FREQUENTIS COMSOFT



CO-Aerocivil-AMHS

System Customisation Document (SCD)

2024_730372_AMHS-Upgrade-SCD, 2024-02-12
V1.0

© FREQUENTIS COMSOFT 2024

GRÁFICO DE LA HISTORIA

VERSIÓN	FECHA	CAMBIÓ LOS CAPÍTULOS...	CAUSA DEL CAMBIO	AUTOR
1.0	2024-01-25	-/-	Versión inicial	NSU

Número total de páginas: 59

FREQUENTIS COMSOFT GmbH
Wachhausstr. 5a, 76227 Karlsruhe, Alemania, http://www.frequentis-comsoft.com/
Registro Commercial Mannheim HRB 724029, Director General: Constantin von Reden

Todos los derechos reservados. Ninguna parte del documento puede ser reproducida, procesada o distribuida en cualquier forma o por cualquier medio, electrónico o mecánico, para cualquier propósito, sin el permiso escrito de FREQUENTIS COMSOFT GmbH.

Los nombres de empresas o productos mencionados en este documento pueden estar sujetos a la protección de la ley de marcas comerciales, la ley de marcas o la ley de patentes.

electronically released
2024-06-03

CONTENIDO

1 General 6
1.1 Introducción 6
1.2 Preámbulo 6
1.3 Definiciones y acrónimos 6
1.4 Audiencia prevista 7
1.5 Normas Soportadas del Sistema AFTN/AMHS 7
2 Resumen de la solución 9
2.1 Arquitectura 9
2.2 Vision General del Sistema 10
2.3 Diseño del Sistema 12
2.4 Interfaces 15
2.4.1 Interfaces Seriales 15
2.4.2 Interfaces LAN TCP/IP 16
2.5 Virtualización 16
2.5.1 Host ESXi 16
2.5.2 Almacenamiento 17
2.5.3 Redes Virtuales 17
2.5.4 Máquinas virtuales 19
2.5.5 Dimensionamiento de las Máquinas Virtuales 20
2.5.5.1 Dimesionamiento AIDA-NG VM 20
2.5.5.2 Dimensionamiento CADAS-ATS VM 20
2.5.5.3 Licencia VMWare 20
2.5.5.4 Consideraciones del entorno virtual 21
2.6 Instalación y despliegue del sistema 22
2.6.1 Instalación del sistema 22
2.6.2 Despliegue Operativo 22
2.7 Consideraciones sobre el diseño del sistema 23
3 Componentes del Sistema 24
3.1 AIDA-NG 24
3.1.1 Propiedades y características de AIDA-NG 25
3.1.2 Detalles del AIDA-NG incluidos en el Upgrade 28
3.1.3 Traffic Throughput 30
3.1.4 Colas de mensajes 31
3.2 CADAS-ATS 31
3.2.1 Propiedades y características de CADAS-ATS 32
3.2.2 Los detalles de CADAS-ATS incluidos en la actualización 34
3.2.3 Manejo de mensajes IWXXM 40

3.3 CNMS 40
3.3.1 Introducción 40
3.3.2 Descripción funcional 41
3.3.3 Monitorización de Servidores VM Host 42
3.4 CCMS 42
3.4.1 Generación de kickstart 44
3.5 Sistema Operativo 44
4 Seguridad del Sistema 46
4.1 General 46
4.2 Características de seguridad de aplicaciones / software 46
4.2.1 Seguridad del sistema operativo 46
4.2.2 Seguridad X.400/AMHS 46
5 Red (Network) 47
5.1 Red del Sistema 47
5.2 Red de Servicios 47
5.3 Servicio de acceso remoto 47
5.4 Seguridad de la red 48
6 Hardware 49
6.1 Servidores 49
6.2 Workstations 50
6.3 Display para Supervisión y Workstations de Monitorización 51
6.4 Equipamiento de Red 51
6.5 Receptor GPS/ Servidor horario NTP 52
7 Disponibilidad, fiabilidad y mantenimiento 53
7.1 Clasificación de la gravedad de los fallos 54
8 Anexo A: Artículos suministrados por el cliente (CFI) 55
8.1 Equipo suministrado por el cliente / Usuario Final 55
8.2 Datos e información facilitados por el cliente/Usuario Final 57
8.3 Servicios prestados por el cliente/Usuario Final 59

ILUSTRACIONES

Fig.1: Visión general del sistema 11
Fig.2: GUI de acoplamiento 34
Fig.3: Articulo 18 de un formulario FPL relacionado antes y después de la expansión 35
Fig.4: Formulario de mensaje RQR NOTAM 35
Fig.5: FPL modifica la configuración de los parámetros del sistema 36
Fig.6: Error y advertencia en la configuración del color en la configuración del esquema de colores 37
Fig.7: Diálogo de entrada asistida del tema 10a 38
Fig.8: Visor IWXXM 39
Fig.9: Asesoría de Ciclones Tropicales (TCA) 39

TABLAS

Tab. 1: Documentos del usuario final 6
Tab. 2: Interfaces de red 16
Tab. 3: AIDA-NG Tabla de Características 28
Tab. 4: Carga de CPU medida (cifras de carga de ejemplo) 31
Tab. 5 Propiedades e instalaciones de CADAS-ATS 33
Tab. 6: Especificación del Servidor 50
Tab. 7: Especificación de la Workstation 51
Tab. 8: Especificación del Technical Monitoring Display 51
Tab. 9: Especificación del System LAN Switch 52
Tab. 10: Especificación Reloj GPS 52
Tab. 11: Equipo Suministrado por el Cliente/Usuario Final 56
Tab. 12: Datos e información facilitados por el cliente/Usuario Final 58
Tab. 13: Servicios prestados por el cliente/Usuario Final 59

1 General

1.1 Introducción

Este documento detalla la personalización del sistema para la Suministro, instalación y puesta en servicio de una actualización al sistema AMHS CO-UAEAC-AMHS_System_Upgrade.

Por lo tanto, este SCD es la documentación central del diseño (técnico) del Sistema, ya que describe la disposición general del sistema y el alcance de la entrega del Proyecto y enlaza los demás documentos de diseño. Además, contiene adaptaciones y mejoras específicas para este proyecto.

Si para una referencia no se indica una revisión explícita, se aplica siempre la última revisión.

Tenga en cuenta que no todo el material de referencia enumerado forma parte de cada fase del proyecto, en particular, no todos los documentos referenciados están aún disponibles o adaptados durante la fase de diseño del proyecto.

Ref.- No.	Documento	Document Identifier
[R1]	Especificaciones Tecnicas UAEAC	Formato de Especificaciones Tecnicas
[R2]	Documento de asignación de direcciones	CO-Aerocivil-AMHS, CO-Aerocivil-AMHS_AAD
[R3]	Plan de instalación y documentación del hardware	CO-Aerocivil-AMHS,CO-Aerocivil-AMHS-HWDoc

Tab. 1: Documentos del usuario final

1.2 Preámbulo

Este documento detalla el alcance técnico para la entrega, suministro e instalación de una actualización del sistema de manejo de mensajes aeronáuticos AMHS de Frequentis Comsoft.

1.3 Definiciones y acrónimos

"Cliente" significa Frisson Technologies SAS.

"País" significa Colombia

"FCO" significa Frequentis Comsoft GmbH.

"Proyecto" es el alcance de esta oferta referida por el FCO como AMHS System Upgrade.

“El Sistema” representa todo el equipo y los componentes entregados en este Proyecto.

“Usuario Final” Significa UAEAC (Unidad Administrativa Especial de Aeronáutica Civil)

1.4 Audiencia prevista

Este documento está enfocado a:

- Ingenieros de sistemas y personal técnico,
- Directores de proyecto,
- Los equipos del proyecto, y
- Personal de calidad y seguridad.

1.5 Normas Soportadas del Sistema AFTN/AMHS

La siguiente tabla enumera las normas básicas y las versiones relevantes para las declaraciones de conformidad ante las autoridades reguladoras pertinentes.

Existen numerosas normas y publicaciones industriales adicionales que son pertinentes para la aplicación de la AIDA-NG pero que no figuran en la tabla siguiente, como los documentos a los que hacen referencia las normas básicas. Se enumeran directamente en las secciones de este documento en las que se describen los detalles de aplicación correspondientes.

Documento	Identificador de Documento
ICAO Annex 10, *Aeronautical Telecommunications*/*Volume II: Communication Procedures including those with PANS status*, 7th edition, 2016	ICAO Annex 10
ICAO Annex 11, *Air Traffic Services*, 14th edition, 2016	ICAO Annex 11
ICAO Doc 9880, *Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols*, *Parts I to IV*, 2nd edition, 2018	ICAO Doc 9880
ICAO Doc 9896, *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols*, 2nd edition, 2015	ICAO Doc 9896
ICAO EUR Doc 020, *EUR AMHS Manual*, 14th edition, 2019	ICAO EUR Doc 020
ICAO EUR Doc 021, *ATS Messaging Management Manual*, 14th edition, 2019	ICAO EUR Doc 021
ICAO EUR Doc 022, *EUR AFS Security Guidelines*, 7th edition, 2015	ICAO EUR Doc 022
EUROCONTROL *Specification for the Initial Flight Plan*, EUROCONTROL-SPEC-0101, edition 1.3, 2018	EUROCONTROL-SPEC-0101

Documento	Identificador de Documento
EUROCONTROL *Specification on the Air Traffic Services Message Handling System (AMHS)*, EUROCONTROL-SPEC-0136, edition 2.1, 2018	EUROCONTROL-SPEC-0136

2 Resumen de la solución

La actualización del sistema CO-AMHS se refiere a la entrega, instalación e integración de una actualización de software al sistema existente de AFTN/AMHS en Colombia.

Se entregarán durante el proyecto aplicaciones de software y sistemas operativos actualizados

Para el proyecto, FCO proporcionará una solución que:

- Se instalará en las instalaciones del Cliente CGAC (sistema principal)
- Incluye un producto estándar AMHS basado en el paquete de software central FCO Extended ECG. Este producto está diseñado para operar el conmutador AFTN, la pasarela AFTN/AMHS y el servidor de mensajes ATS dentro de un marco de mensajes común y armonizado, junto con un sistema de gestión unificado.
- Incluye un producto terminal estándar de AMHS UA y AFTN, que se basa en un sistema cliente/servidor y libera al usuario final del ATS de todos los problemas relacionados con el AMHS mediante la máxima integración del AMHS en el sistema general,
- Representa un enfoque innovador, técnicamente superior y rentable.
- Tiene en cuenta las necesidades iniciales de servicios de mensajería ampliados.

2.1 Arquitectura

El sistema propuesto consta de varios subsistemas COTS maduros y de última generación (hardware y software) que juntos forman la solución.

La estrategia de diseño del FCO para contrarrestar la obsolescencia y permitir un mantenimiento cómodo y sin problemas del propio sistema y sus componentes se basa en tres pilares:

1. **Productos COTS** - el Sistema se basa en una serie de software y hardware COTS maduros y de última generación:
    - **AIDA-NG** (Aeronautical Integrated Data Agent – Next Generation), que es el producto avanzado y totalmente integrado del sistema de conmutación de mensajes AFTN/AMHS de Frequentis Comsoft que incluye una pasarela universal para todo tipo de mensajes aeronáuticos.
    - **CADAS-ATS** (Frequentis COMSOFT Aeronautical Data Access System – Air Traffic Services), que es un sistema cliente/servidor que proporciona servicios completos de usuario final de ATS. El sistema soporta la operación de terminales cliente AFTN y terminales cliente Agente de Usuario AMHS en paralelo permitiendo una transición suave de AFTN a AMHS.
    - **CCMS** (Central Configuration Management Suite), que se utiliza para la gestión de la configuración del Sistema.
    - **CNMS** (Freqauentis COMSOFT Network Management System), el sistema de gestión de red que permite supervisar todos los componentes del Sistema.

- Los servidores de aplicaciones están virtualizados. Esto reduce las dependencias del sistema con respecto a los servidores de hardware.
- Los servidores y las estaciones de trabajo son todos productos COTS de HP. Todos los componentes de red son productos COTS CISCO.

