizar en toda la red el formato de la comunicación entre CTC y enclavamiento, independientemente de la tecnología de ambos, eliminando equipamientos intermedios con función de adaptadores de protocolos.

En sistemas de información se deberán adoptar las medidas de seguridad adecuadas para cumplir la legislación a la que está obligada a Adif (o la legislación que aplica a Adif), así como la Política de Seguridad de la Información y normativas vigentes en la entidad.

2.2.-MODIFICACIÓN 2

Se añade la definición del estándar empleado para la implementación de RSA y el padding a emplear para la implementación de RSA mediante el estándar PKCS#1 v2.2.

Texto original en el capítulo 7.2.3:

(...)

Se utilizarán claves RSA de 2048 bits que serán generadas, renovadas y distribuidas por Adif.

Una vez inicializada la comunicación se hace uso de la clave de sesión compartida y el algoritmo HMACSHA512 para generar los CAMRC a incluir en todos los mensajes.

(...)

Texto propuesto:

(...)

Se utilizarán claves RSA de 2048 bits que serán generadas, renovadas y distribuidas por Adif.

Se utilizará para la implementación del algoritmo RSA el estándar PKCS#1 v2.2 (RFC 8017) con padding PKCS #1 v1.5.

Una vez inicializada la comunicación se hace uso de la clave de sesión compartida y el algoritmo HMACSHA512 para generar los CAMRC a incluir en todos los mensajes.

(...)

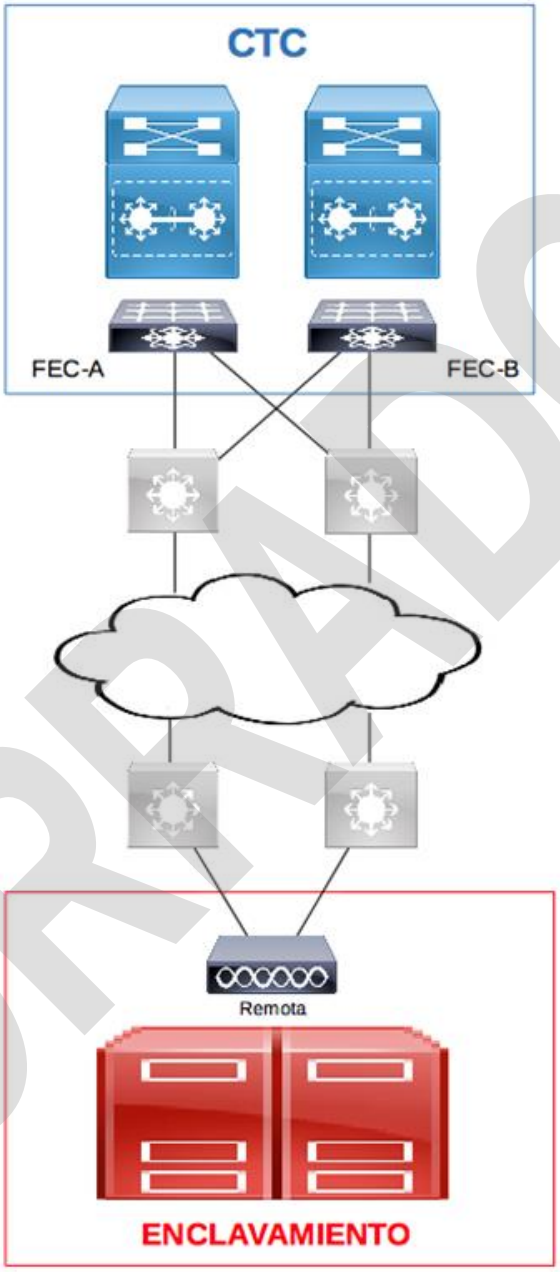
2.3.-MODIFICACIÓN 3

Se añade aclaración sobre el número de FEC que pueden existir en un CTC.

Texto original en los capítulos 7.3.4.1 y 7.3.4.2:

7.3.4.1 ARQUITECTURA SIMPLE

En la arquitectura simple existe una única Remota con n canales disponibles con los FEC, entre los cuales habrá m canales inicializados ($m \leq n$) y un único canal activo.



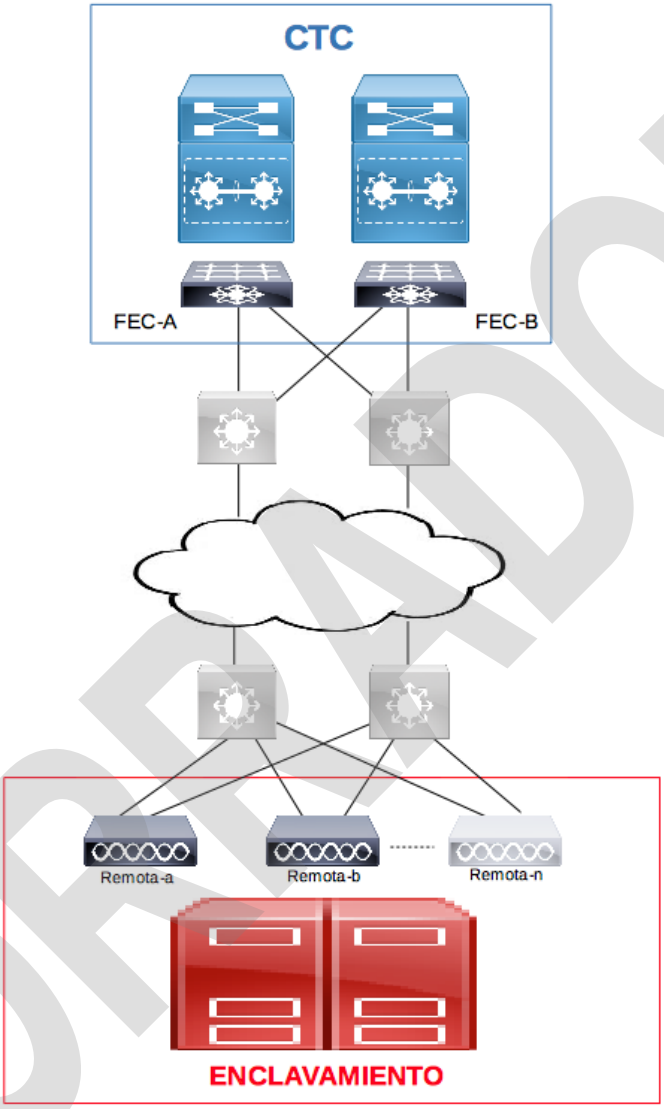
Esquema de arquitectura simple.

En este ejemplo, la comunicación se puede establecer a través de ocho posibles canales disponibles.

n = (Nº de FEC=2) x (Nº de IP de cada FEC=2) x (Nº de Remotas=1) x (Nº de IP de cada Remota=2) = 8

7.3.4.2 ARQUITECTURA REDUNDANTE

En esta arquitectura existen dos o más Remotas con n canales disponibles con los FEC, entre los cuales habrá m canales inicializados ($m \leq n$) y un único canal activo.



Esquema de arquitectura redundante

En este ejemplo, suponiendo que existen 3 Remotas, la comunicación se podría establecer a través de 24 posibles canales disponibles.

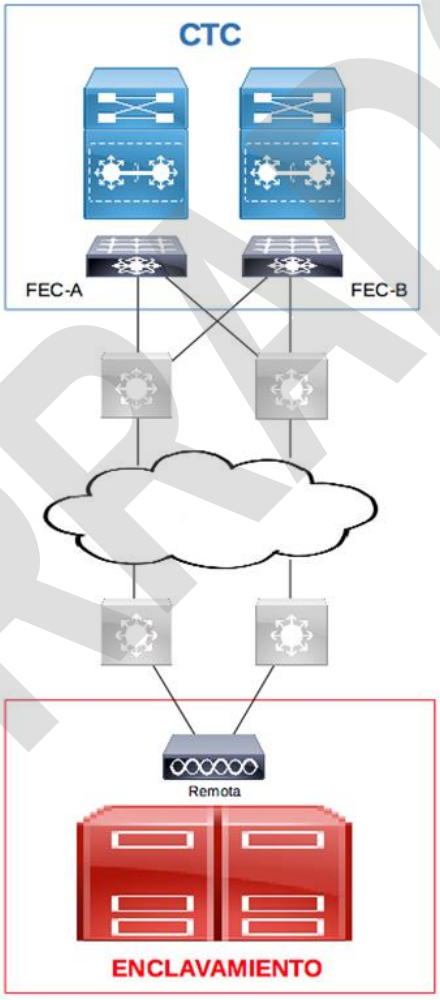
n = (Nº de FEC=2) x (Nº de IP de cada FEC=2) x (Nº de Remotas=3) x (Nº de IP de cada Remota=2) = 24

Texto propuesto:

7.3.4.1 ARQUITECTURA SIMPLE

En la arquitectura simple se instalará una única Remota con la que podrán comunicar los FEC del CTC a través de n canales disponibles, entre los cuales habrá m canales inicializados ($m \leq n$) y un único canal activo.

