

Guía de Seguridad de las TIC

CCN-STIC 1416

Procedimiento de Empleo Seguro
MIL2004-2xHSR-L3 de SoCe System-on-Chip engineering/Novatronic



Agosto 2020

Edita:



© Centro Criptológico Nacional, 2020
NIPO: 083-20-140-9

Fecha de Edición: agosto de 2020

SoCe ha participado en la realización y modificación del presente documento.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Agosto de 2020



Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

INDICE

1 INTRODUCCIÓN	5
2 OBJETO Y ALCANCE	6
3 ORGANIZACIÓN DEL DOCUMENTO	7
4 FASE DE DESPLIEGUE E INSTALACIÓN	8
4.1 ENTREGA SEGURA DEL PRODUCTO	8
4.2 ENTORNO DE INSTALACIÓN	8
4.3 REGISTRO Y LICENCIAS	8
4.4 CONSIDERACIONES PREVIAS	9
4.5 INSTALACIÓN.....	9
5 FASE DE CONFIGURACIÓN	10
5.1 MODO DE OPERACIÓN SEGURO	10
5.2 AUTENTICACIÓN.....	10
5.3 ADMINISTRACIÓN DEL PRODUCTO.....	11
5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.....	11
5.3.2 CONFIGURACIÓN DE ADMINISTRADORES	13
5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	14
5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS	14
5.6 GESTIÓN DE CERTIFICADOS.....	16
5.7 SERVIDORES DE AUTENTICACIÓN	17
5.8 SINCRONIZACIÓN HORARIA	17
5.9 AUTO-CHEQUEOS.....	17
5.10 SNMP.....	18
5.11 ALTA DISPONIBILIDAD	18
5.12 AUDITORÍA	19
5.12.1 REGISTRO DE EVENTOS	19
5.12.2 ALMACENAMIENTO LOCAL	20
5.12.3 ALMACENAMIENTO REMOTO	21
5.13 SERVICIOS DE SEGURIDAD	22
6 FASE DE OPERACIÓN Y MANTENIMIENTO.....	23
6.1 ACTUALIZACIONES	24
7 CHECKLIST.....	27
8 REFERENCIAS	29
9 ABREVIATURAS.....	30

1 INTRODUCCIÓN

1. *MIL2004* es un equipo militar de comunicaciones potente y flexible. Este equipo proporciona comunicación de red de capa 2 y capa 3 en el modelo de interconexión de sistemas abiertos OSI con capacidades de alta velocidad y disponibilidad en combinación con unas altas medidas de seguridad. Incorpora una plataforma configurable *Xilinx Zynq Ultrascale+ MPSoC* para proporcionar capacidades de computación tanto *hardware* como *software*.
2. Las principales características de este equipo son:
 - a) Adaptado a las necesidades de Programas Militares de Defensa que requieren plataformas de computación y comunicación heterogéneas.
 - b) Interfaces de comunicación de diferentes velocidad y tipo:
 - 20x Puertos 10/100/1000Base-T gestionables.
 - 4x Puertos 1000Base-SR/LR para enlaces de Fibra Óptica.
 - 1x Puerto Ethernet de Servicio de propósito general.
 - 1x Puerto de Consola RS232 auxiliar.
 - c) Gestión, seguridad y monitorización multicapa.
 - d) Supervisor independiente del estado interno del equipo mediante microcontrolador resistente a radiaciones.
 - e) Dispositivos internos de seguridad.
 - f) Fuente de alimentación de doble redundancia MIL-STD-704-AC/DC.
 - g) Panel frontal de indicadores LED.
 - h) Filtros duales de entrada de energía en línea EMI/EMC.
 - i) Monitorización de temperatura (Mín./Máx.) en tiempo real.
 - j) Modos de control del sistema: *Remote Reset, Battleshort & Standby*.
 - k) Testado y certificado por laboratorio independiente de acuerdo con los estándares MIL-STD-810G & MIL-STD-461G.

2 OBJETO Y ALCANCE

3. El presente documento recoge el procedimiento de empleo seguro para el equipo MIL2004-2xHSR-L3, que combina una potente matriz con un bloque de conmutación HSR/PRP dedicado, que presenta la siguiente configuración de puertos:
 - 20x Puertos 10/100/1000Base-T gestionables.
 - 4x Puertos 1000Base-SR/LR para enlaces de Fibra Óptica, sobre los que es posible configurar 2 anillos HSR u otras combinaciones.
 - 1 x Puerto Ethernet de Servicio de propósito general.
4. El diseño está enfocado en proporcionar aceleración *hardware* en las operaciones de conmutación de paquetes en las Capas 2 y 3 del modelo OSI en combinación con una alta disponibilidad *Ethernet* (Capa 2). **La versión de *firmware* sobre la que hace referencia este documento es la 19.12.**

3 ORGANIZACIÓN DEL DOCUMENTO

5. El presente documento se estructura de acuerdo con los siguientes capítulos:

- **Apartado 4.** En este apartado se recogen recomendaciones que deben tenerse en cuenta durante la fase de despliegue e instalación del producto.
- **Apartado 5.** En este apartado se recogen las recomendaciones que deben tenerse en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- **Apartado 7.** Finalmente, en este apartado se resumirá a modo de *checklist* las recomendaciones listadas en los apartados anteriores que deben tenerse en consideración a la hora de utilizar el equipo.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

6. Tras la recepción del equipo, deberá verificarse que el etiquetado de la caja coincide con el etiquetado del equipo, con la referencia del albarán, y con el código especificado en el pedido. En especial, debe comprobarse que la configuración de la fuente de alimentación recibida coincide con la que el usuario tiene previsto utilizar.
7. Para ello, el usuario deberá usar como referencia la codificación del Sistema de alimentación integrado. A continuación, se muestra un ejemplo decodificación específica y la correspondencia cada una de las secciones del código con distintos aspectos del modelo de equipo seleccionado:

MIL2004¹2xHSR-L3²/PLUS³/2DR 28VDC⁴ 220VAC⁵ D-150W⁶/B⁷/E⁸

- 1 – Nombre de producto
- 2 – Código de Personalidad
- 3 – Versión del sistema
- 4 – Fuente de alimentación principal
- 5 – Fuente de alimentación secundaria
- 6 – Salida de tensión PSU
- 7 – Mecánica
- 8 - Color

4.2 ENTORNO DE INSTALACIÓN

8. El equipo MIL2004-2xHSR-L3 no ha sido concebido para su instalación en un Centro de Proceso de Datos (CPD), por lo que no aplican los requisitos de seguridad física asociados a estos espacios.
9. El equipo ha sido diseñado para el sector defensa y normalmente se instala de forma embarcada en vehículos móviles, tanto de tierra como de aire o mar, que ya cuentan con un sistema de seguridad propio del sector, por lo que no es necesario considerar ningún requisito de seguridad relativo al entorno..

4.3 REGISTRO Y LICENCIAS

10. El usuario no requiere realizar ningún registro de licencias. El propio fabricante del equipo MIL2004-2xHSR-L3 es quien lleva el registro de los números de serie de los equipos, así como de todos los componentes tanto *hardware* como *software* del mismo para poder realizar una correcta trazabilidad de todos los equipos.