2. **Estándares Abiertos.** Siempre que sea posible se utilizan estándares abiertos para las interfaces internas y externas. La adhesión a los estándares tiene la inestimable ventaja de que todos los productos conformes a los estándares pueden conectarse a los productos de otros proveedores que también implementen un estándar determinado.

3. **Modularidad** de la arquitectura y la clara identificación de sus interfaces es una ventaja en sí misma, ya que los diversos componentes pueden combinarse tal como el cliente los necesita, lo que significa aún más flexibilidad. Por razones de redundancia, los componentes críticos están disponibles en múltiples instancias. El usuario no se verá molestado por esta redundancia ya que el sistema es transparente y puede manejar por sí mismo todas las cuestiones relacionadas con la sincronización, el acceso remoto y la administración. En definitiva, un enfoque como éste proporciona un grado máximo de disponibilidad y un diseño claro y comprensible. Además, el diseño modular del sistema facilita considerablemente la formación, el mantenimiento y el apoyo. También proporciona un alto grado de seguridad de la inversión, ya que el cliente tiene la posibilidad de adaptar y rediseñar la configuración en un momento posterior si es necesario.

2.2 Vision General del Sistema

El diseño del sistema que se detalla en este documento trata de la entrega, instalación e integración de un sistema AMHS en el ámbito del proyecto CO-Aerocivil-AMHS para Frisson Technologies SAS.

A petición de Frisson Technologies SAS, FCO proporcionará un sistema AFTN/AMHS con los siguientes componentes

- Servidor de mensajes ATS (MTA), pasarela AMHS/AFTN y conmutador AFTN,
- Aplicación del agente de usuario del AMHS,
- Servicio de directorio de la RTA.

El sistema operativo de tratamiento de mensajes actuará como el nuevo conmutador internacional de mensajes AFTN/AMHS en Colombia para las redes AFTN/AMHS.

La siguiente figura muestra la arquitectura del sistema y ofrece una visión general de alto nivel del sistema CO-Aerocivil-AMHS:

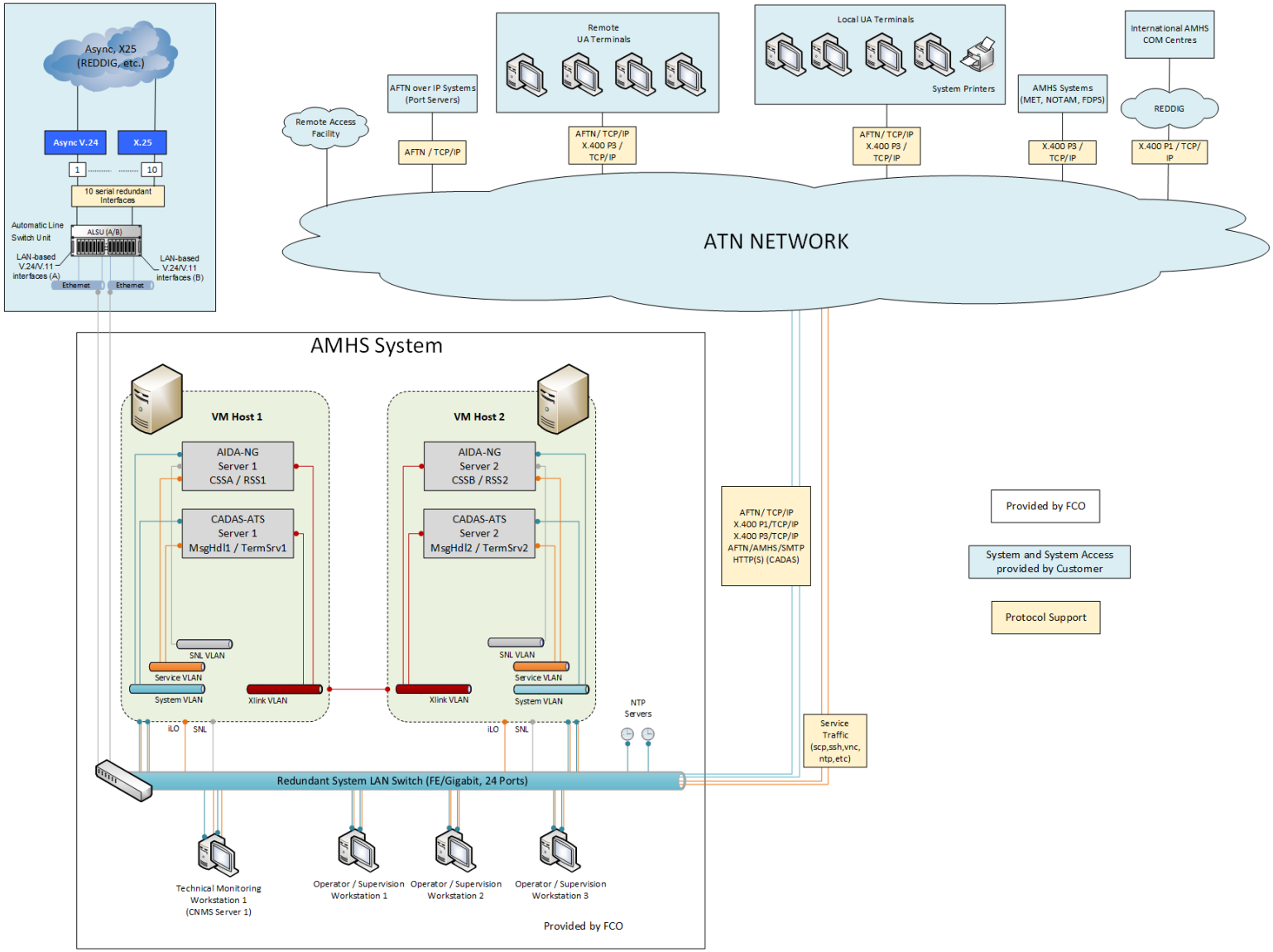


Fig.1: Visión general del sistema

2.3 Diseño del Sistema

El nuevo sistema mantendrá las funciones del sistema actual más las nuevas propias de este proceso de actualización. En lugar de que las aplicaciones ejecuten en servidores físicos, los servicios centrales serán proporcionados por varias plataformas de servidores virtualizados. El sistema operativo (AMHS/AFTN) se instalará en el CGAC en el armario existente junto con el equipo auxiliar para proporcionar la conectividad necesaria.

Varios terminales de operación y control del sistema están distribuidos por los edificios del Usuario final. Todos los componentes están interconectados por la LAN del Sistema, LAN de acceso y LAN SNL.

El Sistema se integrará en la infraestructura LAN del Usuario final respetando las políticas de seguridad vigentes.

Todos los servidores y estaciones de trabajo están instalados con el sistema operativo Linux, los terminales de Usuario (UA) Son compatibles con sistema Windows:

Componente	Descripción
AIDA-NG Para más detalles, véase el capítulo 3.1	Integrado en VM Host 1, 2 como Máquinas Virtuales Conmutador de mensajes / MTA / Pasarela AFTN/AMHS Sistema redundante de tratamiento de mensajes aeronáuticos con Servidor de mensajes ATS (MTA), Pasarela AFTN/AMHS, Conmutador AFTN Admite servicios AMHS ampliados: • File Transfer Body Part • Extensiones de encabezamiento IPM • Seguridad AMHS Gestionado por 4 estaciones de trabajo de operador/supervisión en el sistema.
CADAS-ATS Servers Para más detalles, véase el capítulo 3.2	Integrado en VM Host 1, 2 como Máquinas Virtuales Sistema Terminal Cliente/Servidor AFTN/AMHS UA basado en WEB redundante para la conexión de buzones de usuarios AFTN y AMHS UA y usuarios registrados a través de terminales cliente (HTTP o HTTPS con un certificado correcto).

Componente	Descripción
	Ofrece un esquema de licencias para operar hasta 400 buzones, 100 Grupos AFTN/AMHS y gestión de 500 usuarios registrados. Es capaz de manejar 110 sesiones simultáneas de terminales AFTN/AMHS UA y 5 Sesiones de administracion. La retención de la base de datos para mensajes, registros y eventos sera de hasta 90 días. Admite servicios AMHS ampliados: • Parte del cuerpo de transferencia de archivos • Extensiones de encabezamiento IPM • Seguridad AMHS
CADAS-ATS UA Client Terminals Para más detalles, véase el capítulo 3.2	La aplicación del terminal cliente CADAS-ATS UA está basada en JAVA y, por lo tanto, es completamente independiente del sistema operativo de la estación de trabajo, por ejemplo, Linux o Microsoft Windows. El hardware requerido para el terminal cliente CADAS-ATS UA es una estación de trabajo estándar de última generación basada en PC, independiente de cualquier proveedor o modelo. Se reutilizaran las actuales estaciones de trabajo UA. Estas estaciones esta distribuidas por todo el país, no se considera suministro de UA nuevas, se requiere la instalacion del nuevo Software y el motor actualizado de Java. El terminal cliente puede equiparse con cualquier impresora estándar USB de matriz de puntos o láser en blanco y negro, que puede utilizarse para cualquier fin de impresión, por ejemplo, el filtrado automático y la impresión en línea de mensajes (planes de vuelo, etc.). Las impresoras USB pueden conectarse a través de CUPS, para su uso con diversas aplicaciones. Las impresoras no entran en el ámbito de este projecto. Todos los terminales cliente pueden estar equipados con adaptadores LAN duplicados, que funcionan como interfaz de enlace (compatible con todos los sistemas operativos estándar).
CNMS Server/Client	Se instala la estación de gestión de red Frequentis Comsoft (CNMS) basada en SNMP, que permite supervisar

Componente	Descripción
Para más detalles, véase el capitulo 3.3	completamente no sólo los sistemas AIDA-NG y CADAS-ATS, sino todo el entorno, incluidos todos los componentes con capacidad SNMP, como los componentes de red, los terminales CADAS-ATS remotos, el estado del sistema de copia de seguridad, etc. El CNMS permite crear y configurar individualmente esquemas gráficos y las correspondientes funcionalidades de actualización para la supervisión central y detallada de todo el entorno (basado en SNMP). Frequentis Comsoft entregará el esquema inicial, que se ajusta plenamente a los componentes suministrados. También es posible una función adicional para añadir UAs a la supervision. **CENTROCOM OPS Monitor:** En una (1) estacion de trabajo de Supervisión Técnica que incluyen el mismo ámbito funcional que la estación de trabajo de Operador/Supervisor. Se instalará un servidor CNMS. El Servidor CNMS funcionan independientemente. De este modo se garantiza que haya un sistema de supervisión en funcionamiento en caso de que falle una de las estaciones de trabajo.
Workstation de operador/supervisión	**OPS System:** El sistema está gestionado por tres (4) estaciones de trabajo de operador/supervisión AFTN/AMHS que permiten configurar, operar y supervisar completamente los sistemas AIDA-NG y CADAS-ATS en todos sus aspectos. Las estaciones de trabajo no están dedicadas a funciones especiales; sólo depende del usuario conectado, qué perfil funcional se ofrece. Los roles de usuario son configurables individualmente y en línea. Como se puede acceder a CADAS-ATS y CNMS a través de un navegador web, las estaciones de trabajo de Operador/Supervisión también se pueden utilizar para dichas aplicaciones simultáneamente. Se pueden conectar impresoras USB a las estaciones de trabajo, a través de CUPS, para su uso con varias aplicaciones. Las impresoras no entran en el ámbito de esta propuesta.
LAN redundante de sistema. Para más detalles, véase el capitulo 5	Se instalarán dos (2) conmutadores Fast Ethernet/Gigabit de 48 puertos, que proporcionan VLAN y capacidades de enrutamiento de capa 3.