En el ejemplo de la siguiente figura se han contemplado únicamente 2 FEC, aunque el número podrá variar según el modelo de arquitectura del CTC. Por ejemplo, un CTC con 2 nodos, en el que en cada nodo existan 2 FEC de producción y 2 FEC de preproducción, tendrá un total de 8 FEC.



Esquema de arquitectura simple.

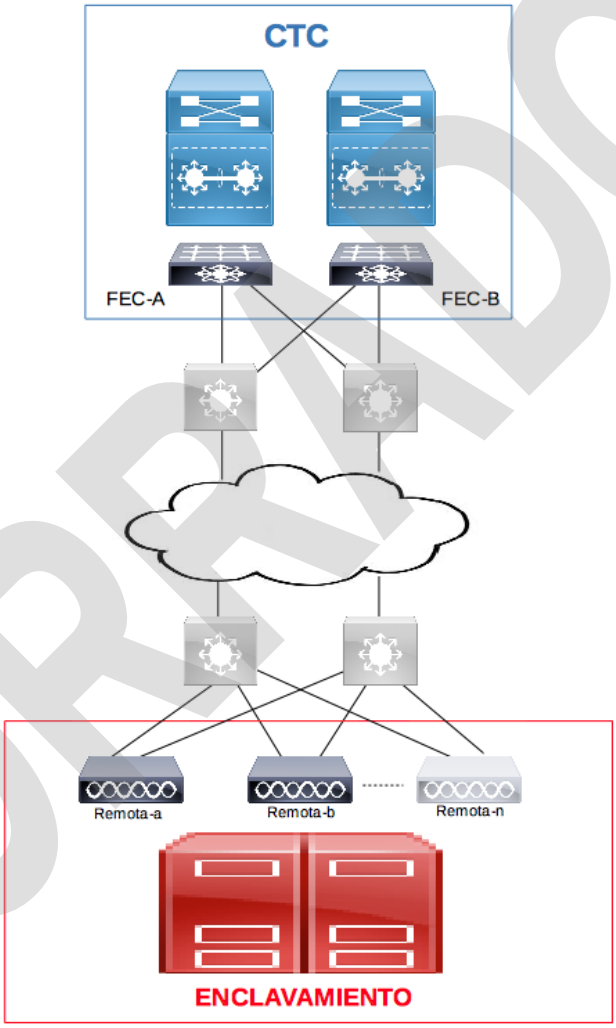
En este ejemplo, en el que se han contemplado 2 FEC y 1 Remota, la comunicación se podría establecer a través de ocho posibles canales disponibles.

n = (Nº de FEC=2) x (Nº de IP de cada FEC=2) x (Nº de Remotas=1) x (Nº de IP de cada Remota=2) = 8.

7.3.4.2 ARQUITECTURA REDUNDANTE

En una arquitectura redundante se instalarán dos o más Remotas con las que podrán comunicar los FEC del CTC a través de n canales disponibles, entre los cuales habrá m canales inicializados ($m \leq n$) y un único canal activo.

En el ejemplo de la siguiente figura se han contemplado únicamente 2 FEC, aunque el número podrá variar según el modelo de arquitectura del CTC. Por ejemplo, un CTC con 2 nodos, en el que en cada nodo existan 2 FEC de producción y 2 FEC de preproducción, tendrá un total de 8 FEC.



Esquema de arquitectura redundante

En este ejemplo, en el que se han contemplado 2 FEC y suponiendo que existen 3 Remotas, la comunicación se podría establecer a través de 24 posibles canales disponibles.

n = (Nº de FEC=2) x (Nº de IP de cada FEC=2) x (Nº de Remotas=3) x (Nº de IP de cada Remota=2) = 24.

2.4.-MODIFICACIÓN 4

Se modifica el texto para corregir errata sobre la sincronización.

Texto original en el capítulo 8.1:

8.1.-FORMATO DE LOS PAQUETES

(...)

- La Marca de tiempo (MARCA DE TIEMPO): 8 bytes. Esta marca la genera el emisor (FEC o Remota) en el momento de componer el mensaje. Por lo tanto, puede darse el caso de existir varios mensajes con la misma marca de tiempo. Se utilizará la marca de tiempo estándar basada en el número de milisegundos transcurridos desde el 01/01/1970 UTC. Se recomienda la sincronización del reloj de los FEC y las Remotas con los servidores NTP de la red de explotación de Adif.

(...)

Texto propuesto:

8.1.-FORMATO DE LOS PAQUETES

(...)

- *La Marca de tiempo (MARCA DE TIEMPO): 8 bytes. Esta marca la genera el emisor (FEC o Remota) en el momento de componer el mensaje. Por lo tanto, puede darse el caso de existir varios mensajes con la misma marca de tiempo. Se utilizará la marca de tiempo estándar basada en el número de milisegundos transcurridos desde el 01/01/1970 UTC. Se debe garantizar la sincronización del reloj de los FEC y las Remotas con los servidores NTP de la red de explotación de Adif.*

(...)

2.5.-MODIFICACIÓN 5

Se modifica el texto para especificar los valores de los números de secuencia para el modo E-E.

Texto original en el capítulo 8.2:

8.2.-ANÁLISIS DE LA CABECERA Y CAMRC DEL MENSAJE RECIBIDO

(...)

- Número de secuencia del FEC por canal inicializado y funcionalidad (Nº SEC FEC *):
  - El FEC genera un número de secuencia independiente según funcionalidad de manera incremental en cada nuevo mensaje que envíe:
    - Nº SEC FEC CC: Comprobación de la comunicación.
    - Nº SEC FEC IM: Indicaciones y mandos.

- La Remota debe monitorizar el número de secuencia del FEC por funcionalidad comprobando que aumenta el Nº SEC FEC * en cada mensaje recibido. En el caso que la Remota detecte un fallo de numeración en los Nº SEC FEC *, descartará el mensaje recibido, enviando al FEC el mensaje ERROR DETECTADO POR REMOTA y cerrará las comunicaciones por dicho canal.
- En el caso que la Remota responda a un mensaje del FEC, deberá incorporar en el mensaje de respuesta el campo Nº SEC FEC * del paquete recibido.
- En el caso que la REMOTA responda con un mensaje de confirmación de la recepción a un mensaje del FEC del tipo IM en el modo E-E, el Nº SEC REMOTA IM será siempre 0.
- El FEC comprobará que recibe en la respuesta de la Remota el Nº SEC FEC * correspondiente a la última petición enviada. En caso de recibir un Nº SEC FEC * que no corresponda, descartará el mensaje interpretando que no se ha recibido bien por parte de la Remota, enviará a la Remota el mensaje ERROR DETECTADO POR FEC y cerrará las comunicaciones por dicho canal.
- En el caso que la Remota inicie espontáneamente el envío de mensajes de cambio de estado (exclusivamente en modo E-E), el número de secuencia Nº SEC FEC IM será siempre 0. Cuando el FEC reciba este número de secuencia interpretará que es un mensaje generado por la REMOTA que no es respuesta a un mensaje anterior.