4.4 CONSIDERACIONES PREVIAS

11. Es recomendable tener en cuenta la distancia del equipo MIL2004-2xHSR-L3 a los paneles de conexión, ya que se utiliza cableado muy específico y de una longitud determinada, que es suministrado por el fabricante.
12. También es necesario disponer de una superficie de anclaje poco rugosa, que permita la correcta disipación de calor a través de la superficie de contacto con la base de anclaje del equipo MIL2004-2HSR-L3.

4.5 INSTALACIÓN

13. El equipo se suministra con una mecánica del equipo MIL2004-2xHSR-L3 que incluye una base para el anclaje mediante 6 tornillos M4 a una superficie estable. Además, dicha base desempeña funciones de disipación por lo que, para aplicaciones intensivas con elevados requisitos de disipación es recomendable que la superficie de anclaje tenga una rugosidad inferior a los 2um, para conseguir una superficie de contacto óptima.
14. Para el arranque del equipo no es necesario seguir ninguna secuencia preestablecida. Solo es necesario conectar el cable de alimentación al equipo para tener acceso a él a través de los puertos serie y Ethernet.
15. El resto de cableado puede conectarse y desconectarse mientras el equipo está funcionando, sin afectar a su correcta operativa. En este apartado se describe cómo llevar a cabo la instalación de cada componente del producto, haciendo énfasis en los aspectos necesarios para la instalación y configuración segura.
16. El equipo se suministra con todo el *firmware* preinstalado y no requiere de componentes adicionales tipo *token*, etc. para su correcto funcionamiento.

5 FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

18. El estado inicial del equipo tiene habilitados por defecto los mecanismos de seguridad especificados en este Procedimiento de Empleo.

5.2 AUTENTICACIÓN

19. El equipo permite ser gestionado mediante los mecanismos de acceso *interfaz web*, *SSH* y *puerto serie*. En cada uno de ellos, el usuario debe autenticarse mediante un usuario y contraseña.
20. El equipo MIL2004-2xHSR-L3 define dos (2) roles de usuarios, distinguiéndolos entre sí en función de los permisos de acceso a características de configuración. Ambos roles tienen asociados un nombre de usuario y una contraseña. Los dos (2) roles soportados por el equipo son:
 - **Basic user:** Acceso a configuraciones básicas de red, configuración de protocolos de *switch*, lectura de estadísticos y lectura de *logs*. No permite el uso del modo AVANZADO del equipo.
 - **Advanced user:** Permite todo lo contenido en el rol de *Basic user* y además permite operar con el modo AVANZADO del equipo que incluye:
 - Modificación de reglas de rutado.
 - Modificación de parámetros de seguridad propios del equipo (timeout, fail2ban, firewall...)
 - Actualización del firmware del equipo.
 - Aplicación de parches.
 - Cambio de contraseñas.
 - Cambio de imagen característica del equipo.
 - Subida de nuevos certificados para el establecimiento de conexiones seguras.
21. Para el acceso mediante interfaz web, el equipo dispone de un usuario definido para cada rol:
 - Para el rol *Basic user*, se ha definido el usuario **user**.
 - Para el rol *Advanced user*, se ha definido el usuario **admin**.
22. Si el acceso se realiza por SSH o puerto serie, solo está disponible el rol de *Advanced user*, a través del usuario soc-e.
23. Las contraseñas asociadas a los usuarios deben cumplir con el siguiente requisito de seguridad, que no puede ser modificado:
 - Longitud mínima de 12 caracteres.

24. Deberán utilizarse contraseñas largas, compuestas por al menos tres (3) juegos de estos tipos de caracteres: letras minúsculas, mayúsculas, números y caracteres especiales.
25. El MIL2004-2xHSR-L3 dispone de la utilidad específica para llevar a cabo un registro de los intentos fallidos de inicio de sesión en sus interfaces de acceso. De esta forma, se pueden modificar la configuración de dicha utilidad para establecer el número de intentos fallidos. Un usuario no podrá llevar a cabo una autenticación exitosa a cualquiera de las interfaces del equipo una vez que alcance el número de intentos fallidos establecidos en la configuración de la utilidad *fail2ban*. Los parámetros de número de intentos fallidos y tiempo de bloqueo se pueden configurar en el fichero */etc/fail2ban/jail.d/jail.local.vars*.
26. Cuando un usuario es bloqueado, es necesario esperar a que transcurra el tiempo de bloqueo. No será posible su desbloqueo de ninguna otra manera.
27. Además, el equipo implementa mecanismos de seguridad para proteger las credenciales de autenticación para que no puedan ser accesibles por ningún usuario ni dispositivo conectado al dispositivo.
28. El MIL2004-2xHSR-L3 impide que ningún usuario o dispositivo no autorizados pueda utilizar o acceder a las contraseñas de usuario de la siguiente forma:
 - a) Todas las contraseñas almacenadas están protegidas criptológicamente y nunca en texto plano.
 - b) El equipo evita la lectura de contraseñas cuando se introducen en la interfaz de configuración mediante su ofuscación.
 - c) El equipo no dispone de ningún tipo de mecanismo o característica que permita la lectura de las contraseñas.
29. En el [apartado 5.5](#) se describen los mecanismos de cifrado utilizados para la protección de las claves almacenadas.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

30. El equipo MIL2004-2xHSR-L3 permite la administración de su configuración tanto de forma local como remota a través de sus interfaces:
 - Mediante la interfaz web y la conexión mediante SSH se puede realizar una administración remota de su configuración.
 - Mediante la conexión al puerto serie se puede realizar una administración local de su configuración.
31. Para todas las posibilidades de conexión, el equipo requerirá unas credenciales de usuario (nombre de usuario y contraseña) para poder acceder a la configuración del propio equipo. Si se accede por interfaz web aparecerá la siguiente ventana:

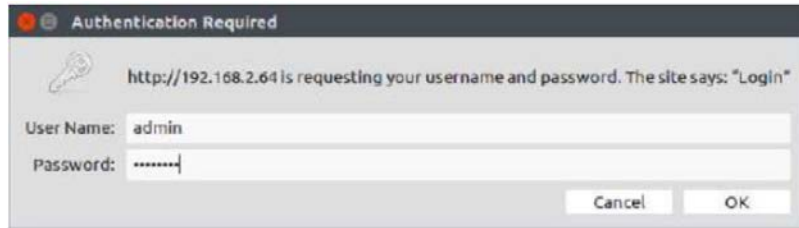


Figura 1. Autenticación en interfaz web

32. Mientras que, si se realiza la conexión mediante terminal (ya sea utilizando SSH o por puerto serie), aparecerá el siguiente tipo de diálogo (esto dependerá del programa utilizado para realizar la conexión):



Figura 2. Autenticación mediante terminal

33. El equipo permite la configuración del tiempo de finalización de sesión en todas las interfaces de acceso que dispone (interfaz web, conexión SSH y puerto serie). Este tiempo de finalización de sesión puede ser modificado por un usuario con el rol *advanced user* en el fichero:
- `/home/soc-e/.bashrc` variable `TMOU`T en segundos para el acceso mediante SSH y puerto serie
 - `/etc/spt_service/configs/current/session_timeout.conf`
variable `session_timeout` en minutos para el acceso mediante interfaz web
34. Se recomienda establecer tiempos de finalización de sesión iguales o inferiores a **10 minutos**.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