Componente	Descripción
	La LAN de Sistema Redundante de los sistemas OPS proporciona la conexión de los servidores host VM 1 y 2 con los puestos de operador/supervisor, técnico/mantenimiento. La LAN del Sistema redundante estará conectada a la RED ATN proporcionando acceso a los socios de comunicación remotos basados en IP de la AFTN/AMHS, al acceso remoto y a todos los sistemas basados en IP de la AFTN/AMHS conectados directamente. Redundancia LAN: La redundancia de la LAN del Sistema se basa en el uso de NIC Teaming en servidores virtuales e interfaces LAN bonding en todos los componentes (estaciones de trabajo, terminales, etc). Esto permite cambiar sin problemas de un segmento LAN a otro totalmente transparente para la aplicación y sin pérdida de datos. Para más detalles, véase el capítulo 2.4. of NIC Teaming in virtual servers and LAN bonding interfaces in all components (workstations, terminals, etc). This allows a seamless switch from one LAN segment to the other LAN segment fully transparent to the application and without any loss of data.
NTP Access	Todos los componentes del sistema pueden sincronizarse mediante la señal horaria basada en NTP. Se suministraran dos (2) Servidores de Tiempo Hopf con sus antenas y accesorios.

2.4 Interfaces

El sistema propuesto está conectado principalmente a través de la LAN del Sistema Redundante. Esto proporciona todas las conexiones TCP/IP necesarias a los sistemas locales, a los MTA remotos y a las estaciones de trabajo UA. Véase el capítulo 4.2 para más detalles.

2.4.1 Interfaces Seriales

Conexiones por medio de líneas serie pueden ser posibles a través de los Port Server o el subsistema SNL.

Las líneas serie estarán permanentemente conectadas al sistema Principal. Los transceptores Digiport convierten la línea serie en TCP/IP. El tráfico convertido a TCP/IP puede ser fácilmente reenviado a la capa Ethernet hacia el servidor AIDA-NG activo.

Se reutilizara el SNL existente.

2.4.2 Interfaces LAN TCP/IP

Interfaz LAN	Descripción	Referencia
Máquinas virtuales CO-Aerocivil-AMHS↔ Red ATN	Enlace ascendente del sistema OPS CO-Aerocivil-AMHS a través de la subred de transición L3 enrutada	Arquitectura del Sistema
CO-Aerocivil-AMHS VMs ↔ Red REDDIG II	Enlace ascendente del sistema OPS CO-Aerocivil-AMHS a la red REDDIG II Interfaz X.400/AMHS P1	Arquitectura del Sistema
Líneas locales del AMHS P3	Interfaz X.400/AMHS P3	Arquitectura del Sistema
AFTN líneas locales AFTN sobre TCP/IP	AFTN sobre TCP/IP	Detalles, véase el capítulo AFTN de la CIE

Tab. 2: Interfaces de red

2.5 Virtualización

La evaluación de diferentes soluciones de virtualización por parte de Frequentis Comsoft encontró que VMware era la más adecuada. VMware tiene, con mucho, la mayor cuota de mercado y ESXi se considera el hipervisor más sofisticado y potente del mercado. VMware es el líder indiscutible y es compatible con todos los principales sistemas operativos y plataformas de hardware. Existe soporte oficial para los servidores HP seleccionados y Linux.

La redundancia se considera una gran contribución a la alta disponibilidad. Por lo tanto, los conceptos de redundancia conocidos de la solución AMHS de FCO se mantienen en el entorno virtual. Dos plataformas de un subsistema redundante siempre se asignan a dos sistemas huésped que se implementan en dos hosts virtuales diferentes para eliminar puntos únicos de falla en la capa física.

La virtualización es completamente transparente para los socios de comunicación, ya que continúan accediendo a la aplicación sobre una base IP. El diseño actual de la red se mantiene en la medida de lo posible. Se necesitan direcciones IP adicionales para los hosts de VM.

El mecanismo probado de Kickstart para instalar / recuperar plataformas se mantiene y se aplica a los sistemas invitados (capa virtual). Esto se complementará con documentación sobre un mecanismo para la instalación / recuperación de los sistemas host (capa física).

2.5.1 Host ESXi

El primer paso para configurar la virtualización es la instalación del Hypervisor VMware ESXi. El hipervisor está disponible en VMware, pero también está disponible una versión personalizada de HPE. Esta imagen personalizada garantiza que el hardware tenga un soporte

óptimo y, por lo tanto, sea la opción seleccionada. Para mayor comodidad, un DVD de instalación grabado con la imagen de HPE será parte de la entrega.

La siguiente es una captura de pantalla de la interfaz de usuario de la consola directa de ESXi (DCUI):

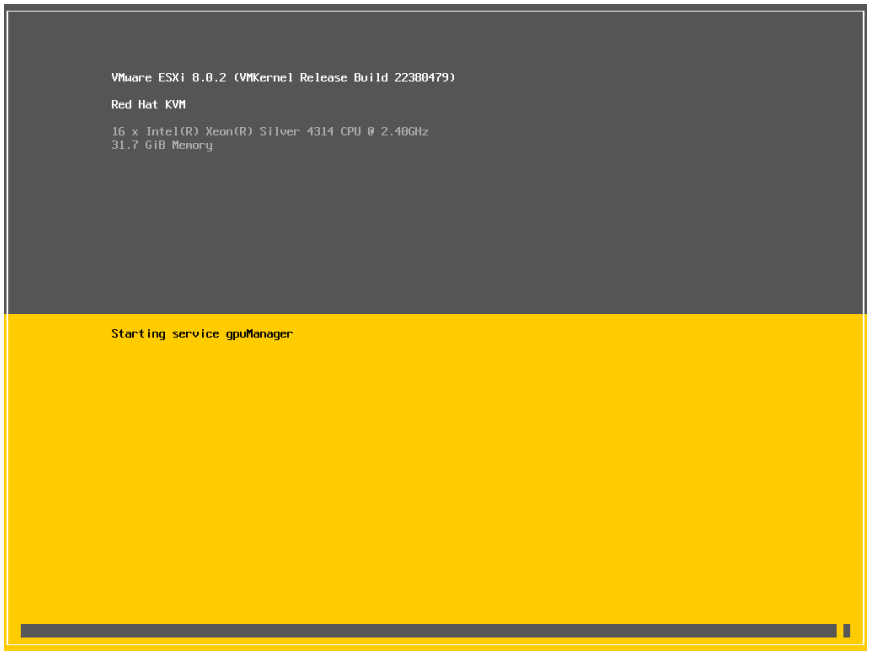


Fig. 1 ESXi – Interfaz de Usuario consola directa

Solo se pueden cambiar algunas configuraciones con DCUI, principalmente configuraciones de red que permiten el acceso a la consola del host HTML de ESXi.

2.5.2 Almacenamiento

El almacenamiento RAID 5 completo disponible se asignará a un almacén de datos VMFS que será compartido por todas las VM.

2.5.3 Redes Virtuales

Hasta 8 NICs físicas están disponibles en cada servidor. Se conectarán dos NIC físicas a la LAN del sistema en los conmutadores CISCO, y dos conectadas como enlace cruzado entre los servidores host. Teaming es utilizado por el host para la redundancia NIC excluyendo el reparto de carga.

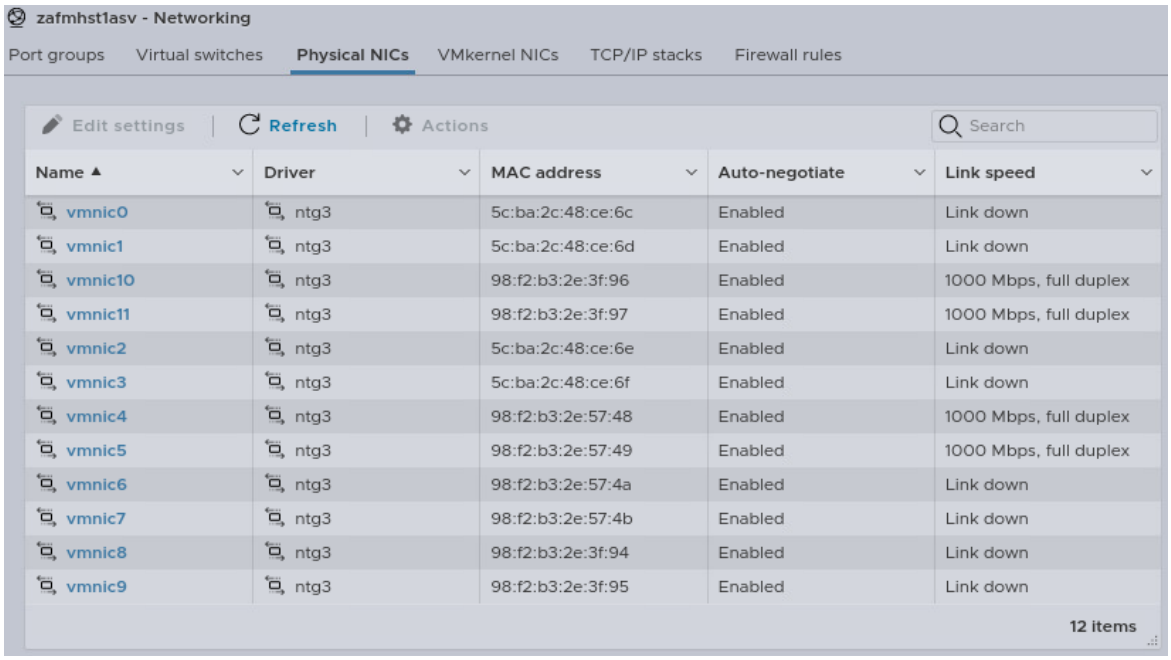


Fig. 2 ESXi host – NICs físicas

Las NIC se asignarán a diferentes conmutadores virtuales, dos para cada LAN interna y externa, si es necesario, uno para el SNL y la LAN de administración en los conmutadores CISCO, y dos para el enlace cruzado del servidor (conectado directamente entre el servidor host). El host utiliza la formación de equipos para la redundancia de NIC, excluyendo la carga compartida.

Se define un grupo de puertos para cada uno de los conmutadores virtuales. Las NIC virtuales de VM se asignarán a estos grupos de puertos.

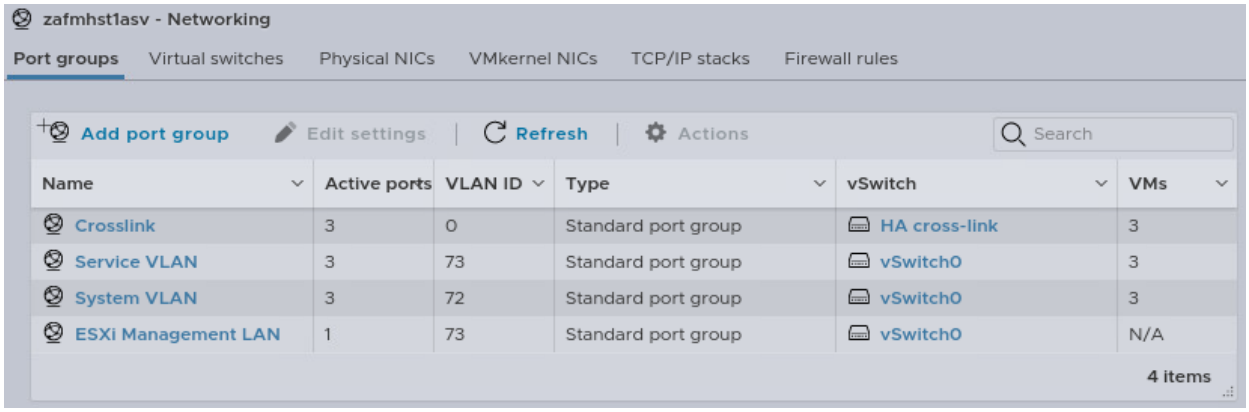


Fig. 3 ESXi - Networking – grupos de puertos

El conmutador virtual de la red de gestión (vSwitch) es el único disponible de forma predeterminada. Inicialmente tiene asignada la NIC física 0 (vmnic0). Esta red solo es visible en el host, no en las VM.