- Nº de secuencia de la Remota por canal inicializado y funcionalidad (Nº SEC REMOTA *):
  - La Remota genera un número de secuencia independiente según funcionalidad de manera incremental en cada nuevo mensaje que envíe:
    - Nº SEC REMOTA CC: Comprobación de la comunicación.
    - Nº SEC REMOTA IM: Indicaciones y mandos.
  - El FEC debe monitorizar el número de secuencia de la Remota comprobando que aumenta el Nº SEC REMOTA * en cada mensaje recibido. En el caso que el FEC detecte un fallo de numeración en el Nº SEC REMOTA *, descartará el mensaje recibido, enviando a la Remota el mensaje ERROR DETECTADO POR FEC y cerrará las comunicaciones por dicho canal.
  - En el caso que el FEC responda a un mensaje de la Remota, deberá incorporar en el mensaje de respuesta el campo Nº SEC REMOTA * del paquete recibido.
  - En el caso que el FEC responda a un mensaje de la Remota del tipo IM en el modo E-E, el Nº SEC FEC IM será siempre 0.
  - La Remota comprobará que recibe en la respuesta del FEC el Nº SEC REMOTA * correspondiente al último mensaje enviado. En caso de recibir un Nº SEC REMOTA * que no corresponda, descartará el mensaje interpretando que no se ha recibido bien por parte del FEC, enviará al FEC el mensaje ERROR DETECTADO POR REMOTA y cerrará las comunicaciones por dicho canal.
  - En el caso que el FEC inicie el envío de los mensajes, el número de secuencia Nº SEC REMOTA * será siempre 0 en el primer mensaje.
  - En el caso que el FEC inicie espontáneamente el envío de mensajes (exclusivamente en modo E-E), el número de secuencia Nº SEC REMOTA IM será siempre 0. Cuando la REMOTA reciba este número de secuencia interpretará que es un mensaje generado por el FEC que no es respuesta a un mensaje anterior.

(...)

Texto propuesto:

8.2.-ANÁLISIS DE LA CABECERA Y CAMRC DEL MENSAJE RECIBIDO

(...)

- *Número de secuencia del FEC por canal inicializado y funcionalidad (Nº SEC FEC *):*
  - *El FEC genera un número de secuencia independiente según funcionalidad de manera incremental en cada nuevo mensaje que envíe, salvo las excepciones para el modo E-E indicadas más adelante en este mismo apartado:*
    - *Nº SEC FEC CC: Comprobación de la comunicación.*
    - *Nº SEC FEC IM: Indicaciones y mandos.*
  - *La Remota debe monitorizar el número de secuencia del FEC por funcionalidad comprobando que aumenta el Nº SEC FEC * en cada mensaje recibido. En el caso que la Remota detecte un fallo de numeración en los Nº SEC FEC *, descartará el mensaje recibido, enviando al FEC el mensaje ERROR DETECTADO POR REMOTA y cerrará las comunicaciones por dicho canal.*
  - *En el caso que la Remota responda a un mensaje del FEC, deberá incorporar en el mensaje de respuesta el campo Nº SEC FEC * del paquete recibido.*
  - *En el caso que la REMOTA responda con un mensaje de confirmación de la recepción a un mensaje del FEC del tipo IM en el modo E-E, el Nº SEC REMOTA IM será siempre 0.*
  - *El FEC comprobará que recibe en la respuesta de la Remota el Nº SEC FEC * correspondiente a la última petición enviada. En caso de recibir un Nº SEC FEC * que no corresponda, descartará el mensaje interpretando que no se ha recibido bien por parte de la Remota, enviará a la Remota el mensaje ERROR DETECTADO POR FEC y cerrará las comunicaciones por dicho canal.*
  - *En el caso que la Remota inicie espontáneamente el envío de mensajes (exclusivamente en modo E-E), el número de secuencia Nº SEC FEC IM será siempre 0. Cuando el FEC reciba este número de secuencia interpretará que es un mensaje generado por la REMOTA que no es respuesta a un mensaje anterior.*
- *Nº de secuencia de la Remota por canal inicializado y funcionalidad (Nº SEC REMOTA *):*
  - *La Remota genera un número de secuencia independiente según funcionalidad de manera incremental en cada nuevo mensaje que envíe, salvo las excepciones para el modo E-E indicadas más adelante en este mismo apartado:*
    - *Nº SEC REMOTA CC: Comprobación de la comunicación.*
    - *Nº SEC REMOTA IM: Indicaciones y mandos.*
  - *El FEC debe monitorizar el número de secuencia de la Remota comprobando que aumenta el Nº SEC REMOTA * en cada mensaje recibido. En el caso que el FEC detecte un fallo de numeración en el Nº SEC REMOTA *, descartará el mensaje recibido, enviando a la Remota el mensaje ERROR DETECTADO POR FEC y cerrará las comunicaciones por dicho canal.*
  - *En el caso que el FEC responda a un mensaje de la Remota, deberá incorporar en el mensaje de respuesta el campo Nº SEC REMOTA * del paquete recibido.*
  - *En el caso que el FEC responda a un mensaje de la Remota del tipo IM en el modo E-E, el Nº SEC FEC IM será siempre 0.*

- *La Remota comprobará que recibe en la respuesta del FEC el Nº SEC REMOTA * correspondiente al último mensaje enviado. En caso de recibir un Nº SEC REMOTA * que no corresponda, descartará el mensaje interpretando que no se ha recibido bien por parte del FEC, enviará al FEC el mensaje ERROR DETECTADO POR REMOTA y cerrará las comunicaciones por dicho canal.*
- *En el caso que el FEC inicie el envío de los mensajes, el número de secuencia Nº SEC REMOTA * será siempre 0 en el primer mensaje.*
- *En el caso que el FEC inicie espontáneamente el envío de mensajes (exclusivamente en modo E-E), el número de secuencia Nº SEC REMOTA IM será siempre 0. Cuando la REMOTA reciba este número de secuencia interpretará que es un mensaje generado por el FEC que no es respuesta a un mensaje anterior.*

(...)

2.6.-MODIFICACIÓN 6

Se elimina la duplicidad de definición del parámetro LMR y se corrige error en el ejemplo del final del apartado.

Texto original en el capítulo 9.4.1:

9.4.1.-Mensaje: INICIALIZACIÓN DE LA COMUNICACIÓN

(...)

PARÁMETROS = la cadena de inicialización tendrá el formato siguiente:

Parámetro1:Valor1, Parámetro2:Valor2,..., ParámetroN:ValorN

Los parámetros a incluir serán los siguientes:

- VP: Versión del protocolo. [1..n].[0..9]. Indica la versión del Protocolo que debe tener el enclavamiento con el que se está inicializando la comunicación
- VC: Versión del catálogo. [1..m].[0..9]. Indica la versión del Catálogo de Indicaciones que debe tener el enclavamiento con el que se está inicializando la comunicación
- TR: Tiempo máximo en milisegundos que debe esperar la Remota a las respuestas del FEC. [500..30000]
- TT: Tiempo máximo en milisegundos de espera de testeo de la comunicación. [100..10000]
- MC: Modo de Comunicación. MC:[PR|EE]
- LMR: Longitud máxima del mensaje de la Remota al FEC (cabecera incluida). [32..65535] [151..65.535]
- LMR: Longitud máxima del campo CAMBIOS DE ESTADO en los mensajes ESTADO COMPLETO y CAMBIOS DE ESTADO enviados de la Remota al FEC. Valor máximo 65448.
- NRR: Número de reintentos de envío de mensajes de la Remota al FEC. [0..5]

(...)

Texto propuesto:

9.4.1.-Mensaje: INICIALIZACIÓN DE LA COMUNICACIÓN

(...)

***PARÁMETROS** = la cadena de inicialización tendrá el formato siguiente:*

Parámetro1:Valor1, Parámetro2:Valor2,..., ParámetroN:ValorN

Los parámetros a incluir serán los siguientes:

- *VP: Versión del protocolo. [1..n].[0..9]. Indica la versión del Protocolo que debe tener el enclavamiento con el que se está inicializando la comunicación*
- *VC: Versión del catálogo. [1..m].[0..9]. Indica la versión del Catálogo de Indicaciones que debe tener el enclavamiento con el que se está inicializando la comunicación*
- *TR: Tiempo máximo en milisegundos que debe esperar la Remota a las respuestas del FEC. [500..30000]*
- *TT: Tiempo máximo en milisegundos de espera de testeo de la comunicación. [100..10000]*
- *MC: Modo de Comunicación. MC:[PR|EE]*
- *LMR: Longitud máxima del campo CAMBIOS DE ESTADO en los mensajes ESTADO COMPLETO y CAMBIOS DE ESTADO enviados de la Remota al FEC. Valor máximo 65448.*
- *NRR: Número de reintentos de envío de mensajes de la Remota al FEC. [0..5]*

(...)