35. El MIL2004-2xHSR-L3 admite un único usuario con perfil de administrador para acceder a la configuración del equipo a través del Web Manager. Deberá modificarse la contraseña por defecto cuando se use por primera vez y cada vez que sea necesario, de acuerdo a la política de actualización de contraseñas. Para modificar la contraseña del usuario administrador en el Web Manager, el usuario debe acceder al menú "Account" haciendo *click* en la siguiente sección:

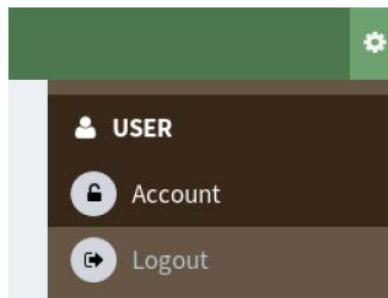


Figura 3. Menú "Account"

36. El menú anterior solo está disponible para el usuario Administrador. Una vez en el menú "Account", el usuario deberá introducir dos veces la nueva contraseña y guardar los cambios, tal y como se muestra en la siguiente imagen.

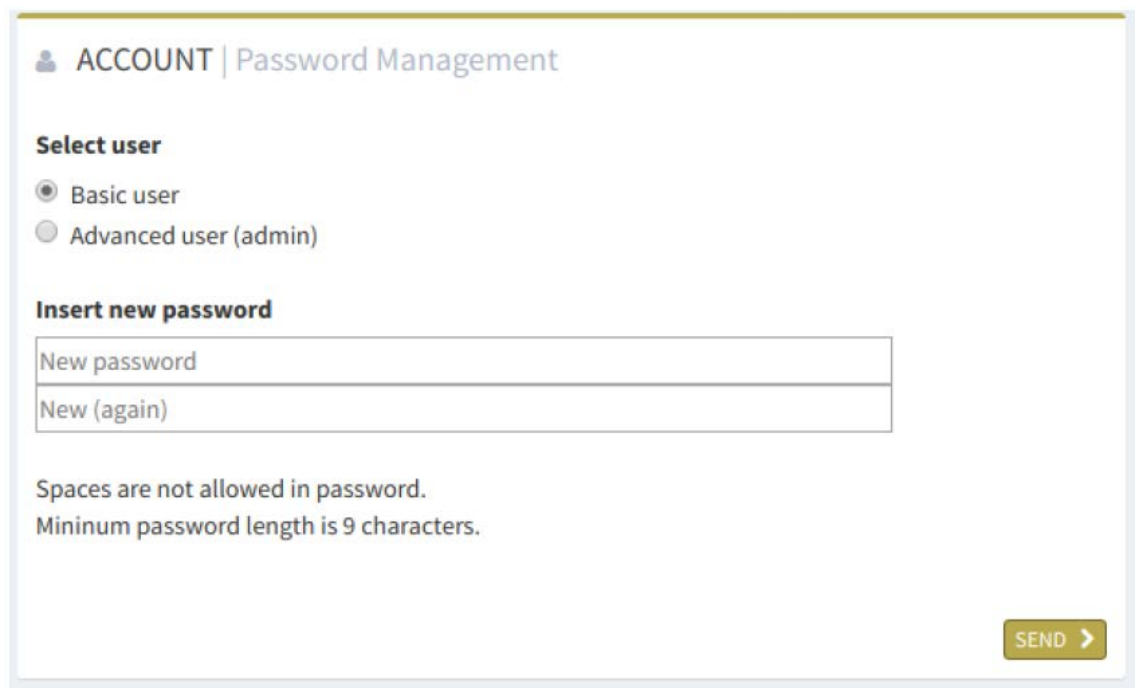


Figura 4. Menú para el cambio de contraseñas

37. Del mismo modo, el equipo sólo admite un usuario con perfil de administrador para acceder a través de SSH. Para modificar la contraseña del usuario administrador de SSH, deberá utilizarse el comando *passwd* en la línea de comandos CLI e introducir la nueva contraseña cuando se solicite.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Como norma general, deberán deshabilitarse todos aquellos puertos, servicios o interfaces que no vayan a ser utilizados.

38. El MIL2004-2xHSR-L3 permite habilitar o deshabilitar los puertos como una característica de seguridad con el objetivo de evitar conexiones no deseadas al propio equipo. Para llevar a cabo esta configuración se debe utilizar el acceso mediante línea de comandos que ofrece el equipo y ejecutar el siguiente comando:

- **`spt_config_reg -f J1A:enable_port -w 0x0`**

39. De este modo, se deshabilita el puerto J1A del equipo para impedir el paso de tráfico por el mismo. Si se necesita habilitar un puerto, hay que utilizar el mismo comando, pero de la siguiente forma:

- **`spt_config_reg -f J1A:enable_port -w 0x1`**

40. Del mismo modo, es posible habilitar y deshabilitar servicios e interfaces mediante línea de comando con comandos análogos a los anteriores.

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

41. El equipo MIL2004-2xHSR-L3 proporciona un canal de comunicación seguro al administrador remoto. Para cada una de las situaciones en las que un administrador realiza una conexión remota al equipo, se proporcionan los siguientes mecanismos de seguridad:

- Uso de HTTPS para el acceso mediante la interfaz web. Para ello hay que acceder al navegador mediante la siguiente URL: *https://device's-IP* donde *device's IP* es la dirección IP asignada al mismo.
- Uso del protocolo SSH para realizar acceso al equipo mediante el uso de terminal. El equipo soporta SSH v2 para operaciones remotas, proporcionando mecanismos de cifrado y autenticación a la comunicación.

42. El equipo soporta IEEE 802.1X para hacer posible el establecimiento de comunicaciones seguras. Este estándar se utiliza para implementar un control de acceso basado en puertos en la red donde se encuentra el equipo desplegado. El protocolo basado en este estándar es EAPOL (*EAP encapsulation over LANs*). EAPOL es un *framework* de autenticación que permite bloquear el paso de una comunicación a través de un puerto del equipo excepto el tráfico EAPOL. Mientras que no se produzca la autenticación de un dispositivo en un puerto, no se podrá desbloquear. Es posible configurar esta característica llevando a cabo los siguientes pasos:

- **A través de la interfaz web:** En el menú superior, seleccionar la funcionalidad *Advanced Network -> Port Security*. En este apartado se mostrará la lista de puertos del equipo. En esta lista se puede seleccionar un puerto determinado y seleccionar el *authentication type* deseado. Las opciones disponibles son:

- Modo de autenticación manual. Permite al usuario bloquear o permitir el tráfico que transcurre por un puerto de forma manual.
- Modo de autenticación 802.1X. Permite la ejecución del protocolo EAPOL que habilita la autenticación SAKÉ.
- Modo de autenticación de direcciones MAC. Permite a una dirección MAC conectarse a un puerto determinado. Esta configuración se puede realizar de forma manual.
- **A través de la conexión mediante SSH o puerto serie:** También es posible realizar la configuración descrita en el punto anterior mediante la modificación de los siguientes archivos:
 - `/etc/spt_service/configs/current/hostapd.conf.vars` donde para cada uno de los puertos se deberá indicar:
 - Y: si se desea bloquear de forma manual el tráfico de un puerto.
 - N: si se desea desbloquear de forma manual el tráfico de un puerto.
 - Dirección MAC: si se desea restringir el tráfico de entrada de un puerto solamente a una dirección MAC.
 - 8021x: si se desea utilizar la autenticación SAKÉ sobre el protocolo EAPOL para desbloquear o bloquear el puerto.
 - `/etc/spt_service/configs/current/hostapd.eap.config` para configurar los parámetros de la autenticación SAKÉ.
- Por otra parte, el equipo permite el uso del protocolo *Syslog v3*, el cuál puede ser utilizado para la gestión del sistema y así como mecanismo de obtención de información del sistema, análisis del mismo y mensajes de depuración del sistema. Este protocolo utiliza *Common Event Format (CEF)* para la generación de eventos al que se le incluye una capa de seguridad mediante TLS (Transport Layer Security) versión 1.2 como protocolo criptográfico para proporcionar seguridad a la comunicación mediante el uso de certificados X.509. La versión de openssl se puede comprobar con el comando:
 - ***openssl versión***que se corresponde con la versión *1.0.2k-fips*, teniendo Openssl soporte de TLS 1.2 desde la versión 1.0.1.
- 43. El equipo incluye la capacidad de proporcionar seguridad en el uso del protocolo SNMP, utilizado para intercambiar información de administración y configuración entre los dispositivos de una red determinada. Para cumplir esto, se **debe utilizar SNMPv3**, versión soportada en el equipo. Para configurar el equipo para que solo use esta versión, el usuario debe acceder a través del Web Manager al menú de configuración del protocolo SNMP, pinchando en el botón correspondiente. Al hacerlo, la siguiente ventana aparecerá en pantalla:

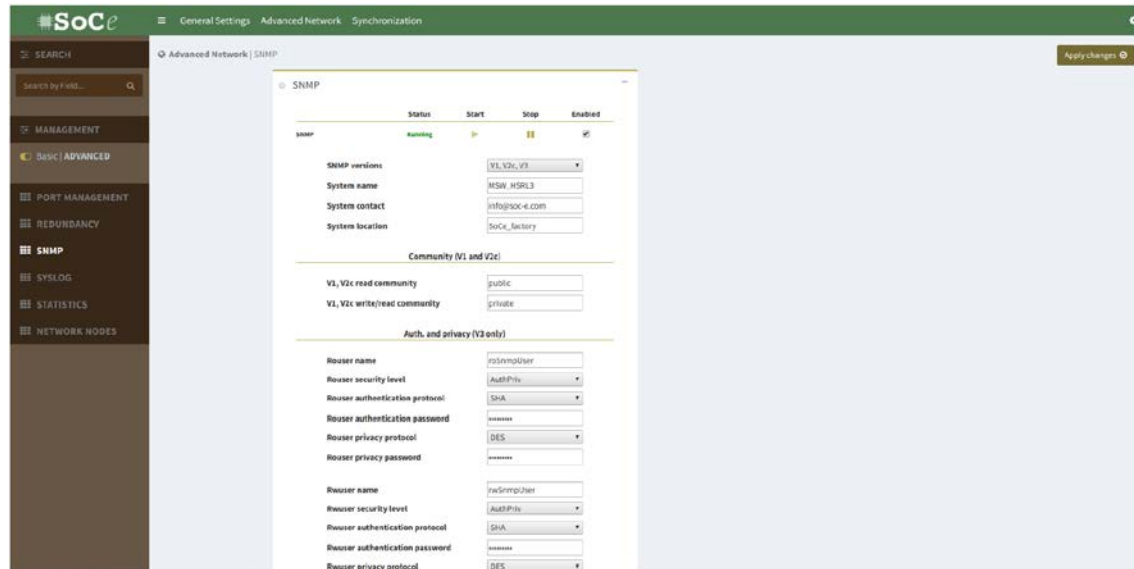


Figura 5. Opciones de configuración del protocolo SNMP

44. Para que el equipo utilice el protocolo SNMPv3, es necesario seleccionar “V3” en el desplegable *SNMP versions*.
45. En particular, el equipo MIL2004-2xHSR-L3 soporta el uso de las siguientes suites de cifrado:
 - Uso de HTTPS/TLS para la administración web.
 - Uso de SSH-2.0-OpenSSH_7.4 curve 25519-sha256 para el acceso de la interfaz SSH.
 - Uso de SHA-512 para llevar a cabo la protección de las contraseñas de usuario de SSH almacenadas.
 - Uso de SHA-256 para llevar a cabo la protección de las contraseñas de usuario de la interfaz web.
46. Los protocolos anteriores se encuentran habilitados por defecto y no es posible su modificación.

5.6 GESTIÓN DE CERTIFICADOS

47. La gestión y actualización de los certificados se realiza a través de la interfaz web del dispositivo (la herramienta *Web Manager*). El administrador deberá generar en un PC un par de clave privada- certificado y firmarlo con una CA de confianza que esté incorporada en los navegadores de los PCs que deseen acceder al equipo. Una vez se disponga de esos archivos, el administrador deberá conectarse a través de la interfaz web, a la sección *Certificates* del menú *Account*. A través de dicha sección, el usuario puede subir al equipo las nuevas claves privadas y públicas que permitirán establecer comunicaciones seguras. Para más información, se puede consultar la sección D5.3 de la guía de configuración “191203 Personality: 2xHSR-L3 19.12”.

48. El equipo hace uso de certificados X.509v3 en el establecimiento de las comunicaciones que realiza. Este tipo de certificados son utilizados por el protocolo HTTPS, cuando se realiza el acceso a la interfaz web de configuración del equipo y cuando se hace uso del protocolo *Syslog* v3 para tener acceso a información de auditoría, información general del sistema, información de análisis realizados y mensajes de depuración.
49. El equipo no incluye ningún mecanismo de validación de certificados, por lo que la gestión de estos deberá realizarse manualmente mediante un procedimiento establecido.