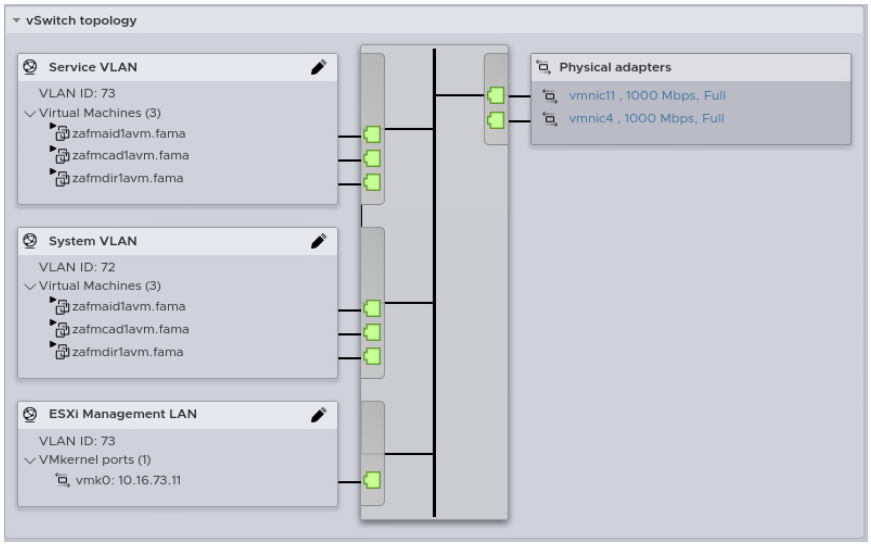


Fig. 4 ESXi – Gestor de redes vSwitch

2.5.4 Máquinas virtuales

Se configurarían Cuatro (4) máquinas virtuales para consolidar el diseño de los sistemas COL-AMHS

Todas las máquinas virtuales se pueden administrar mediante su respectiva consola de host HTML de vSphere. La siguiente captura de pantalla es un ejemplo de la vista principal de administración de VM:

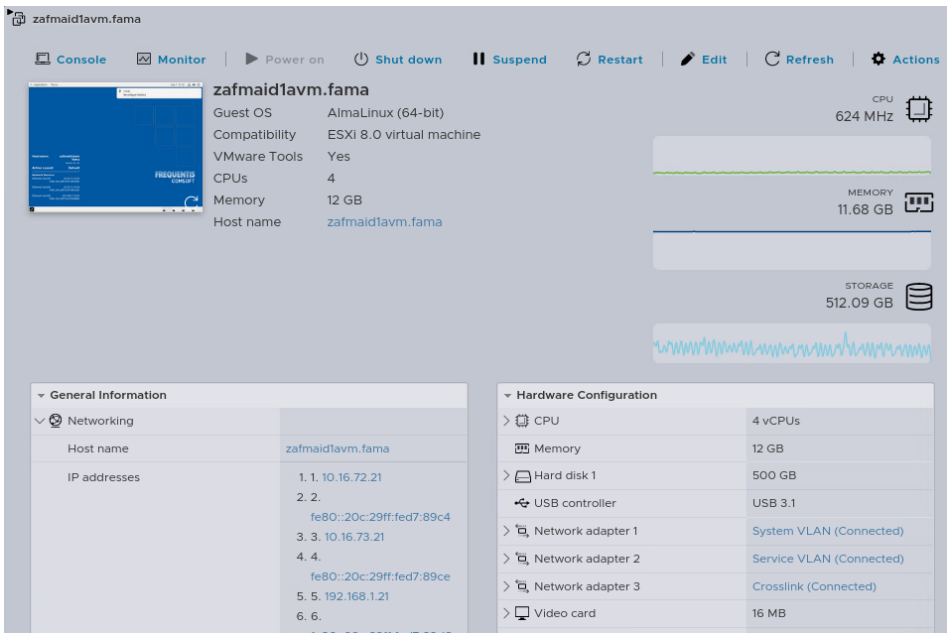


Fig. 5 VM – Vista de gestión

En funcionamiento normal, no debería ser necesario reiniciar las VM manualmente porque están configuradas para iniciarse automáticamente en un orden específico cuando se inicia el host.

Las consolas se pueden abrir en una ventana, pero también es posible cambiar a la vista de pantalla completa. Tenga en cuenta que es posible que algunos atajos no estén disponibles en la consola porque son utilizadas por el sistema operativo de la estación de trabajo de administración. Todas las acciones necesarias seguirán estando disponibles.

Cada máquina virtual en ejecución tiene su propio archivo de registro, vmware.log, almacenado en el volumen VMFS. De forma predeterminada, el archivo de registro se rota cada vez que se enciende la máquina virtual, pero la rotación de archivos es configurable.

2.5.5 Dimensionamiento de las Máquinas Virtuales

Cada uno de los recursos hardware del servidor se dividirá en dos (2) Máquinas Virtuales tal y como se indica en el capítulo 2.2. Las especificaciones propuestas para los servidores se detallan en el capítulo 6.2.

Los recursos hardware de los servidores son suficientes para la correcta operación del Sistema.

2.5.5.1 Dimesionamiento AIDA-NG VM

- Processor: 4 vCPUs
- RAM: 16 GB
- Storage: 500 GB
- Virtual Network Interface: 4
- Virtual DVD drive: 1
- USB controller: 1x USB 2.0

2.5.5.2 Dimensionamiento CADAS-ATS VM

- Processor: 4 vCPUs
- RAM: 16 GB
- Storage: 500 GB
- Virtual Network Interface: 3
- Virtual DVD drive: 1
- USB controller: 1x USB 2.0

2.5.5.3 Licencia VMWare

Para el alcance, los requisitos y las especificaciones de hardware del sistema propuesto, la FCO considera el suministro de la licencia Essential Plus de Broadcom/VMWare ESXi con capacidad de hasta tres servidores físicos en su última versión estable.

2.5.5.4 Consideraciones del entorno virtual

Al ser un sistema misional que ejecuta tareas en tiempo real se deben tener las siguientes consideraciones al momento de configurar el ambiente virtualizado

- Thick provisioning - Aprovisionamiento grueso para el almacenamiento
- Toda la RAM debe estar reservada (o sin sobresuscripción), sin intercambio a disco, sin compresión de memoria, sin balooning de memoria
- En las plataformas CSS/RSS se debe reservar los ciclos de CPU
- Evite vMotion+DRS (migración en vivo) en todas las máquinas virtuales.
- Asegúrese de que los discos virtuales de los RSS y de los manejadores de mensajes se mantengan en distintos almacenes de datos (por ejemplo, utilice reglas antiafines intra-VM)
- No utilices las instantáneas en el entorno operativo.

2.6 Instalación y despliegue del sistema

La coordinación entre Frisson, la UAEAC y Frequentis Comsoft es necesaria para garantizar una instalación sin problemas y la puesta en funcionamiento del sistema. Un posterior plan de transición describirá todas las actividades necesarias para la puesta en servicio del nuevo sistema.

2.6.1 Instalación del sistema

El sistema se instalará en un armario existente en el CGAC.

No se prevé el funcionamiento simultáneo del sistema propuesto y del sistema AMHS-COL original. Durante la instalación y la transición, los dos Sistemas se colocarán uno al lado del otro, no debería haber necesidad de nuevos cables de instalación UTP para la conexión hacia los dispositivos externos (OWP, CNMS, UATs, impresoras) y hacia la red ATN. Para dichas conexiones se implementará una de las siguientes opciones

Migración de la totalidad desde los paneles UTP existentes del armario existente al nuevo equipamiento, migración uno a uno de los cables de instalación existentes.

La instalación del sistema propuesto se realizará mientras el sistema AMHS-COL existente sigue operativo. Se garantizará que la instalación del sistema propuesto no interfiere en modo alguno con el funcionamiento del sistema existente y no causará ningún retraso ni pérdida de mensajes.

Instalación de los relojes GPS reemplazando el HW Actual

2.6.2 Despliegue Operativo

El despliegue del sistema se planificará para garantizar interrupciones mínimas del tráfico operativo AFTN/AMHS, tanto nacional como internacional. Se presentará un plan de transición antes de las actividades in situ y se realizará conjuntamente con el Control de Colombia con lo siguiente como mínimo:

- Concepto de transición

- Concepto de desmantelamiento

- Configuración del sistema

- Descripción de cada paso de la transición que deba realizarse

- Duración y calendario de las fases

- Procedimientos de desmantelamiento

- Impacto en el servicio operativo

En el día "0", el sistema AMHS COL modernizado se transferirá a la explotación en toda su extensión, incluidos todos los canales AFTN/AMHS internacionales y nacionales existentes y todos los terminales UAT. Después de este día, no quedará ningún usuario AFTN/AMHS ni ningún terminal UAT conectado al sistema AMHS original.

2.7 Consideraciones sobre el diseño del sistema

En cuanto al diseño del sistema para esta oferta se asumió lo siguiente:

Algunos componentes de hardware del sistema existente pueden mantenerse, de acuerdo con la viabilidad según el funcionamiento actual.

Los productos y actividades serán instalados y ejecutadas en las instalaciones de CGAC, donde se intervendrá únicamente el CORE del sistema, el suministro, configuración y conexión de las UA Locales, extendidas y remotas serán responsabilidad de la UAEAC a través de su red ATN.

Se reutilizará el gabinete existente así como la infraestructura útil (Energía, Cableado estructurado, Fibras, Port Servers, SNL-2H)

La UAEAC proveerá la infraestructura y configuraciones necesarias para la conexión con los demás centros COM a través de la REDDIG, los sistemas locales ATM, MET, FLOW, etc y las UAS Locales, extendidas y remotas.

3 Componentes del Sistema

Las siguientes secciones describen los productos FCO incluidos en la solución para este Proyecto, cada uno en la versión que ha sido cuidadosamente seleccionada para ajustarse a la aplicación de negocio del Cliente.

Se incluirán en el sistema las últimas versiones de los productos de software. Las funciones de software, como los formularios de mensajes del sistema, cumplen las últimas ediciones de todas las documentaciones estándar pertinentes de la OACI y Eurocontrol disponibles en el momento de la producción del sistema.

3.1 AIDA-NG

AIDA-NG ("Aeronautical Integrated Data Agent - Next Generation") actúa como pasarela multiprotocolo y sistema de retransmisión de mensajes entre varias redes de comunicación. Por lo tanto, proporciona una amplia gama de protocolos de aplicación para la interconexión con los sistemas del usuario final y el mundo exterior. Los interlocutores de comunicación externos se conectan directa o indirectamente a través de otras pasarelas de mensajes o procesadores frontales de mensajes.

Lógicamente, AIDA-NG consta de tres subsistemas:

- **AIDA-NG CSS** (Subsistema central) es el conmutador de mensajes y el componente de pasarela,
- **AIDA-NG RSS** (Subsistema de grabación) es el componente de base de datos, y
- **AIDA-NG OSS** (Subsistema de Operadores) es el subsistema para los puestos de trabajo de los operadores.

AIDA-NG se gestiona mediante una HMI dedicada que se ejecuta en plataformas de hardware independientes (OSS), instaladas en los terminales de gestión del sistema.

En las instalaciones redundantes, las dos instancias AIDA-NG de un sistema están permanentemente activas, es decir, la aplicación AIDA-NG está cargada y activa en ambos servidores y contiene datos idénticos, ya que la aplicación en espera se actualiza permanentemente con los datos de la aplicación operativa. Esto incluye también la duplicación de las bases de datos (registros de tráfico, diarios, estadísticas, eventos, etc.). En consecuencia, una conmutación al servidor en espera es un proceso sencillo, directo y rápido, que suele ejecutarse en menos de cinco segundos, dependiendo de la cantidad de tráfico en cola. Se evitan estrictamente un largo proceso de recuperación del sistema y el alto riesgo de que se dañen los sistemas de archivos compartidos (punto único de fallo), que son los principales puntos débiles de las soluciones de clustering estándar.

El concepto de redundancia garantiza plenamente que todas las conexiones basadas en LAN se restablezcan automáticamente tras la ejecución de la conmutación. AIDA-NG utiliza el comando "ARP gratuito" para el restablecimiento de todas las conexiones basadas en IP.

AIDA-NG puede manejar un número casi ilimitado de usuarios conectados a través de varias conexiones serie o LAN. El número de usuarios no está limitado por el software, sino que sólo depende de los recursos disponibles del sistema.

AIDA-NG registrará los mensajes completos recibidos o transmitidos (este es un ajuste de configuración en CCMS).