2.7.-MODIFICACIÓN 7

Se modifica el texto del campo Nº SEC REMOTA IM.

Texto original en los apartados 9.6.1, 9.8.1, 9.8.2, 9.8.5, 9.8.6:

9.6.1.-Mensaje: PETICIÓN DE ESTADO COMPLETO

(...)

Nº SEC REMOTA IM = último número de secuencia recibido de la Remota. Si es tras una inicialización, el valor será 0x01.

(...)

9.8.1.-Mensaje: ENVÍO DE ÓRDENES

(...)

Nº SEC REMOTA IM = último número de secuencia recibido de la Remota.

(...)

9.8.2.-Mensaje: RECEPCIÓN DE ÓRDENES

(...)

Nº SEC REMOTA IM = último número de secuencia recibido de la Remota.

(...)

9.8.5.-Mensaje: CONFIRMACIÓN DE MANDO ESPECIAL

(...)

Nº SEC REMOTA IM = último número de secuencia recibido de la Remota.

(...)

9.8.6.-Mensaje: CANCELACIÓN DE MANDO ESPECIAL

(...)

Nº SEC REMOTA IM = último número de secuencia recibido de la Remota.

(...)

Texto propuesto:

9.6.1.-Mensaje: PETICIÓN DE ESTADO COMPLETO

(...)

***Nº SEC REMOTA IM** = En modo P-R: último número de secuencia recibido de la Remota.*

En modo E-E: siempre a 0x00.

Si es tras una inicialización, independientemente del modo de comunicación, el valor será 0x00.

(...)

9.8.1.-Mensaje: ENVÍO DE ÓRDENES

(...)

***Nº SEC REMOTA IM** = En modo P-R: último número de secuencia recibido de la Remota.*
En modo E-E: siempre a 0x00.

(...)

9.8.2.-Mensaje: RECEPCIÓN DE ÓRDENES

(...)

***Nº SEC REMOTA IM** = En modo P-R: último número de secuencia recibido de la Remota.*

En modo E-E: siempre a 0x00.

(...)

9.8.5.-Mensaje: CONFIRMACIÓN DE MANDO ESPECIAL

(...)

***Nº SEC REMOTA IM** = En modo P-R: último número de secuencia recibido de la Remota.*

En modo E-E: siempre a 0x00.

(...)

9.8.6.-Mensaje: CANCELACIÓN DE MANDO ESPECIAL

(...)

***Nº SEC REMOTA IM** = En modo P-R: último número de secuencia recibido de la Remota.*

En modo E-E: siempre a 0x00.

(...)

2.8.-MODIFICACIÓN 8

Se modifica el texto del campo Nº SEC FEC IM.

Texto original en los apartados 9.6.3, 9.7.2, 9.8.3 y 9.8.4:

9.6.3.-Mensaje: RECONOCIMIENTO DE CAMBIOS DE ESTADO

(...)

Nº SEC FEC IM = número de secuencia generado por el FEC.

(...)

9.7.2.-Mensaje: CAMBIOS DE ESTADO

(...)

Nº SEC FEC IM = número de secuencia recibido en el último mensaje del FEC.

(...)

9.8.3.-Mensaje: RESPUESTA DE ÓRDENES

(...)

Nº SEC FEC IM = número de secuencia recibido en el último mensaje del FEC.

(...)

9.8.4.-Mensaje: RECONOCIMIENTO DE RESPUESTA DE ÓRDENES

(...)

Nº SEC FEC IM = número de secuencia generado por el FEC.

(...)

Texto propuesto:

9.6.3.-Mensaje: RECONOCIMIENTO DE CAMBIOS DE ESTADO

(...)

***Nº SEC FEC IM** = En modo P-R: número de secuencia generado por el FEC.*
En modo E-E: siempre a 0x00.

(...)

9.7.2.-Mensaje: CAMBIOS DE ESTADO

(...)

***Nº SEC FEC IM** = En modo P-R: número de secuencia recibido en el último mensaje del FEC.*

En modo E-E: siempre a 0x00.

(...)

9.8.3.-Mensaje: RESPUESTA DE ÓRDENES

(...)

***Nº SEC FEC IM** = En modo P-R: número de secuencia recibido en el último mensaje del FEC.*

En modo E-E: siempre 0x00.

(...)

9.8.4.-Mensaje: RECONOCIMIENTO DE RESPUESTA DE ÓRDENES

(...)

***Nº SEC FEC IM** = En modo P-R: número de secuencia generado por el FEC.*

En modo E-E: siempre a 0x00.

(...)

2.9.-MODIFICACIÓN 9

Se incluye el campo LONGITUD en el CAMRC.

Texto original en el capítulo 9.6.3:

9.6.3.-Mensaje: RECONOCIMIENTO DE CAMBIOS DE ESTADO

(...)

CAMRC = HMACSHA512 (Clave de Sesión, ID FEC + ID REMOTA + Nº SEC FEC IM + Nº SEC REMOTA IM + MARCA DE TIEMPO + ID MENSAJE + NUM TOTAL MENSAJES + NUM ORDEN DE MENSAJE + RECONOCIMIENTO)

(...)

Texto propuesto:

9.6.3.-Mensaje: RECONOCIMIENTO DE CAMBIOS DE ESTADO

(...)

***CAMRC** = HMACSHA512 (Clave de Sesión, ID FEC + ID REMOTA + Nº SEC FEC IM + Nº SEC REMOTA IM + LONGITUD + MARCA DE TIEMPO + ID MENSAJE + NUM TOTAL MENSAJES + NUM ORDEN DE MENSAJE + RECONOCIMIENTO).*

(...)

2.10.-MODIFICACIÓN 10

Se corrige error en el campo LONGITUD y se añade valor.

Texto original en los capítulos 9.8.2 y 9.8.3:

9.8.2.-Mensaje: RECEPCIÓN DE ÓRDENES

(...)

LONGITUD = 2 bytes. Define el tamaño en bytes de los datos específicos del mensaje.

En este caso Tamaño(ID Mensaje) + Tamaño(ID ORDEN) + Tamaño(TIPO RESPUESTA) + Tamaño(TIEMPO ESTIMADO DE RESPUESTA) = 5

(...)

9.8.3.-Mensaje: RESPUESTA DE ÓRDENES

(...)

LONGITUD = 2 bytes. Define el tamaño en bytes de los datos específicos del mensaje.

En este caso Tamaño(ID Mensaje) + Tamaño(ID ORDEN) + Tamaño(RESPUESTA) + Tamaño(CÓDIGO DE RECHAZO)

(...)

Texto propuesto:

9.8.2.-Mensaje: RECEPCIÓN DE ÓRDENES

(...)

***LONGITUD** = 2 bytes. Define el tamaño en bytes de los datos específicos del mensaje.*

En este caso Tamaño(ID Mensaje) + Tamaño(ID ORDEN) + Tamaño(TIPO RESPUESTA) + Tamaño (TIEMPO ESTIMADO DE RESPUESTA) = 4

(...)

9.8.3.-Mensaje: RESPUESTA DE ÓRDENES

(...)

***LONGITUD** = 2 bytes. Define el tamaño en bytes de los datos específicos del mensaje.*

En este caso Tamaño(ID Mensaje) + Tamaño(ID ORDEN) + Tamaño(RESPUESTA) + Tamaño(CÓDIGO DE RECHAZO) = 4

(...)

2.11.-MODIFICACIÓN 11

Se modifica el texto para añadir el código de respuesta 0x03 y se amplía el texto del código de rechazo 0x00 en el mensaje de RESPUESTA DE ÓRDENES para aquellos casos en los que el enclavamiento no proporciona información de orden aceptada/rechazada.

Texto original en el capítulo 9.8.3:

9.8.3.-Mensaje: RESPUESTA DE ÓRDENES

(...)