5.7 SERVIDORES DE AUTENTICACIÓN

50. En esta versión del equipo, no se soportan servidores externos de autenticación.

5.8 SINCRONIZACIÓN HORARIA

51. El equipo MIL2004-2xHSR-L3 soporta diferentes mecanismos de sincronización horaria configurables por el usuario a través de la herramienta *Web Manager*, tal y como se muestra en la siguiente imagen:

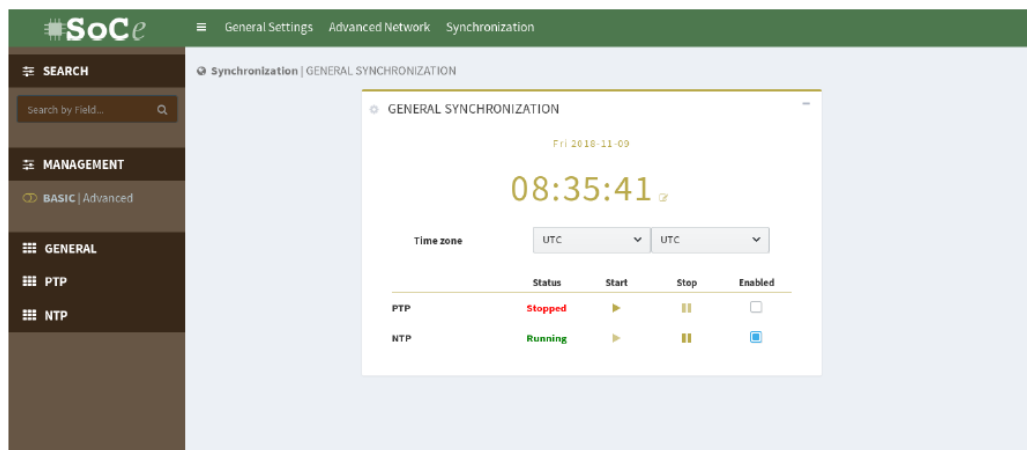


Figura 6. Opciones de sincronización horaria

52. El menú de sincronización que aparece en la imagen anterior permite habilitar o deshabilitar los protocolos de sincronización soportados por el equipo. Estos protocolos son los siguientes:
- *NTP - Network Time Protocol*
 - *IEEE 1588v2 / PTP - Precision Time Protocol*
53. Se recomienda configurar el dispositivo para el uso de servidores NTP/PTP, de forma que todos los dispositivos desplegados puedan llevar a cabo el registro de eventos de forma precisa.

5.9 AUTO-CHEQUEOS

54. El equipo MIL2004-2XHSR-L3 dispone de un mecanismo denominado *Built-in TEst* (BITE). Este mecanismo permite al equipo realizar pruebas a sí mismo con el

objetivo de asegurar un correcto funcionamiento. BITE realiza una lista de pruebas de funcionamiento en los componentes internos del equipo y realiza estas pruebas de tres formas diferentes:

- **Prueba al inicio cada vez que el equipo se inicia.** Esta prueba se realiza de forma automática.
- **Pruebas continuadas.** Cada 5 minutos se lleva a cabo la realización de las pruebas que realiza BITE. Esta prueba también es de carácter automático.
- **Pruebas bajo demanda.** Estas pruebas se realizan de forma manual y por un usuario autorizado. Para realizar una prueba de forma manual hay que ir a través de la interfaz web, a la configuración del equipo y a continuación, utilizar el menú *Tools* -> *BITE* y ejecutar la opción *Exec*.

55. Los resultados de análisis quedan registrados en el equipo y, en caso de detectarse alguna incidencia, se apaga el led correspondiente del frontal del equipo.
56. Para más información acerca del uso y funcionalidades del BITE deberá consultarse el capítulo 9 de la guía de configuración “191203 Personality: 2xHSR-L3 19.12”.

5.10 SNMP

57. El dispositivo soporta el protocolo SNMPv3 para el intercambio de información de administración. Para más información sobre su configuración, ver apartado [5.5 Configuración de protocolo seguros](#).

5.11 ALTA DISPONIBILIDAD

58. El equipo MIL2004-2xHSR-L3 está preparado para ofrecer alta disponibilidad a nivel *hardware* gracias a que su diseño incluye opciones de redundancia en la fuente de alimentación. Para disponer de fuente de alimentación redundante en el equipo, es necesario solicitarla durante el proceso de compra de este.
59. En el plano de comunicaciones, el equipo soporta dos enlaces redundantes que pueden configurarse como HSR (*High-availability Seamless Redundancy*) o PRP (*Parallel Redundancy Protocol*), protocolos de comunicaciones redundantes de alta disponibilidad, que se caracterizan por un tiempo de recuperación de 0 segundos. Para configurar esta funcionalidad, es necesario acceder al menú *Redundancy* disponible en la sección *Advanced Network* del Web Manager del equipo.