AIDA-NG permitir la interconexión de datos a través de canales TCP-IP y serial RS232

Los tiempos de retención de las diferentes bases de datos de AIDA-NG pueden configurarse por separado (utilizando CCMS), por ejemplo, las bases de datos de tráfico pueden configurarse para almacenar 90 días de datos, los eventos pueden almacenarse, por ejemplo, durante 60 días. La configuración del tiempo de retención debe coincidir con el espacio disponible en disco bajo la carga dada.

3.1.1 Propiedades y características de AIDA-NG

A continuación, se enumeran las características presentes en el sistema AMHS-COL. Estas se trasladarán al nuevo sistema. Sin embargo, aún es posible eliminar características que UAEAC Control considere innecesarias, como el convertidor FPL 2012 y las funcionalidades obsoletas.

Durante el proyecto, la documentación del producto se adaptará, de acuerdo, para que coincida exactamente con el conjunto final de características.

Función	Descripción
Mensajes ASYB	Mensajes AFTN sobre el protocolo ASYB (byte asíncrono) según las especificaciones del ITU-T.
Mensajería TCP simple (IPv4)	Mensajes directamente sobre el protocolo TCP/IPv4.
X.400 P1 sobre TP0 TCP (IPv4)	Implementación del protocolo X.400-P1 mediante TP0/TCP/IPv4 según las especificaciones ISO/OSI.
X.400 P3 sobre TP0 TCP (IPv4)	Implementación del protocolo X.400-P3 a través de TCP/IPv4 según las especificaciones ISO/OSI.
Manejo de mensajes de la AFTN	Manejo de mensajes AFTN de acuerdo con las especificaciones de la OACI.
Manejo de mensajes del AMHS	El manejo de los mensajes de AMHS de acuerdo con las especificaciones de la OACI.
Importación de la tabla de búsqueda de AMC	Importación de las tablas de búsqueda de direcciones del AMHS a partir de los archivos proporcionados por el AMC (es decir, registro MD, tabla CAAS, tabla de direcciones de usuario).
La generación de la línea de rumbo del AMHS	Generación configurable del final de la línea de rumbo en el MTCU. (Sin esta característica el sistema se comporta estrictamente conforme a los SARP).
Mapeo de prioridades del AMHS	Mapeo configurable de las prioridades de AFTN/X.400 en la MTCU.

Función	Descripción
	(Sin esta característica el sistema se comporta estrictamente conforme a los SARP).
AMHS EUR Desviaciones	Comportamiento específico de la OACI-EUR (hasta por lo menos EUR AMHS Manual v14.0)
Servicios extendidos del AMHS (DIR)	Implementación del grupo funcional del DIR del servicio ampliado del AMHS según las especificaciones de la OACI.
Servicios ampliados del AMHS (FTBP)	Implementación del grupo funcional FTBP del servicio ampliado del AMHS según las especificaciones de la OACI. Mínimo 2MB
Servicios ampliados del AMHS (IHE)	Implementación del grupo funcional IHE del servicio ampliado del AMHS según las especificaciones de la OACI.
AMHS MTCU IPN y manejo de informes	Posibilidad de cambiar el manejo del MTCU de los IPN y los informes. Sin esta característica, la MTCU intentará convertir los IPN e informes. Nota: La opción de descartar los IPN e informes no se ajusta a los SARP.
Manejo de mensajes X.400	Manejo de mensajes X.400 según las especificaciones ISO/OSI.
La conveniencia de la IRC	Conveniente edición de los CRI (Indicadores de Ruta Colectiva): Búsqueda y sustitución de direcciones en los CRI.
Mapas geográficos	Visualización de la información de diagnóstico (por ejemplo, los estados de conexión de LA) en mapas geográficos.
Barra de herramientas	Barra de herramientas configurable para un rápido acceso a los comandos importantes.
Cálculo del tiempo de tránsito	Comando para calcular los tiempos de tránsito máximo y medio de los mensajes a través del sistema a partir de la base de datos de tráfico.
MEP DEL TCP	Soporte del MEP (Protocolo de Intercambio de Mensajes) para conexiones TCP simples.
TCP simple ack	Soporte de la variante de rack simple para conexiones TCP simples.
Buzones de mensajes	Buzones para enviar y recibir mensajes.
Impresión	Soporte de la impresora.
Sumidero de mensajes	Sumideros de mensajes que pueden ser utilizados como destinos de enrutamiento para el descarte de mensajes.
Control de tráfico	Notificar al operador a través de un evento si no se han recibido mensajes en un período configurable.
Traceo de la cola	Mostrar los mensajes en el diálogo de rastreo de tráfico que aún están pendientes en una cola. Sin este límite, los mensajes en cola no se muestran en la traza, ya que sólo se visualizan las transacciones completas.

Función	Descripción
Repetición con el re-enrutamiento	Reprocesar las tablas de enrutamiento para los mensajes repetidos.
Registro del historial de la cola	Registro de todos los estados de cola de un mensaje.
Archivos	Creación, exportación e importación de archivos de bases de datos con diferente alcance (por ejemplo, archivos de eventos o mensajes para intervalos de tiempo definidos por el usuario o archivos diarios de la base de datos completa).
Desvío basado en la dirección	Preparar y mantener rutas alternativas para los indicadores de ruta de la AFTN en una tabla separada. Cuando estén habilitadas, estas entradas de enrutamiento anularán las entradas de la tabla de enrutamiento normal.
Desvío basado en la dirección con filtro	Posibilidad de especificar filtros para el desvío basado en la dirección.
Configuración de la dirección del AFTN SVC	Especifique las direcciones del AFTN SVC que el sistema procesará automáticamente cuando se active el procesamiento automático del SVC.
Desvío de ruta colectiva	Preparar y mantener listas de expansión alternativas para los indicadores de enrutamiento colectivo de la AFTN en una tabla separada. Cuando estén habilitadas, estas entradas de enrutamiento anularán las entradas de la tabla normal de enrutamiento colectivo.
Modo de desvío de la dirección	Posibilidad de cambiar el modo de operación del desvío basado en direcciones de la AFTN para ser fusionado en la tabla de ruta normal. Sin esta característica la tabla de desviación basada en direcciones tiene prioridad.
Enrutamiento de atributos	Copia de mensajes entrantes. Los mensajes pueden ser seleccionados por los atributos del filtro.
Enrutamiento de atributos para el X.400	Enrutamiento de atributos para el X.400
Enrutamiento de Atributos Exclusivos (suprimir el enrutamiento AD)	Posibilidad de suprimir para las entradas de enrutamiento de atributos seleccionadas el enrutamiento AD que normalmente sigue al enrutamiento de atributos.
Desvío de LA	Desvío de mensajes en base a LA. Los mensajes pueden ser seleccionados por los atributos del filtro.
Entrega paralela en LA	Copia de mensajes salientes en base a LA. Los mensajes pueden ser seleccionados por atributos de filtro.
Manejo de mensajes sobredimensionados	Cortar, segmentar o rechazar los mensajes de gran tamaño. Sin esta característica, los mensajes de la AFTN con una longitud de texto de más de 1800 caracteres son rechazados (3500 para la SITA).

Función	Descripción
Manejo de mensajes de gran tamaño basado en la dirección	Posibilidad de definir el tratamiento de los mensajes de gran tamaño en función de las direcciones de destino.
Enrutamiento de direcciones con múltiples destinos	Posibilidad de especificar más de un destino LA para un indicador de ruta. El mensaje será enrutado a todos los LA de destino dados.
Copia del mensaje X.400	Copia del mensaje X.400
Consultas SNMP	Función simple de gestión de SNMP para supervisar la información de estado de los sistemas externos mediante la consulta de OID individuales.
Agente SNMP	Subagente SNMP específico de la empresa de acuerdo con las especificaciones de la RFC para permitir la supervisión del sistema y los comandos de control seleccionados a través de SNMP.

Tab. 3: AIDA-NG Tabla de Características

3.1.2 Detalles del AIDA-NG incluidos en el Upgrade

Con el objetivo de optimizar la eficiencia y la experiencia del usuario, la actualización del sistema incorporará diversas mejoras. Estas actualizaciones mejoran la estabilidad del sistema y garantizan una robusta operación funcional para los usuarios. A continuación, detallamos las mejoras que se implementarán en esta actualización:

AIDA-NG 64 bit

El AIDA-NG se proporciona ahora de forma nativa como aplicación de 64 bits.

Soporte de EUR AMHS Manual V14.0

El sistema es totalmente compatible con el V14.0 del EUR Doc 020.

- Se proporcionan las estadísticas del AMHS (introducidas con el EUR Doc 020, V10.0).
- Pasa todas las pruebas de conformidad según el Apéndice D actualizado.
- La función de importación del AMC ahora también permite importar las capacidades del usuario del AMHS en los parámetros.

Filtrado de mensajes AFTN de acuerdo con el X.400 LA entrante

Para los mensajes AFTN que han pasado el gateway (pasarela) AFTN/AMHS ahora es posible inspeccionar en qué LA se recibió el mensaje en el X.400 MTA antes de que pasara el gateway.

Esta información puede utilizarse como criterio de filtrado (por ejemplo, para las recuperaciones o las especificaciones del filtro de ruta).

Estructura de menú revisada de la OWP (posición de operador)

La estructura del menú ha sido revisada para una mejor disposición de las entradas del menú.

Mejora de la visualización de los mensajes del X.400

Se ha mejorado la visualización de los mensajes X.400 en las listas (vista de una sola línea y de varias líneas) y en la vista detallada, de manera que la información importante, en particular el cuerpo del texto se muestra en primer lugar.

Visualización configurable de listas de mensajes/eventos

Las columnas en los diálogos de las listas pueden ahora ser ordenadas y redimensionadas para una mejor adaptación de las necesidades individuales.

El contenido de la vista detallada puede mostrarse ahora en un panel de vista previa debajo o al lado del panel de lista en los diálogos de lista.

Toda la disposición (posición, tamaño, disposición de las columnas y uso del panel de vista previa) puede ser almacenada por tipo de diálogo. Para los diálogos de monitoreo de tráfico, la disposición puede ser almacenada por LA individualmente.

La nueva función de filtro de columna permite filtrar rápidamente las entradas en los diálogos de las listas para reducir la visualización en las listas grandes a las entradas con atributos comunes.

Se ha introducido un mecanismo de paginación para manejar listas con un número muy grande de entradas.

Uso de la LMP en la ventana principal

La ventana principal del OSS muestra ahora de forma permanente el uso de los recursos disponibles para las listas de mensajes pendientes.

Filtrado de mensajes AFTN de acuerdo con el X.400 LA entrante

Para los mensajes AFTN que han pasado el gateway AFTN/AMHS ahora es posible inspeccionar en qué LA se recibió el mensaje en el X.400 MTA antes de que pasara el gateway.

Esta información puede utilizarse como criterio de filtrado (por ejemplo, para las recuperaciones o las especificaciones del filtro de ruta).

X.400 Duplicación de mensajes

Utilizando el enrutamiento de atributos o la función de entrega paralela de LA X.400 los mensajes pueden ahora ser duplicados hacia LAs P1 adicionales (otros MTAs), MTCU (gateway AFTN/AMHS) y el buzón del postmaster (agente de usuario interno).

X.400 Copia del mensaje

La función de software AIDA-NG "X.400 Message Copy" descrita en este capítulo se ofrece como una opción y sólo es válida en combinación con la actualización del sistema anterior.

La nueva función de copia X.400 permite seleccionar los mensajes X.400 entrantes a través de filtros y copiarlos a otras direcciones O/R de destino.

Tenga en cuenta que sólo se copiarán los mensajes. Las sondas y los informes no serán copiados por esta función.

Mejora del manejo de las categorías de mensajes

Las categorías de mensajes pueden definirse ahora con identificadores de más de dos caracteres.

Comunicación segura

Apoyo del MEP V2 para la comunicación con CADAS-ATS para asegurar la comunicación contra la corrupción de datos.

3.1.3 Traffic Throughput

Esta sección proporciona información sobre la carga de CPU medida bajo ciertas condiciones de carga de tráfico. Estas pruebas exhaustivas se ejecutaron con una combinación típica de protocolos de comunicación entrantes y salientes, de AMHS a AFTN y viceversa.