RESPUESTA = 1 byte para el tipo de respuesta que puede tomar los siguientes valores:

0x00 -> Orden ejecutada por ENC

0x01 -> Mando especial requerido

0x02 -> Orden no ejecutada (códigos de rechazo)

CÓDIGO DE RECHAZO = 1 byte

0x00 -> Orden ejecutada, mando especial requerido o sin información de rechazo

0x01 -> Orden Rechazada o No permitida

0x02 -> La orden recibida no existe

0x03 -> ME no permitido

0x04 -> ME en curso

0x05 -> En este momento mandos no efectivos (Por ejemplo, si la Remota pierde la comunicación con el ENC)

0x06 -> El CTC que envía la orden no tiene el mando

(...)

Texto propuesto:

9.8.3.-Mensaje: RESPUESTA DE ÓRDENES

(...)

***RESPUESTA** = 1 byte para el tipo de respuesta que puede tomar los siguientes valores:*

0x00 -> Orden ejecutada por ENC

0x01 -> Mando especial requerido

0x02 -> Orden no ejecutada (códigos de rechazo)

0X03 -> Sin información de la ejecución o rechazo de la orden

***CÓDIGO DE RECHAZO** = 1 byte*

0x00 -> Orden ejecutada, mando especial requerido o sin información de ejecución o rechazo

0x01 -> Orden Rechazada o No permitida

0x02 -> La orden recibida no existe

0x03 -> ME no permitido

0x04 -> ME en curso

0x05 -> En este momento mandos no efectivos (Por ejemplo, si la Remota pierde la comunicación con el ENC)

0x06 -> El CTC que envía la orden no tiene el mando

(...)

2.12.-MODIFICACIÓN 12

Se especifica que se deben enviar todos los cambios de estado producidos entre petición y petición en modo P-R.

Texto original en los capítulos 9.7 y 11.1:

9.7.-MENSAJES DE CONOCIMIENTO DE ESTADO

(...)

En modo P-R:

(...)

Cuando la Remota reciba el mensaje PETICIÓN DE CAMBIOS DE ESTADO, enviará el estado de todos los elementos que hayan sufrido cambios desde la anterior petición, mediante los mensajes de CAMBIOS DE ESTADO que sean necesarios. En caso de que no se hayan producido cambios enviará el mensaje SIN CAMBIOS DE ESTADO.

(...)

11.1.- FORMATO DE LAS INDICACIONES

Los mensajes de CAMBIOS DE ESTADO y ESTADO COMPLETO se utilizan para enviar al CTC las indicaciones del enclavamiento. Ambos mensajes contienen el campo CAMBIOS DE ESTADO que se conformará con los valores ASCII de los elementos y sus estados con el siguiente formato.

Etiqueta1,Tipoelemento1,Estadoelemento1;Etiqueta2,Tipoelemento2,Estadoelemento2;...;EtiquetaN,TipoelementoN,EstadoelementoN

La separación entre distintos elementos se realizará utilizando ";", no siendo necesario añadirlo tras el último elemento.

En la NAS 831 "Catálogo de indicaciones para las comunicaciones entre CTC y enclavamiento de Adif mediante uso de protocolos TCP/IP", se detallan las indicaciones oportunas para que las etiquetas identificativas de cada objeto de una instalación especifica se asignen con un criterio preestablecido y homogéneo. Asimismo, en dicha norma se codifican y detallan los diferentes tipos de elementos a utilizar. Cada etiqueta constará del nemónico del enclavamiento, seguido de dos puntos (":") y el nombre del objeto.

(...)

Texto propuesto:

9.7.-MENSAJES DE CONOCIMIENTO DE ESTADO

(...)

<u>En modo P-R:</u>

(...)

Cuando la Remota reciba el mensaje PETICIÓN DE CAMBIOS DE ESTADO, enviará todos los cambios de estado que se hayan producido desde la anterior petición, mediante los mensajes de CAMBIOS DE ESTADO que sean necesarios. En caso de que no se hayan producido cambios enviará el mensaje SIN CAMBIOS DE ESTADO.

(...)

11.1.- FORMATO DE LAS INDICACIONES

Los mensajes de CAMBIOS DE ESTADO y ESTADO COMPLETO se utilizan para enviar al CTC las indicaciones del enclavamiento. Ambos mensajes contienen el campo CAMBIOS DE ESTADO que se conformará con los valores ASCII de los elementos y sus estados con el siguiente formato:

Etiqueta1,Tipoelemento1,Estadoelemento1;Etiqueta2,Tipoelemento2,Estadoelemento2; ...;EtiquetaN,TipoelementoN,EstadoelementoN.

La separación entre distintos elementos se realizará utilizando ";", no siendo necesario añadirlo tras el último elemento.

La posición del elemento en la cadena indica el orden en el que se han producido los cambios de estado, siendo el elemento más a la izquierda el más antiguo. Un mismo elemento podría llegar a aparecer varias veces, quedando en el estado final que determine su última aparición en la cadena.

En la NAS 831 "Catálogo de indicaciones para las comunicaciones entre CTC y enclavamiento de Adif mediante uso de protocolos TCP/IP", se detallan las indicaciones oportunas para que las etiquetas identificativas de cada objeto de una instalación especifica se asignen con un criterio preestablecido y homogéneo. Asimismo, en dicha norma se codifican y detallan los diferentes tipos de elementos a utilizar. Cada etiqueta constará del nemónico del enclavamiento, seguido de dos puntos (":") y el nombre del objeto.

(...)

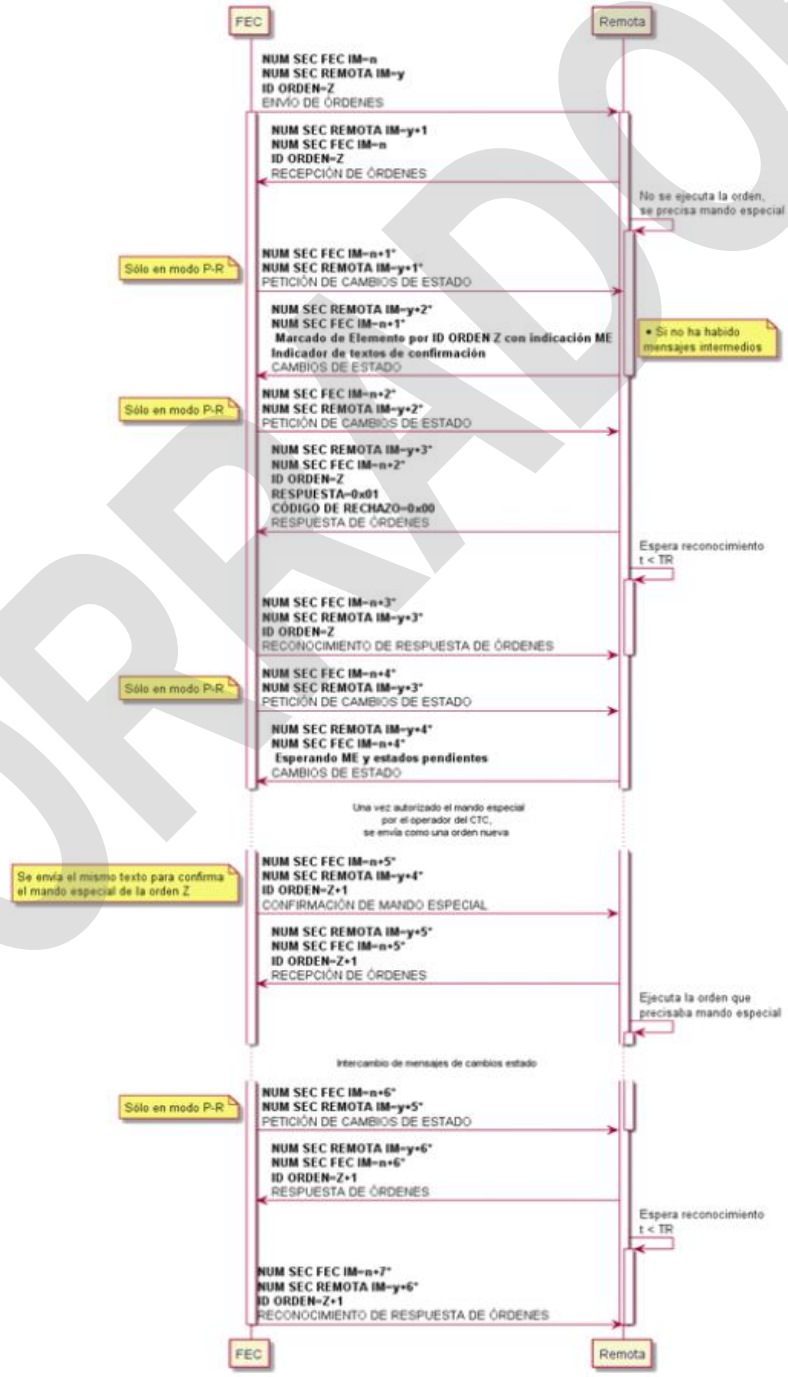
2.13.-MODIFICACIÓN 13

Se modifican los esquemas caso 1 y caso 2 añadiendo el mensaje de RECONOCIMIENTO DE CAMBIOS DE ESTADO a la recepción de CAMBIOS DE ESTADO, según establece el protocolo.