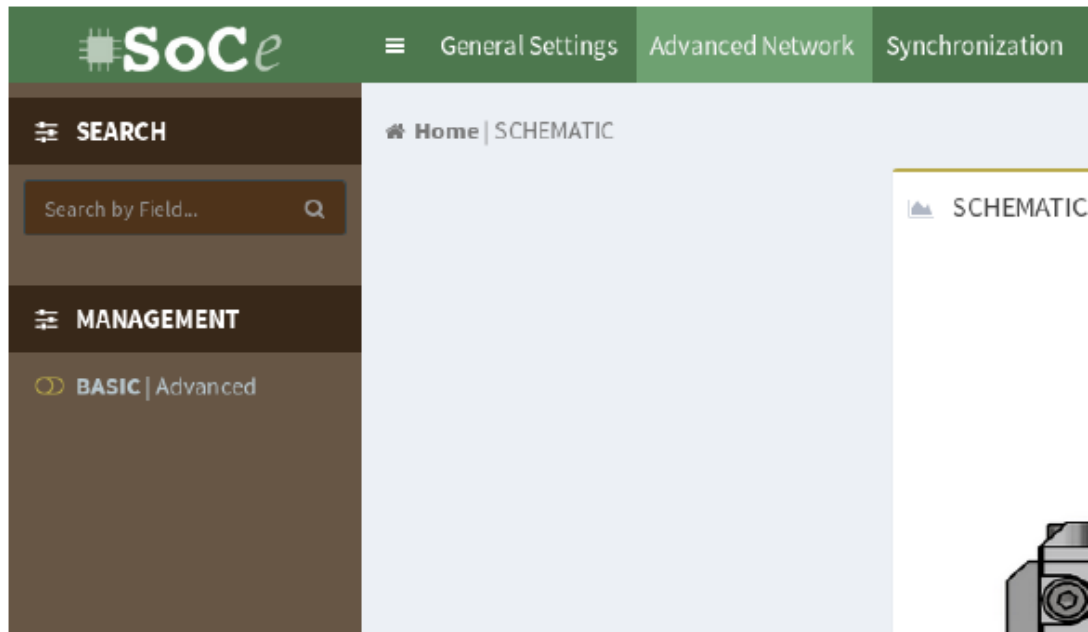


Figura 7. Acceso a la configuración de enlaces redundantes

60. Una vez que se ha accedido a dicho menú, la siguiente ventana aparece en pantalla:

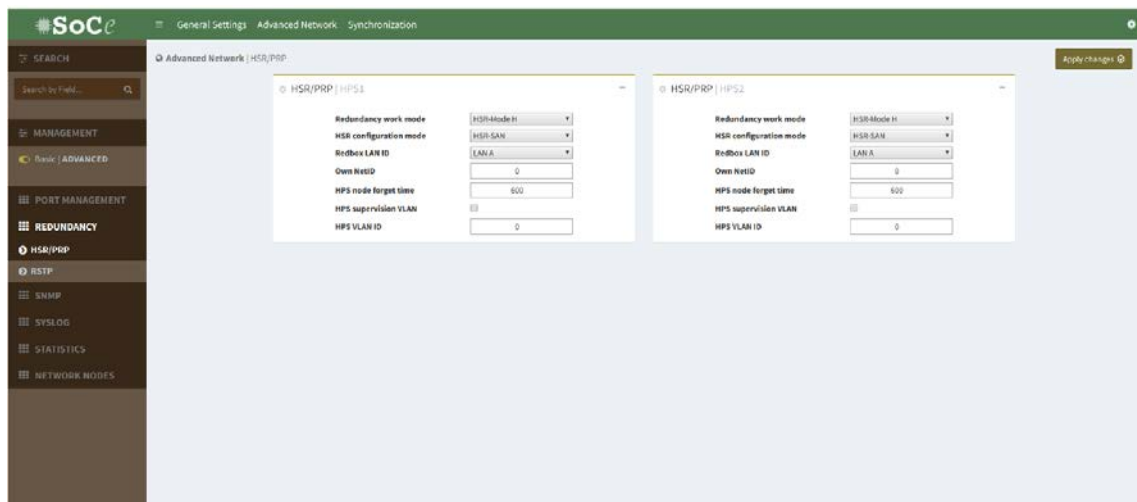


Figura 8. Configuración de enlaces redundantes

61. La redundancia está siempre activada y disponible en el equipo. El menú anterior permite seleccionar entre redundancia HSR o PRP para cada uno de los enlaces redundantes y configurar los parámetros asociados a estos dos protocolos, aunque lo habitual es mantener los parámetros que aparecen por defecto.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

62. El MIL2004-2xHSR-L3 dispone de la capacidad de llevar a cabo un registro de los eventos internos y externos. Esta información de auditoría queda registrada en los

ficheros *auth.log* y *access.log* del propio equipo, que incluyen información sobre los siguientes eventos, entre otros:

- **Monitorización de eventos de sistema**, entre los que se encuentran los eventos de autorización de acceso al sistema. Cualquier intento para obtener acceso al equipo será registrado en estos tipos de eventos. Estos registros son accesibles mediante la interfaz web y la interfaz SSH.
 - **Modificación de la configuración interna al sistema**. Este tipo de eventos son registrados en el sistema y son accesibles mediante la interfaz web y la interfaz SSH del equipo. Este tipo de eventos están relacionados con los servicios de autenticación.
 - **Generación, importación, cambio o eliminación de claves criptográficas**. Cualquier evento relacionado con estas acciones generará un registro de auditoría.
 - **Cambios en las credenciales de usuarios**. Si se produce un cambio de credenciales de usuario, se generará un registro de auditoría que incluya información sobre el evento. Indicar qué eventos se registran y cómo se efectúa el registro. Por ejemplo: fichero de logs de configuración, fichero de logs de sistema, etc.
63. El equipo genera registros de auditoría con la información de fecha, hora, identificación del evento, así como la descripción del propio evento, con el objetivo de proporcionar información precisa de los eventos ocurridos durante el funcionamiento del mismo.
64. A continuación, se incluye una muestra de los registros de auditoría:

```
-- Logs begin at Tue 2019-12-03 09:55:32 CET, end at Tue 2019-12-03 14:35:14 CET. --
Dec 03 09:55:33 localhost.localdomain systemd[1]: Starting Device Configuration Service...
Dec 03 09:55:33 localhost.localdomain spt_service[3601]: [WARNING] SPT Service starting...
Dec 03 09:55:34 MSWHSRL3-70f8e7d00733 systemd[1]: Started Device Configuration Service.
```

Figura 9. Ejemplo de registro de auditoría

5.12.2 ALMACENAMIENTO LOCAL

65. El equipo MIL2004-2xHSR-L3 es capaz de almacenar información de auditoría en sí mismo, la cual es accesible mediante cualquiera de las vías de conexión al propio equipo existentes para el usuario.
66. Para poder visualizar la información almacenada, es necesario acceder al menú *System* disponible en el Web Manager embebido en el equipo, con un usuario administrador. A continuación, se muestra el menú desplegable que da acceso a dicho menú desde la pantalla principal del *Web Manager*:

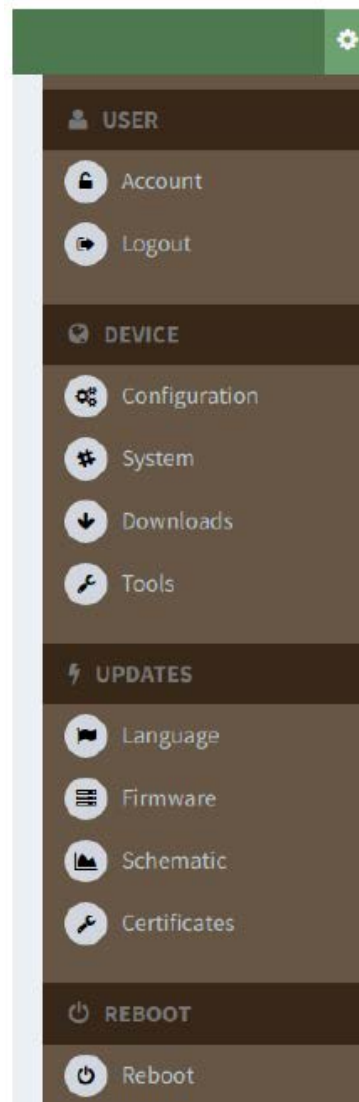


Figura 10. Menú desplegable para acceder a la visualización del almacenamiento local

67. Además, tanto para acceder mediante SSH como mediante puerto serie, se necesitan credenciales. De este modo, se limita el acceso a los registros de auditoría a personal no autorizado. En ningún caso se permite a los usuarios la modificación de registros. Para el caso de borrado de registros, el sistema permite el borrado mediante el uso del comando *delete_audits*.
68. El sistema borrará, cuando sea necesario, los registros más antiguos, ya que dispone de una funcionalidad específica capaz de eliminar registros de auditoría antiguos cuando el espacio de almacenamiento destinado a dicha funcionalidad esté en un 90%.

5.12.3 ALMACENAMIENTO REMOTO

69. El equipo MIL2004-2xHSR-L3 permite la transmisión de la información de auditoría mediante el propio canal de comunicación o interfaz desde la que está siendo visualizada por el usuario.

70. Además, el equipo incluye mecanismos para la utilización de los protocolos Syslogv3 el cual utiliza a su vez el protocolo *Common Event Format (CEF)* para la generación de eventos al que se le incluye una capa de seguridad mediante TLS (*Transport Layer Security*). Para más información, ver apartado [5.5 Configuración de protocolos seguros](#).

5.13 SERVICIOS DE SEGURIDAD

71. El equipo MIL2004-2xHSR-L3 proporciona otros servicios de seguridad:

- *Firewall o Cortafuegos*. Este servicio permite implementar reglas de seguridad a nivel IP. Más información disponible en la web: <https://linux.die.net/man/8/iptables>.
- *Virtual Private Network (VPN)*. Este servicio permite la implementación de redes virtuales privadas. Más información disponible en la web: <https://openvpn.net/community-resources/>.