La siguiente tabla detalla las diferentes condiciones de carga máxima y las correspondientes cargas de CPU medidas durante las pruebas. Las pruebas se ejecutaron en un sistema AIDA-NG redundante cada servidor (HP Proliant DL380 Gen 10) equipado con una CPU Intel(R) Xeon(R) Silver 4110 a 2,10GHz (ocho núcleos, hyperthreading habilitado) y 16 Gigabytes de RAM.

Tipo de Trafico	In:Out
AFTN	90/sec : 150/sec
AMHS	90/sec: 210/sec
AFTN/AMHS Gateway	150/sec : 150/sec
Total Load (excluding the G/W traffic)	180/sec: 360/sec Corresponds to

Tipo de Trafico	In:Out
	15,552,000/day : 31,104,000/day
Total Message amount	>1000 Msg/sec
Average Message Length	AFTN: 1000 bytes X.400 text: 1500 bytes X.400 FTBP: 3000 bytes
Maximum CPU Load	55 %
Queueing	No
Typical Transit Times (for 99% of all messages)	less than 500 msec

Tab. 4: Carga de CPU medida (cifras de carga de ejemplo)

3.1.4 Colas de mensajes

Los tamaños de las colas de mensajes para AIDA-NG son configurables tanto para mensajes AFTN como X.400/AMHS. La configuración se realiza dentro de la configuración del sistema en CCMS. Por defecto, el tamaño de las colas está fijado en 250.000 mensajes o 250 Megabytes (el límite que se alcance primero) para ambos tipos de mensajes. Esto puede incrementarse dependiendo de la memoria disponible configurada para las Máquinas Virtuales AIDA-NG.

Generalmente, el procesamiento de mensajes no se ve afectado por la cantidad de cola presente en AIDA-NG. Sin embargo, una vez alcanzados los límites máximos configurados, la recepción de mensajes se detendrá. El tamaño de llenado de la cola es indicado por las casillas de cola PML y MTA mostradas en el OSS.

3.2 CADAS-ATS

CADAS-ATS es la aplicación "Sistema de Acceso a Datos Aeronáuticos COMSOFT - Servicios de Tráfico Aéreo" y provee la funcionalidad de Agente de Usuario AMHS (UA).

A nivel lógico, CADAS-ATS consiste en los siguientes subsistemas:

- **El Manejador de Mensajes CADAS-ATS** se conecta al interruptor de mensajes y es responsable de toda la funcionalidad de los mensajes,
- **El Servidor de la Terminal CADAS-ATS** es la aplicación del servidor que gestiona la comunicación con la aplicación de la terminal, y
- **Aplicaciones de la terminal CADAS-ATS**: La UA del AMHS (**aplicación de la terminal del Centro de CADAS-ATS**) para los operadores y la aplicación de la terminal de

configuración de aplicaciones (Terminal de Administradores **de CADAS-ATS**) para los administradores.

CADAS-ATS está construido sobre una arquitectura cliente-servidor escalable y fácilmente ampliable.

La administración del sistema CADAS-ATS se realiza ejecutando la aplicación de la Terminal de Administración de CADAS-ATS, basado en HTTP/HTTPS.

Los gestores de Mensajes CADAS-ATS se conectan al MTA AIDA-NG a través del sistema LAN, utilizando ya sea el protocolo MEP (sabor propietario de AFTN sobre TCP) en caso de mensajes AFTN o el protocolo P3 sobre RFC2126 / TCP/IP (IP versión 4) en caso de mensajes AMHS.

Los gestores de Mensajes de CADAS-ATS siempre dirigirán todos los mensajes a través del MTA, incluso aquellos enviados desde un buzón de CADAS-ATS a otro. De esta manera todos los datos de tráfico se almacenan en la base de datos del MTA. Sin embargo, la base de datos en línea de CADAS-ATS contendrá por lo menos 90 días de tráfico.

Las bases de datos CADAS-ATS también almacenan otros datos además del tráfico: estadísticas, parámetros y eventos del sistema.

Las aplicaciones del servidor CADAS-ATS están duplicadas y distribuidas en los dos servidores del sistema redundante. Las aplicaciones funcionan en paralelo y garantizan, con el apoyo de bases de datos duplicadas, una redundancia del 100% sin pérdida de datos (mensajes, configuraciones, parámetros, etc.). Si uno de los servidores queda fuera de servicio, sus terminales asignados se conmutan automáticamente al servidor restante (transacción sin interrupciones). El proceso de conmutación es completamente transparente para el usuario.

La aplicación de la terminal CADAS-ATS construye un cache local almacenado en el propio disco duro de la PC de la estación de trabajo. En caso de que la caché se dañe, por ejemplo debido a la sustitución del hardware por una pieza de repuesto, la caché se reconstruirá automáticamente.

Todos los estados del sistema, las alarmas y los parámetros cubiertos en la base de datos de CADAS-ATS y demás, se conservan incluso después de reiniciar la aplicación de la terminal del AMHS de cualquier estación terminal del AMHS (PC).

3.2.1 Propiedades y características de CADAS-ATS

La siguiente es una lista de características que se incluirán en CADAS-ATS.

En el curso del proyecto, la documentación del producto será, por supuesto, personalizada para que coincida exactamente con el conjunto de características disponibles.

Función	Descripción
AFTN	Envío y recepción de mensajes de la AFTN.
BÁSICO DE AMHS	Envío y recepción de mensajes AMHS apoyando el Servicio de Mensajes Básicos de ATS.

Función	Descripción
AMHS IHE	Apoyo a la generación y recepción de mensajes en con las extensiones de encabezamiento IPM [IHE].
DIRECTORIO AMHS	Soporta el uso del Directorio para acceder al Directorio de la ATN X.500 para buscar usuarios y determinar sus capacidades, por ejemplo, si soportan IHE o FTBP para la conversión de direcciones AFTN - AMHS [DIR].
AMHS FTBP	Apoya el uso de File Transfer Bodyparts, para manejar los archivos adjuntos de los mensajes [FTBP]. Mínimo 2MB
Carpeta	Manejo de la carpeta de mensajes.
Formularios FPL	Formularios de mensajes relacionados con FPL y FPL: FPL, SLP, DEP, ARR, DLA, CNL, CHG, ALR, RCF, CPL, EST, CDN, ACP, LAM, RQP, RQS
FPL 2012	Apoyo a la Enmienda 1 a la Decimoquinta Edición del PANS-ATM (Doc 4444) que entra en vigor el 15 de noviembre de 2012. Se puede configurar una lista de emisores capaces de enviar/recibir según el nuevo formato.
Ruta VFR relajada	El análisis de las partes de VFR de una ruta de FPL y los mensajes relacionados se hace de manera menos estricta. Esto puede ser necesario si los procedimientos locales de los vuelos de helicópteros se utilizan para este tipo de rutas. ¡Por favor, tomar en cuenta que estas rutas no se ajustan a la DOC4444!
Formularios NTM	Formularios para mensajes relacionados con NOTAM, SNOWTAM, ASHTAM y NOTAM.
Formularios MET	Formularios de entrada para los mensajes de METEO: METAR, SPECI, AIRMET, SIGMET, TAF, RQM, Genérico
Estadística	Generación de estadísticas.
Rutas preferentes	Apoyo a las rutas preferenciales.
SNMP	Permite que el sistema CADAS sea monitoreado usando SNMP.
Impresión automática	Soporte de la función de impresión automática de mensajes.
Buzones de correo	Manejo de mensajes y buzones. (envío de mensajes)
Mensajes	Manejo de mensajes y buzones. (control de buzones, recepción de mensajes, etc.)

Tab. 5 Propiedades e instalaciones de CADAS-ATS

3.2.2 Los detalles de CADAS-ATS incluidos en la actualización

Soporte técnico de Java 11

Se requiere la versión 11 de Java para los componentes que se ejecutan en el servidor, así como para las aplicaciones de la terminal del cliente (por ejemplo, la terminal central, la terminal de administración, ...).

Debido a que el marco de trabajo de Java WebStart ya no está disponible en Oracle Java, se utiliza en su lugar la biblioteca del marco de trabajo Update4J. El mecanismo de descarga e inicio de la aplicación es como el WebStart. Eso significa que la aplicación terminal se descarga y se almacena en caché localmente.

Soporte nativo de 64 bits

Tanto el servidor terminal como el manejador de mensajes en CADAS-ATS se proporcionan ahora de forma nativa como aplicación de 64 bits.

GUI de acoplamiento

La interfaz gráfica de usuario ha sido mejorada con una función de acoplamiento. Ahora es posible abrir varias vistas en paralelo y organizar la GUI dependiendo del trabajo que se necesite. Hasta cinco ajustes diferentes se gestionan automáticamente y se pueden cambiar.

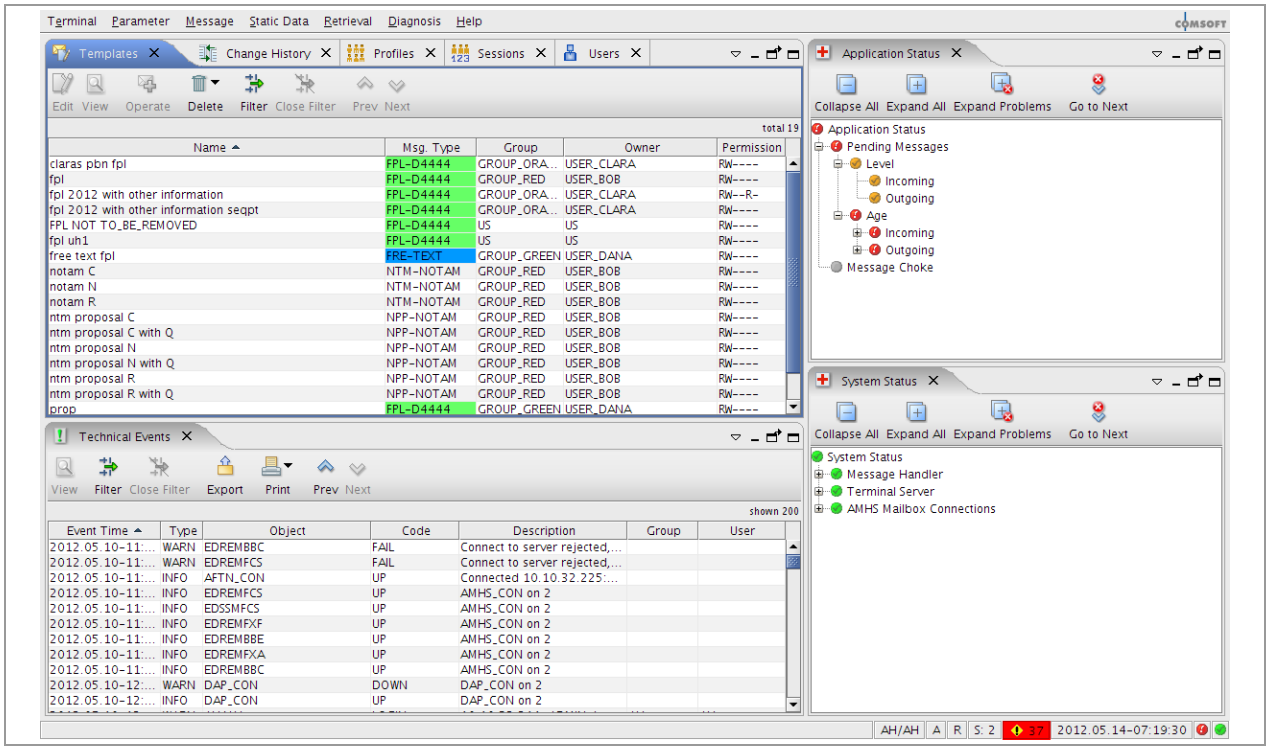


Fig.2: GUI de acoplamiento

Artículo 18 completo para los mensajes relacionados con el FPL

Con la actualización del formato FPL de la OACI para 2012, el FPL relacionado también tuvo la posibilidad de introducir los datos del artículo 18. Esto está destinado a la entrada de información de la fecha de vuelo (DOF). Por lo tanto, los formularios de mensajes relacionados con FPL proporcionan un campo de entrada sólo para la fecha de vuelo. Cuando sea necesario en algunos casos de uso proporcionar más datos, ahora es posible expandir este campo de entrada a un campo de entrada completo del ítem 18 también para los mensajes relacionados.