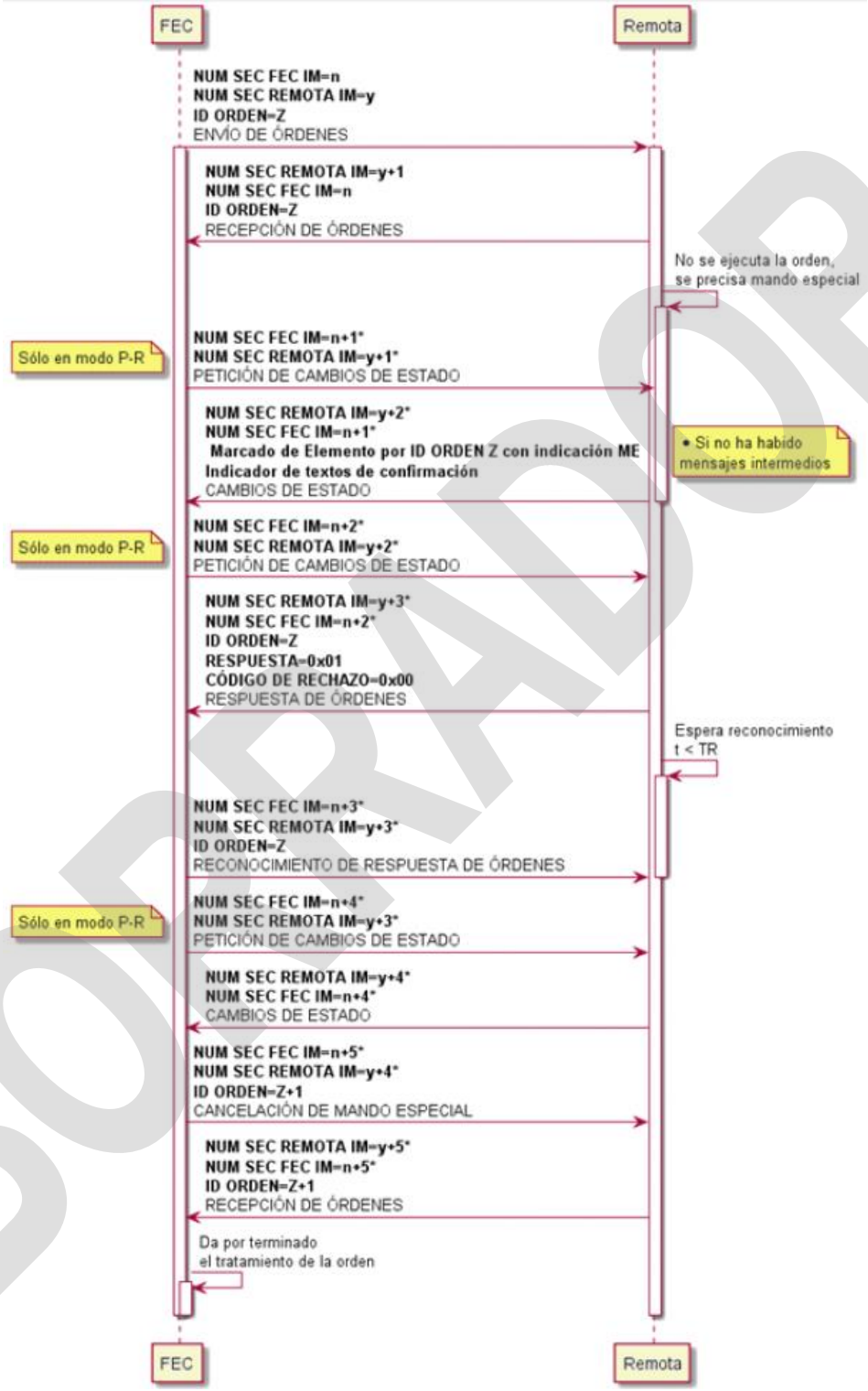
Texto original en el capítulo 10.4.3:

10.4.3.-Envío de órdenes con solicitud de mando especial

Caso 1: Recepción de CONFIRMACIÓN DE MANDO ESPECIAL.