6 FASE DE OPERACIÓN Y MANTENIMIENTO

72. El equipo MIL2004-2xHSR-L3 dispone de mecanismos para verificar el estado del equipo durante la fase de operación y mantenimiento:

- BITE (*Built-in Test capabilities*) descrito en el [apartado 5.9](#) del presente documento. Este mecanismo permite realizar una autochequeo continuo del estado del equipo.

73. Además, los administradores de seguridad deberán llevar a cabo las siguientes tareas de mantenimiento:

- a) Verificar con regularidad la disponibilidad de nuevas actualizaciones del firmware y aplicar los parches de seguridad correspondientes, para mantener la configuración segura del dispositivo. Ver apartado [6.1 Actualizaciones](#).
- b) Realizar comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado. El código fuente del código activo y su integridad deberá verificarse periódicamente y estará libre de software malicioso.
- c) Mantener los registros de auditoria incluyendo los eventos del sistema. Estos registros estarán protegidos de borrado y modificación no autorizada y solamente el personal de seguridad autorizado podrá acceder a ella. La información de auditoría se guardará en las condiciones establecidas en la normativa de seguridad.
- d) Auditar al menos los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.
- e) Controlar el acceso a la información de auditoria de forma que únicamente el personal de seguridad designado pueda acceder a ella.
- f) Almacenar la información de auditoria en las condiciones establecidas en la normativa de seguridad y por el período establecido.
- g) Deberá realizarse una gestión de contraseñas que estará definida en los procedimientos operativos de seguridad del sistema. Estos contendrán, al menos:
 - El período de caducidad de contraseñas a partir del cual deberán cambiarse. No se recomienda un valor superior a 180 días.
 - El número mínimo de cambios necesarios para que una contraseña pueda repetirse. Se considera deseable que este no sea inferior a 5.
 - El período mínimo durante el cual el administrador no podrá cambiar las contraseñas. Esto impedirá que el administrador la cambie en un breve período de tiempo para volver a su

contraseña original. No deberá permitirse la repetición de, al menos, las 5 últimas contraseñas utilizadas.

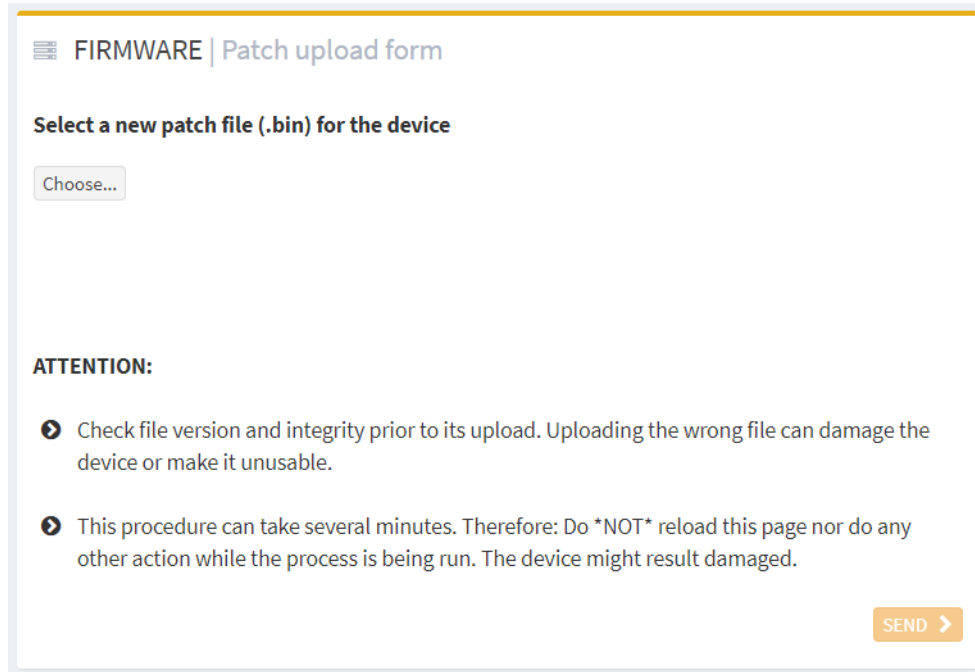
- Longitud mínima de contraseñas. Aunque el dispositivo está configurado por defecto para que esta no contenga menos de 9 caracteres, se considera deseable que la longitud sea menor o igual que 12 caracteres.
- La complejidad de las contraseñas. En general, se consideran contraseñas poco seguras palabras comúnmente utilizadas o cadenas de caracteres consecutivos (Ej.: "1234"). A continuación, se establecen una serie de contraseñas que no debería ser utilizadas:
 - a. Palabras de diccionario.
 - b. Caracteres repetitivos o secuenciales (Ej.: "aaaaaa" o "1234abcd").
 - c. Patrones de teclado (Ej.: 'zaq12wsx' or 'qwertyuiop').
 - d. Nombres propios específicos de contexto, nombres de usuario, nombre del host del sistema, etc.

Además, debe incluirse la restricción en cuanto al número mínimo de letras mayúsculas, minúsculas, dígitos y caracteres especiales que debe contener la contraseña. Se recomienda, que esta contenga un carácter de, al menos, tres (3) de los juegos de estos tipos de caracteres

6.1 ACTUALIZACIONES

74. El equipo MIL2004-2xHSR-L3 dispone de dos (2) mecanismos principales de actualización:

- **Actualización del sistema.** Es posible aplicar un parche de actualización de forma manual en el equipo para actualizar su versión. Para ello, es necesario acceder con un usuario perteneciente al rol de usuarios avanzados en la sección *Firmware->Patch upload from* a través de la interfaz Web. En esta pantalla se muestra el menú donde se puede seleccionar el parche que se desea instalar en el dispositivo.



FIRMWARE | Patch upload form

Select a new patch file (.bin) for the device

Choose...

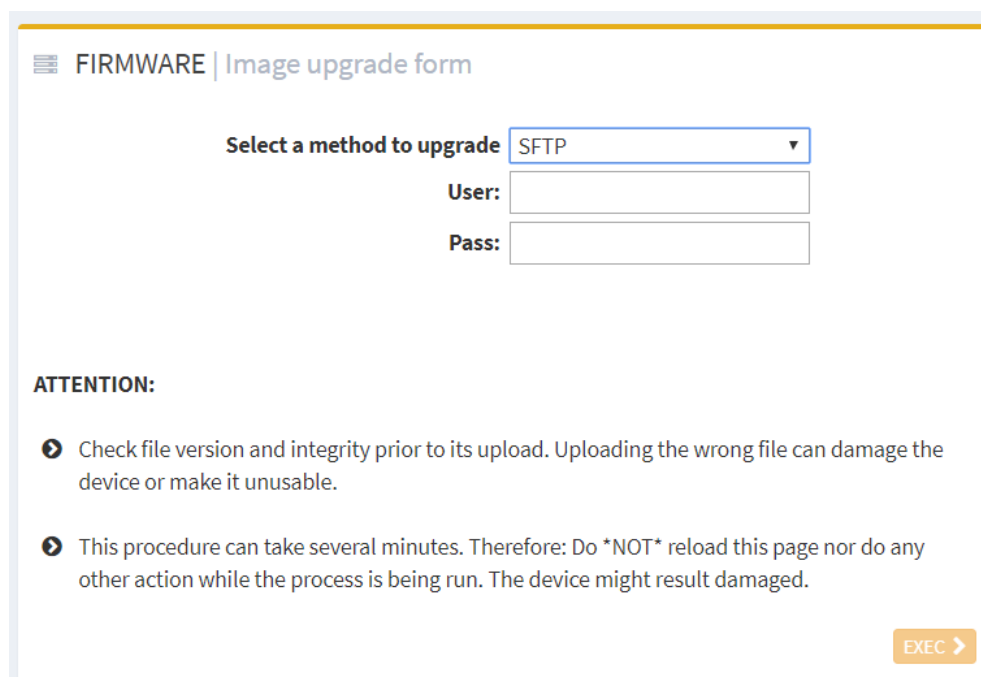
ATTENTION:

- Check file version and integrity prior to its upload. Uploading the wrong file can damage the device or make it unusable.
- This procedure can take several minutes. Therefore: Do ***NOT*** reload this page nor do any other action while the process is being run. The device might result damaged.

SEND >

Figura 11. Menú de selección de parches de seguridad para su instalación en el equipo

- **Actualización de la imagen del sistema.** Esta actualización consiste en una actualización de la imagen completa. Para ello es **necesario** que el equipo tenga conectividad con el servidor soc-e.com. Para realizar esta operación, se debe acceder a través de la aplicación de la interfaz Web al siguiente menú: *Firmware->Image upgrade form* para seleccionar la nueva imagen a aplicar. La carga de la imagen se realiza mediante el uso del protocolo SFTP cuyas credenciales son proporcionadas por el fabricante. La interfaz que visualiza el usuario es la siguiente:



FIRMWARE | Image upgrade form

Select a method to upgrade SFTP ▼

User:

Pass:

ATTENTION:

- Check file version and integrity prior to its upload. Uploading the wrong file can damage the device or make it unusable.
- This procedure can take several minutes. Therefore: Do ***NOT*** reload this page nor do any other action while the process is being run. The device might result damaged.

EXEC >

Figura 12. Menú de configuración para la actualización completa del sistema por SFTP

75. En caso de que el dispositivo forme parte de una red clasificada, podría no ser posible realizar la conexión directa con el servidor soc-e.com, en cuyo caso sería necesario realizar las actualizaciones empleando el mecanismo manual, visto anteriormente, *“Actualización del sistema”*.
76. En ambos casos las actualizaciones se encuentran cifradas y firmadas con la clave privada de SoC-e. El equipo incluye la clave pública de SoC-e y con ella, el proceso de actualización realiza una comprobación de la autenticidad e integridad de la actualización. Además, en el caso de SFTP, el equipo descargará de los servidores de SoC-e un fichero *md5sum.txt* con el propósito de realizar un paso adicional en la verificación de la integridad de los ficheros descargados antes de llevar a cabo la actualización.
77. Además, en los casos en los que el equipo tenga conectividad con el servidor soc-e.com, ofrece la posibilidad de realizar una comprobación manual de la existencia de nuevas versiones disponibles mediante la opción **Click for updates** del menú *Firmware* mencionado. En el caso de que no haya conectividad con soc-e.com desde el equipo, se debe consultar la URL:

https://www.soce.com/checkproductversion.php?product=MSW_HSRL3&version=VERSION

Se debe actualizar ‘VERSION’ por la versión actual (por ejemplo, v19.10) y nos indicará si hay una actualización disponible para esta versión o no.
78. Por último, cabe mencionar que estas actualizaciones solo pueden ser llevadas a cabo por un usuario administrador.

7 CHECKLIST

79. Las recomendaciones de configuración son las siguientes:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto. Inspección del etiquetado y albarán	<input type="checkbox"/>	<input type="checkbox"/>	
CONFIGURACIÓN			
Modificar la contraseña por defecto del <i>Advanced User</i>	<input type="checkbox"/>	<input type="checkbox"/>	
Modificar la contraseña por defecto del <i>Basic User</i>	<input type="checkbox"/>	<input type="checkbox"/>	
CONFIGURACIÓN DE INTERFACES Y PROTOCOLOS SEGUROS			
Deshabilitar puertos no utilizados	<input type="checkbox"/>	<input type="checkbox"/>	
Habilitar control acceso a puerto mediante IEEE 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	
No modificar la configuración de los protocolos seguros habilitados por defecto: HTTPS, SSHv2, SMPv3.	<input type="checkbox"/>	<input type="checkbox"/>	
GESTIÓN DE CERTIFICADOS			
Generación de clave privada – certificado adecuado a la dirección IP del equipo y subida del mismo	<input type="checkbox"/>	<input type="checkbox"/>	
SINCRONIZACIÓN			
Configurar la sincronización del equipo utilizando los protocolos disponibles: NTP o PTP	<input type="checkbox"/>	<input type="checkbox"/>	
ACTUALIZACIONES			
Chequear con regularidad la disponibilidad de nuevas actualizaciones de seguridad. Instalar en caso de que existan.	<input type="checkbox"/>	<input type="checkbox"/>	
SNMP			
Seleccionar y configurar SNMPv3	<input type="checkbox"/>	<input type="checkbox"/>	
ALTA DISPONIBILIDAD			
Conectar diferentes fuentes de alimentación a fuente de alimentación redundante disponible en el equipo	<input type="checkbox"/>	<input type="checkbox"/>	
Habilitar protocolos redundantes HSR/PRP	<input type="checkbox"/>	<input type="checkbox"/>	
OPERACIÓN			
MODO DE OPERACIÓN SEGURO			
Monitorizar los registros de auditoría.	<input type="checkbox"/>	<input type="checkbox"/>	

ACCIONES	SÍ	NO	OBSERVACIONES
Almacenar los registros de auditoría de forma segura y por el tiempo adecuado.	<input type="checkbox"/>	<input type="checkbox"/>	
Chequear con regularidad la disponibilidad de nuevas actualizaciones de seguridad. Instalar en caso de que existan.	<input type="checkbox"/>	<input type="checkbox"/>	
Realizar comprobaciones periódicas de la integridad del HW/SW.	<input type="checkbox"/>	<input type="checkbox"/>	
Ejecutar auto-chequeos del dispositivo (BITE).	<input type="checkbox"/>	<input type="checkbox"/>	

8 REFERENCIAS

CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad, abril 2017.

[1] Guía de configuración *“191203 Personality: 2xHSR-L3 19.12”*

9 ABREVIATURAS

BITE	<i>Built-in Test capabilities</i>
CEF	<i>Common Event Format</i>
CPD	Centro de Procesamiento de Datos
ENS	Esquema Nacional de Seguridad.
HSR	<i>High-availability Seamless Redundancy</i>
IP	<i>Internet Protocol</i>
NTP	<i>Network Time Protocol</i>
PRP	Parallel Redundancy Protocol
PTP	<i>Precise Time Protocol</i>
SNMP	<i>Simple Network Management Protocol</i>
TLS	<i>Transport Layer Security</i>