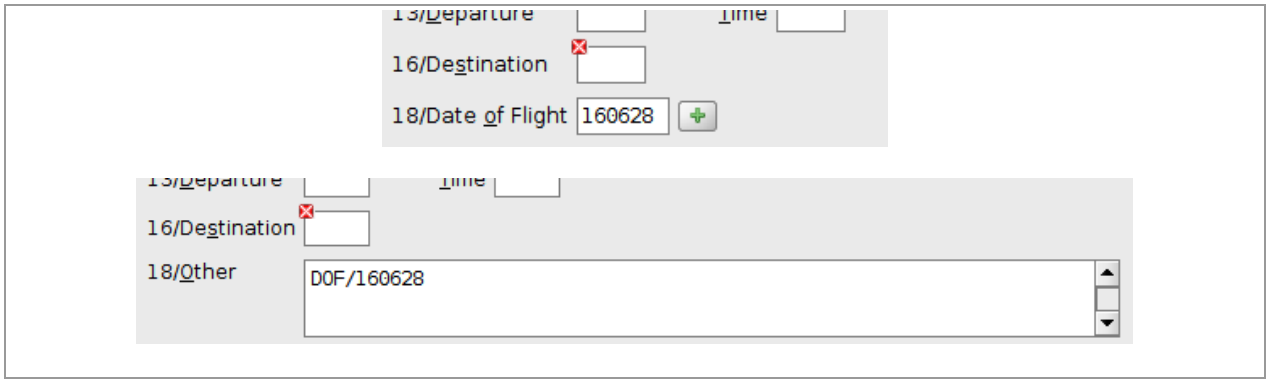


Fig.3: Articulo 18 de un formulario FPL relacionado antes y después de la expansión

Mejora en el soporte para los mensajes RQR

Ahora hay tipos de mensajes adicionales para el RQR notam, el RQR notam original, el RQR ashtam y la lista de control del RQR. Se han mejorado/añadido los formularios de mensajes para esos tipos de mensajes.

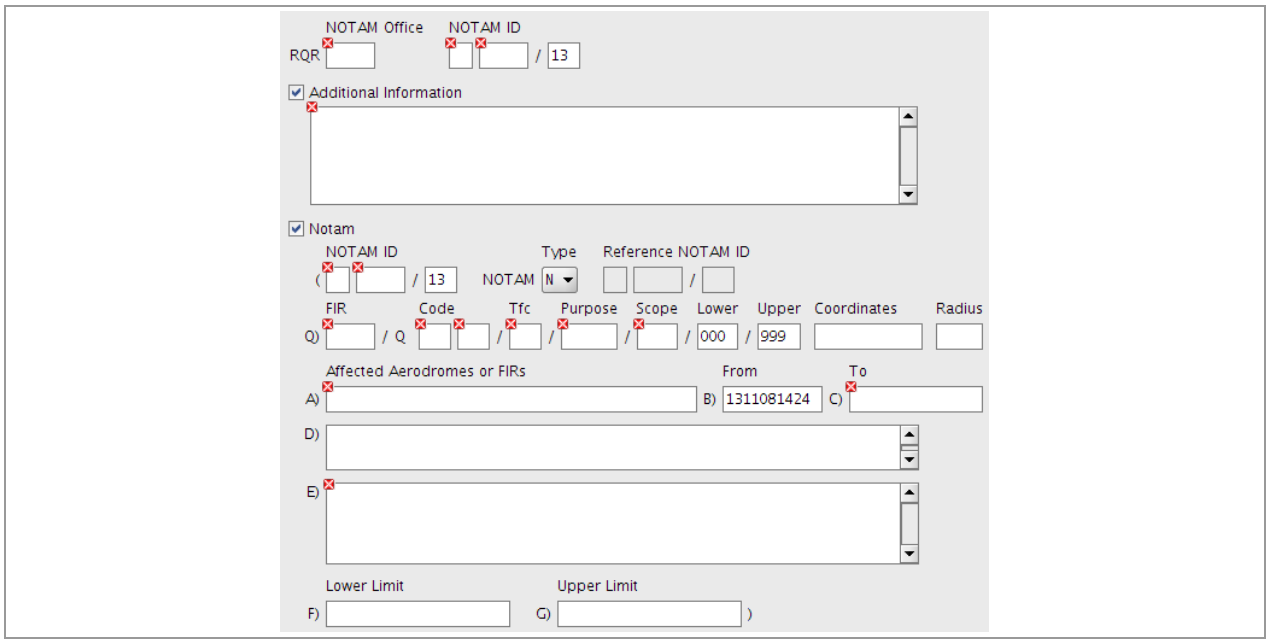


Fig.4: Formulario de mensaje RQR NOTAM

Mejora en función de modificación del FPL

La función de modificación de la FPL permite al usuario actualizar un plan de vuelo. El sistema crea automáticamente los mensajes necesarios para distribuir la información actualizada. El software antiguo creaba un mensaje DLA si sólo se modificaba el punto 13b y creaba un mensaje CHG en caso contrario. El nuevo software también enviará un mensaje CNL para el plan de vuelo antiguo y creará un nuevo mensaje FPL. A través de los parámetros del sistema se puede establecer qué mensaje debe crearse si se modifican ciertos elementos de un plan de vuelo.

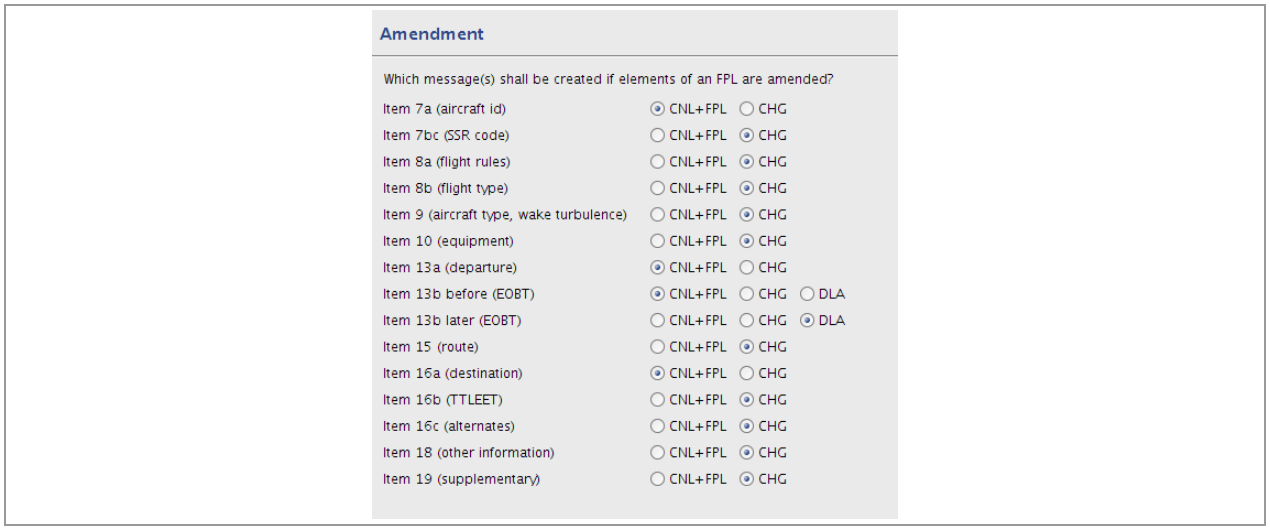


Fig.5: FPL modifica la configuración de los parámetros del sistema

Color configurable para el error y la advertencia a través del esquema de colores

Aunque era posible establecer esquemas de colores, el color que se usaba para los errores y advertencias se codificaba en rojo y naranja. Ahora es posible configurar el color utilizado para indicar errores y advertencias en la configuración de la combinación de colores.

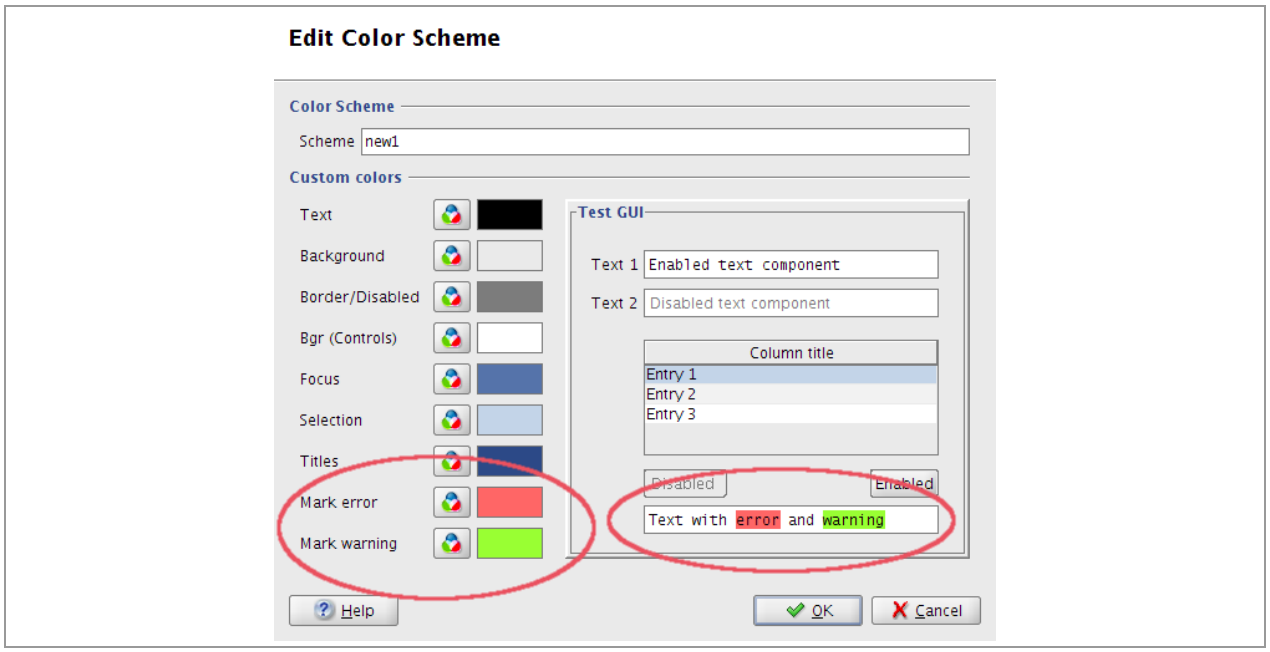


Fig.6: Error y advertencia en la configuración del color en la configuración del esquema de colores

Mejoras en el rendimiento de la carpeta de mensajes

El manejo de datos de la carpeta de mensajes en el lado del servidor, así como en el lado del cliente ha sido mejorado. Se ha reducido la cantidad de datos que se descargan al cliente cuando se actualiza la vista de la carpeta.

Asistencia en materia de insumos para los temas 10a/b y 18

Un diálogo de ayuda para la introducción de datos ayuda a los usuarios a rellenar el artículo 10a/b (equipo) y el artículo 18 (otra información) de los FPL y los mensajes conexos. En lugar de sólo letras, el usuario puede seleccionar el equipo a partir de un texto descriptivo. La ayuda de entrada del ítem 18 ayuda a la entrada de elementos válidos del ítem 18.