Caso 2: Recepción de CANCELACIÓN DE MANDO ESPECIAL

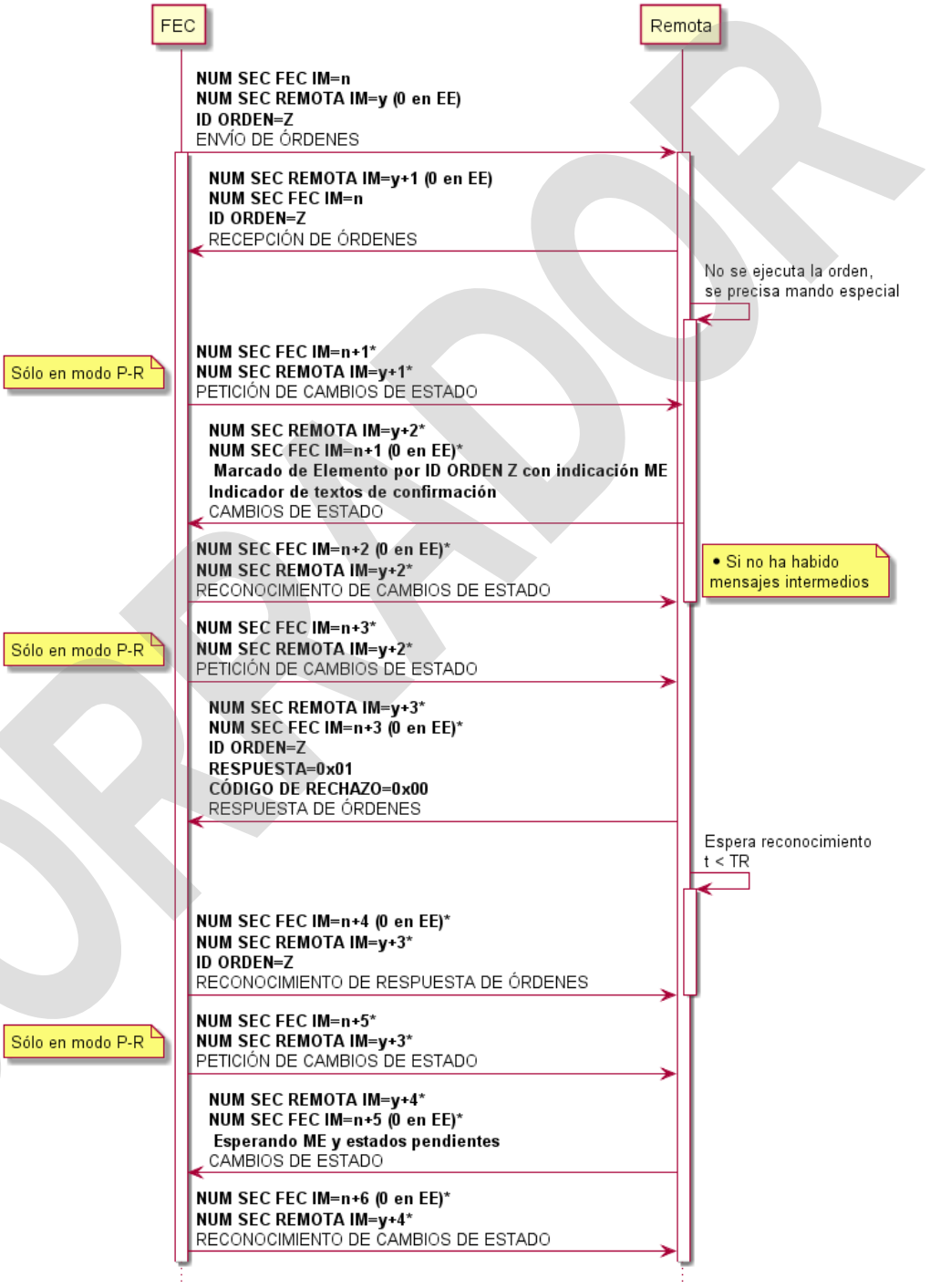


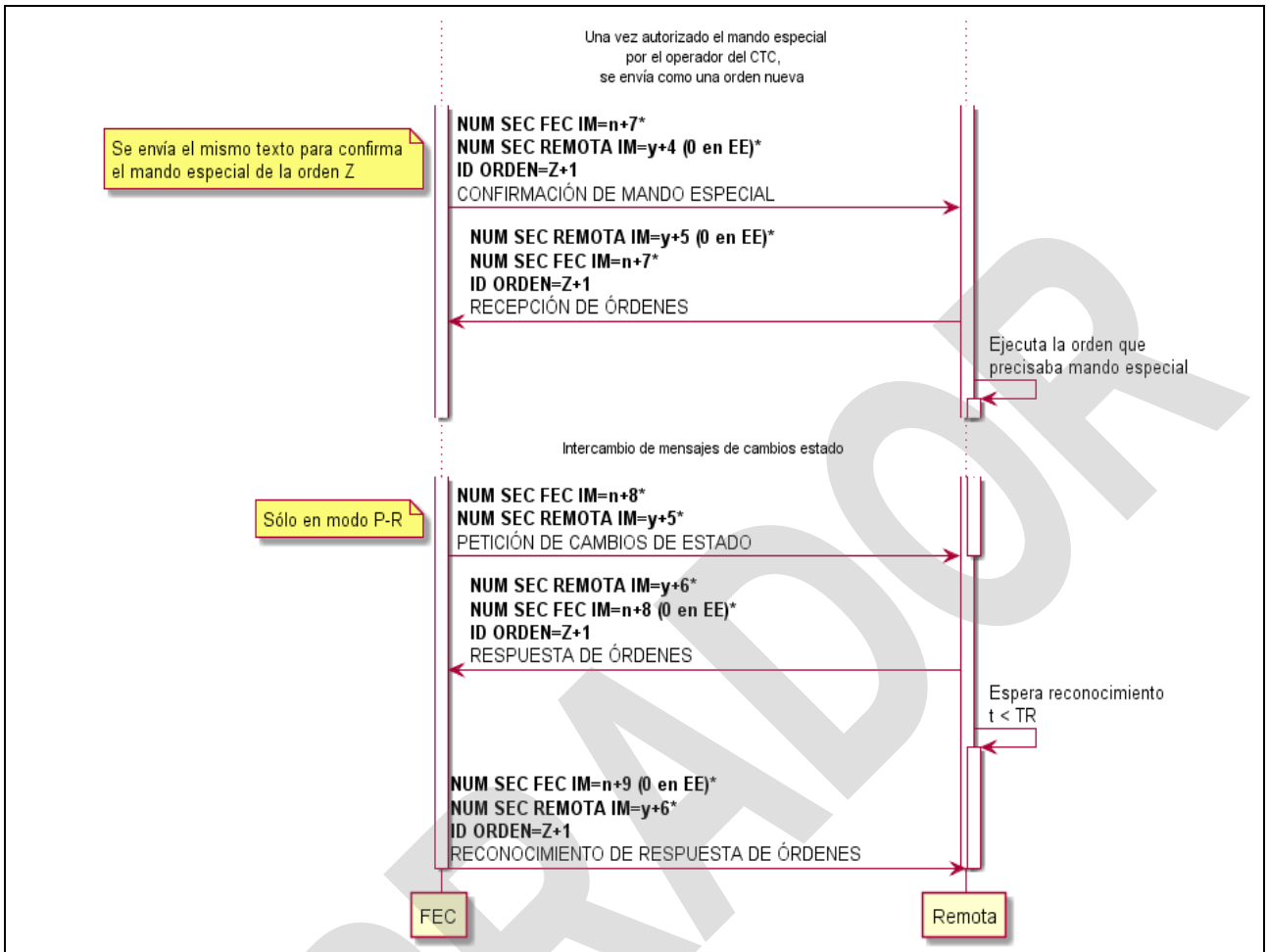
(...)

Texto propuesto:

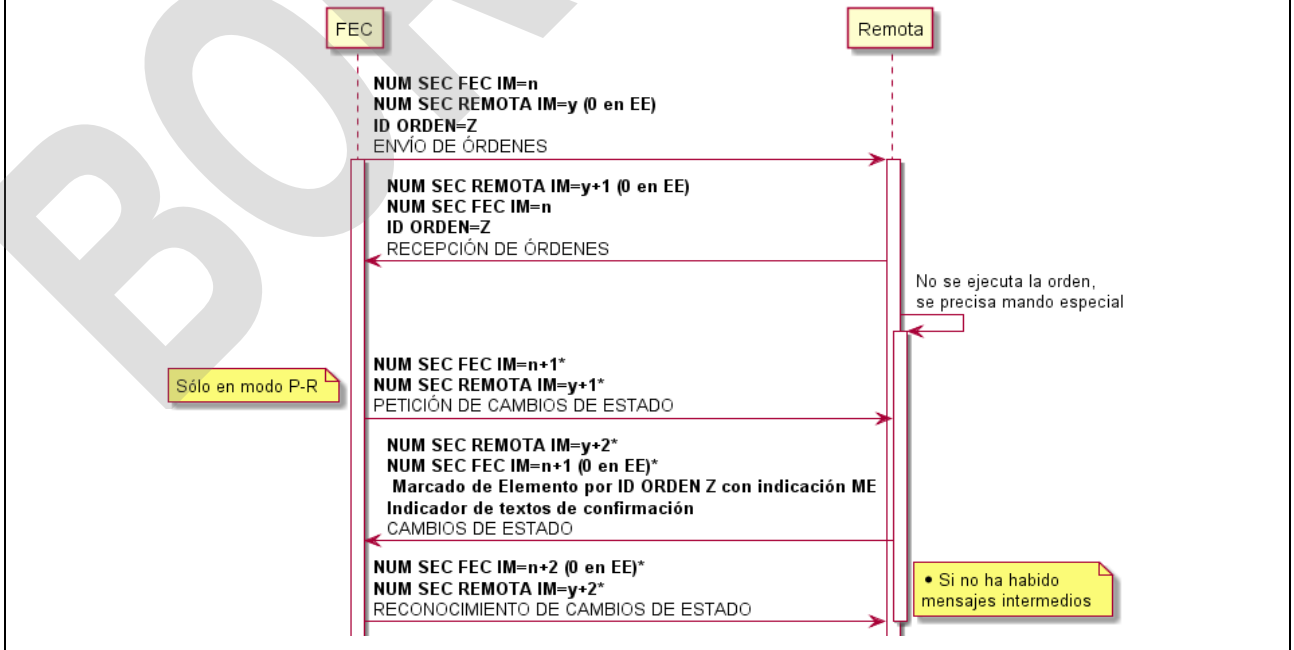
10.4.3.-Envío de órdenes con solicitud de mando especial

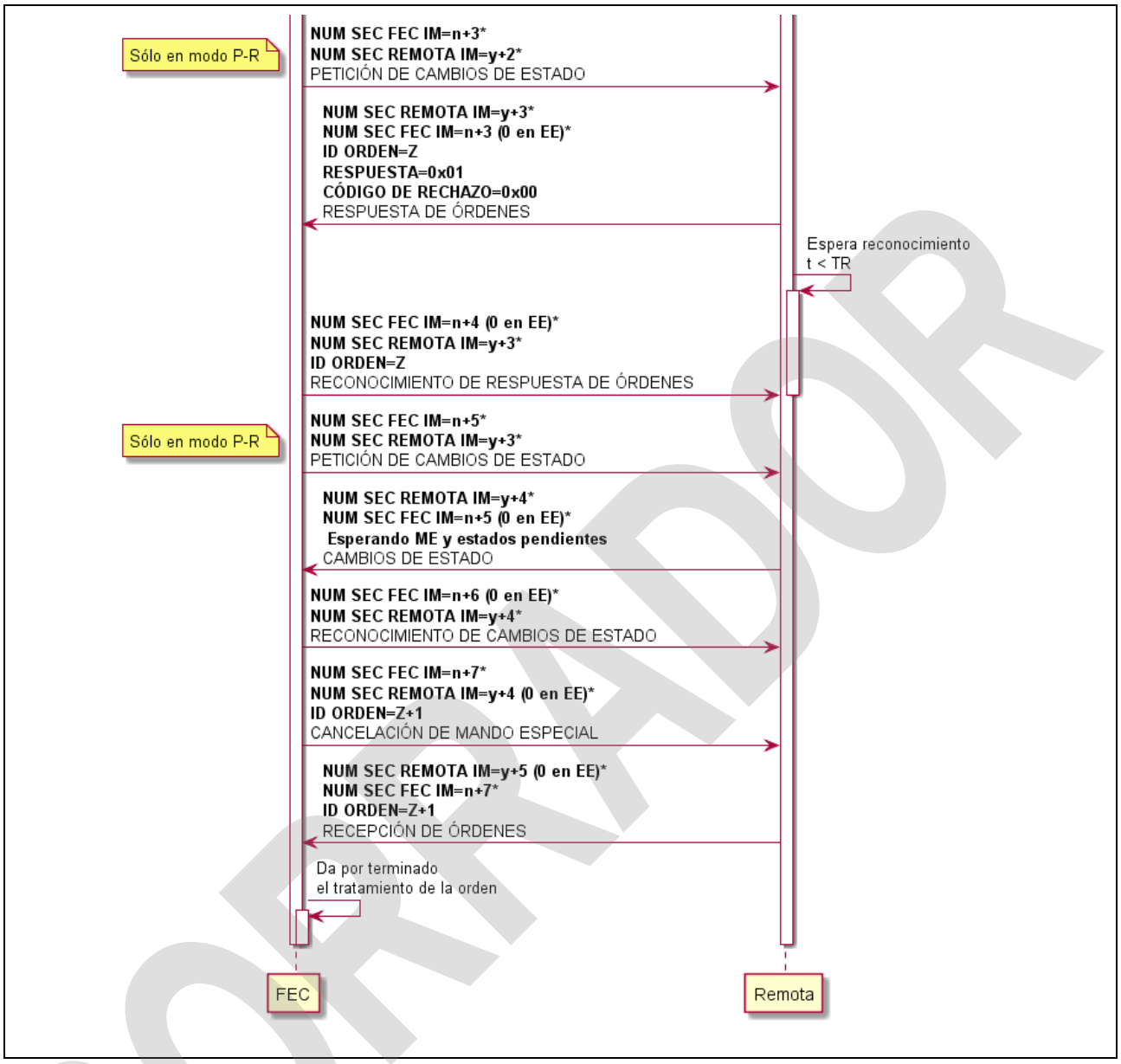
Caso 1: Recepción de CONFIRMACIÓN DE MANDO ESPECIAL (modo P-R).





Caso 2: Recepción de CANCELACIÓN DE MANDO ESPECIAL (modo P-R).





2.14.-MODIFICACIÓN 14

Se añade nuevo apartado 11.3 con los caracteres ASCII admitidos en las órdenes.

Texto propuesto:

11.3.-CODIFICACIÓN ASCII

Los valores ASCII a emplear en el formato de mandos se corresponden con los caracteres imprimibles del 32 al 126 de la codificación US-ASCII, ampliado con los necesarios del ASCII extendido CP437, representados en la siguiente tabla:

ASCII	Hex	Símbolo
32	20	(espacio)
33	21	!
34	22	"
35	23	#
36	24	$
37	25	%
38	26	&
39	27	'
40	28	(

ASCII	Hex	Símbolo
41	29	)
42	2A	*
43	2B	+
44	2C	,
45	2D	-
46	2E	.
47	2F	/
48	30	0
49	31	1
50	32	2

ASCII	Hex	Símbolo
51	33	3
52	34	4
53	35	5
54	36	6
55	37	7
56	38	8
57	39	9
58	3A	:
59	3B	;
60	3C	<

ASCII	Hex	Símbolo
61	3D	=
62	3E	>
63	3F	?
64	40	@
65	41	A
66	42	B
67	43	C
68	44	D
69	45	E
70	46	F

ASCII	Hex	Símbolo
71	47	G
72	48	H
73	49	I
74	4A	J
75	4B	K
76	4C	L
77	4D	M
78	4E	N
79	4F	O
80	50	P

ASCII	Hex	Símbolo
81	51	Q
82	52	R
83	53	S
84	54	T
85	55	U
86	56	V
87	57	W
88	58	X
89	59	Y
90	5A	Z

ASCII	Hex	Símbolo
91	5B	[
92	5C	\
93	5D	]
94	5E	^
95	5F	_
96	60	`
97	61	a
98	62	b
99	63	c
100	64	d

ASCII	Hex	Símbolo
101	65	e
102	66	f
103	67	g
104	68	h
105	69	i
106	6A	j
107	6B	k
108	6C	l
109	6D	m
110	6E	n

ASCII	Hex	Símbolo
111	6F	o
112	70	p
113	71	q
114	72	r
115	73	s
116	74	t
117	75	u
118	76	v
119	77	w
120	78	x

ASCII	Hex	Símbolo
121	79	y
122	7A	z
123	7B	{
124	7C	|
125	7D	}
126	7E	~
164	A4	ñ
165	A5	Ñ

2.15.-MODIFICACIÓN 15

Se reordena la colocación de los capítulos 12, 13 y 14, actualizando la 'Normativa Derogada' y añadiendo párrafos aclaratorios en 'Normativa de referencia'.

Texto original:

12.-NORMATIVA DE REFERENCIA

•NAS 831. Catálogo de indicaciones para las comunicaciones entre CTC y enclavamiento de Adif mediante uso de protocolos TCP/IP.

•UNE-EN 50159:2011. Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Comunicación relacionada con la seguridad en sistemas de transmisión.

•Guía de Seguridad de las TIC CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad.

13.-DISPOSICIONES TRANSITORIAS Y ENTRADA EN VIGOR

El presente documento entrará en vigor en la fecha de su aprobación.

14.-NORMATIVA DEROGADA

El presente documento no deroga ninguna norma.

Texto propuesto:

12.-NORMATIVA DEROGADA

El presente documento deroga a la NAS 830. Protocolo Estándar de Adif para las comunicaciones entre CTC y enclavamiento SCI-CC-A. Versión 1.0. 1ª Edición: Julio de 2021. Adif.

13.-DISPOSICIONES TRANSITORIAS Y ENTRADA EN VIGOR

El presente documento entrará en vigor en la fecha de su aprobación.

14.-NORMATIVA DE REFERENCIA

En el contenido de esta norma se hace referencia a los documentos normativos que se citan a continuación.

Cuando se trate de legislación, será de aplicación la última versión publicada en los diarios oficiales, incluidas sus sucesivas modificaciones.

En el caso de documentos referenciados sin edición y fecha se utilizará la última edición vigente; en el caso de normas citadas con versión exacta, se debe aplicar esta edición concreta.

En el caso de normas UNE EN que establezcan condiciones armonizadas para la comercialización de productos de construcción, que sean transposición de normas EN cuya referencia haya sido publicada en el Diario Oficial de la Unión Europea, será de aplicación la última versión comunicada por la Comisión y publicada en el DOUE.

- *NAS 831. Catálogo de indicaciones para las comunicaciones entre CTC y enclavamiento de Adif mediante uso de protocolos TCP/IP. Adif.*
- *UNE-EN 50159:2011. Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Comunicación relacionada con la seguridad en sistemas de transmisión. AENOR.*
- *Guía de Seguridad de las TIC CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad. Centro Criptológico Nacional. Ministerio de Defensa.*