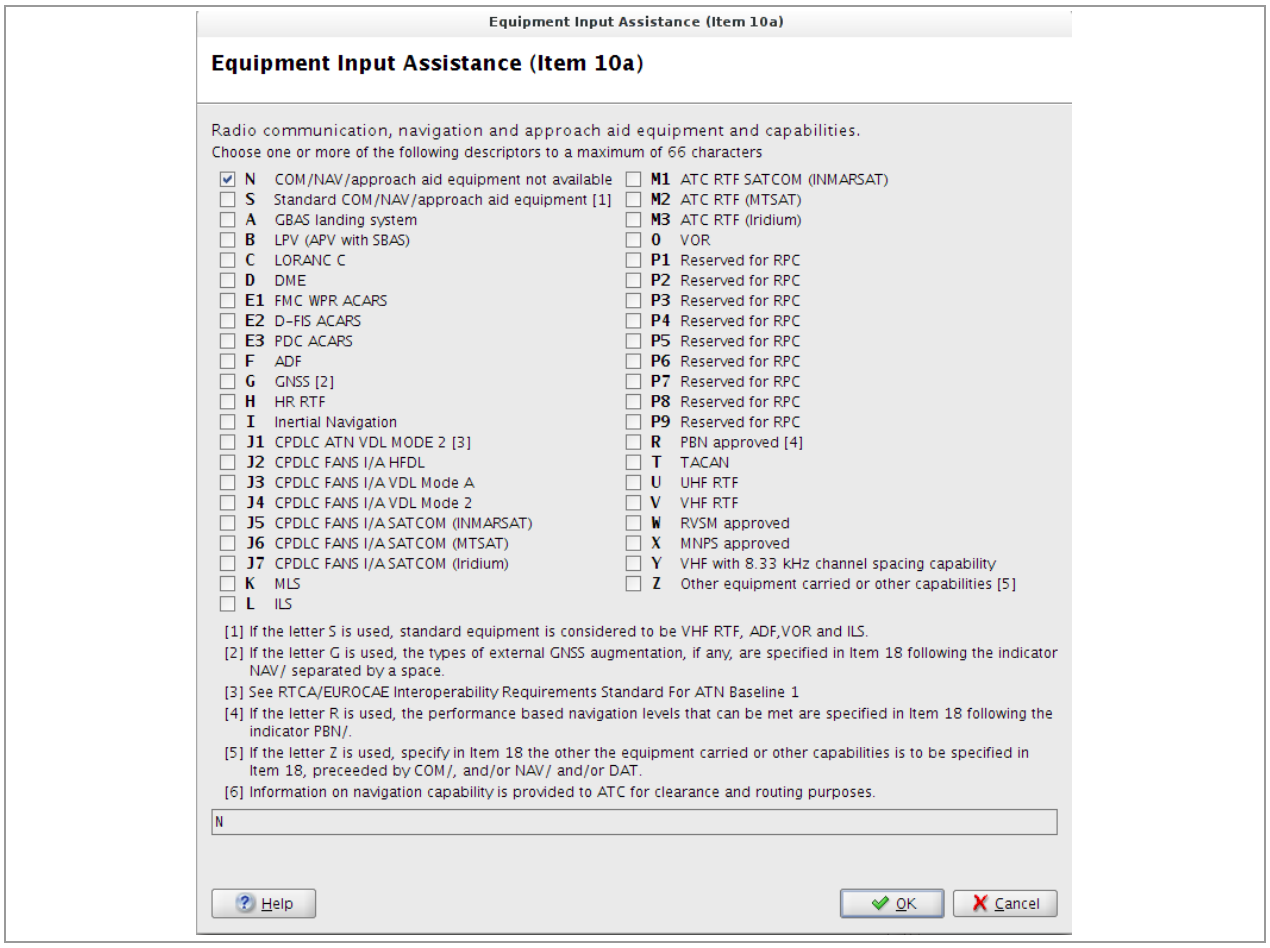


Fig.7: Diálogo de entrada asistida del tema 10a

Visor IWXXM

El IWXXM (Modelo de Intercambio de Información Meteorológica de la OACI) es un formato para la presentación de información meteorológica en XML/GML. Estos datos se envían y reciben a través de los archivos adjuntos del AMHS. El sistema proporciona ahora un visor IWXXM para mostrar los datos IWXXM. Los datos pueden ser inspeccionados como texto XML en bruto, texto XML formateado, árbol XML y árbol especial IWXXM.

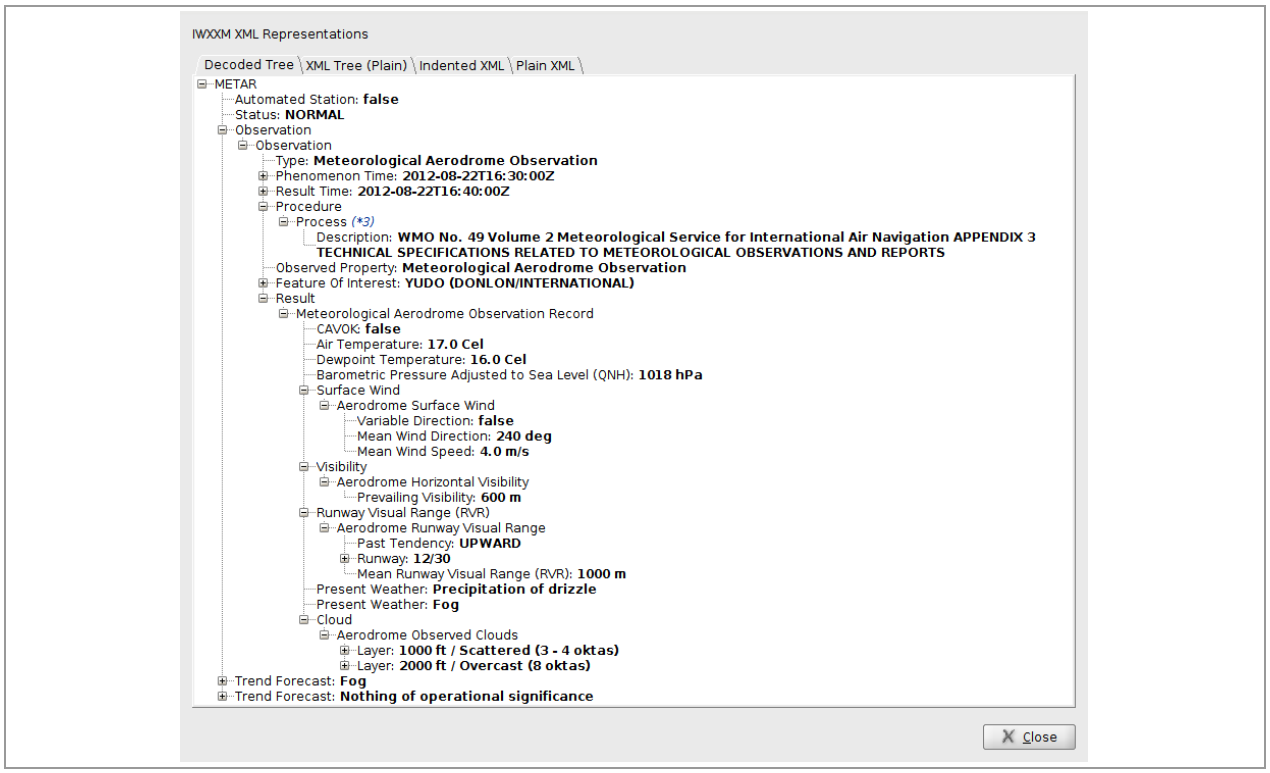


Fig.8: Visor IWXXM

También está disponible un nuevo formulario de mensajes para el tipo de mensaje RQX (solicitud de IWXXM).

El visor del IWXXM (Modelo de Intercambio de Información Meteorológica de la OACI) es compatible con las versiones 2.0 (08.2016) y 2.1 (03.2017) del formato IWXXM con los tipos de mensajes adicionales AIRMET, VAA (Asesoría de Cenizas Volcánicas) y TCA (Asesoría de Ciclones Tropicales).

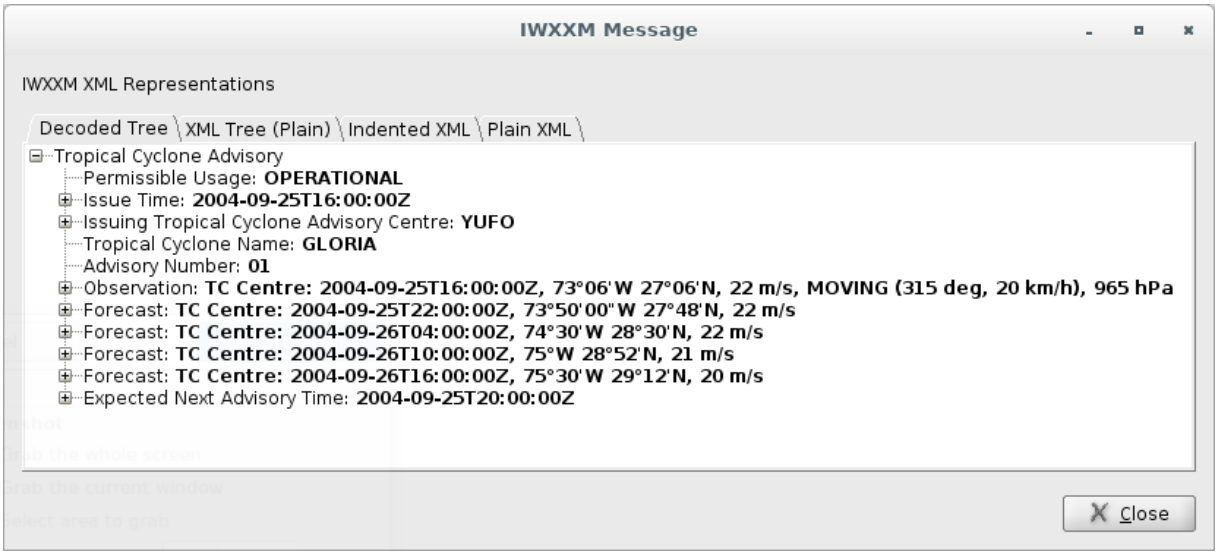


Fig.9: Asesoría de Ciclones Tropicales (TCA)

3.2.3 Manejo de mensajes IWXXM

Dentro del documento *IWXXM Upgrade Technical Description*, se encuentra una descripción detallada de los posibles escenarios y su funcionamiento con la utilidad IWXXM.

3.3 CNMS

3.3.1 Introducción

El CNMS ("COMSOFT Network Management System") se utilizará para la supervisión de todos los componentes de software y hardware.

CNMS se basa en Nagios, una solución probada y ampliamente utilizada para la supervisión de sistemas y redes.

La interfaz de usuario de CNMS está basada en un navegador y se puede acceder a ella desde cualquier punto de una red conectada (es decir, desde cualquier puesto de trabajo).

CNMS es capaz de enviar Traps SNMP para alarmas configurables. Normalmente, las alarmas se configuran para eventos críticos, por ejemplo, un fallo del hardware del servidor o de un componente de software o mal funcionamiento de los componentes.

Este concepto garantiza una gran extensibilidad mediante el uso de interfaces de sistema abiertas. CNMS está preconfigurado para admitir muchos componentes de red y hardware COTS, así como aplicaciones de software de FCO, como AIDA-NG y CADAS-ATS. Una interfaz de software específica permite conectar aplicaciones y secuencias de comandos específicas para mejorar aún más la rica funcionalidad.

De acuerdo con los requisitos de un sistema fiable y flexible, se aplican los siguientes atributos generales del sistema:

- **Basada en código abierto:** La aplicación se basa en gran medida en software de código abierto.
- **Estándar de facto:** El núcleo de CNMS se basa en el paquete de software Nagios, el estándar de facto de código abierto para la monitorización de redes. Ha demostrado ser una solución fiable para la monitorización de redes en muchas grandes empresas.
- **Acceso basado en web:** Los administradores y operadores pueden acceder a todas las funciones esenciales del software a través de un navegador web estándar.
- **Basado en SNMP:** Para la supervisión y el control, CNMS utiliza el sencillo protocolo de gestión de redes SNMP. Es compatible con las versiones 1, 2c y 3 de SNMP.
- **Extensibilidad:** El potente mecanismo de plugins y la sencilla API de Nagios permiten adaptar y ampliar el software a las necesidades del cliente. Se pueden utilizar plug-ins para implementar métodos y protocolos de supervisión propios (por ejemplo, SNMP, HTTP, JMX, WMI, etc.).

3.3.2 Descripción funcional

La aplicación CNMS se utilizará para la supervisión central de todos los componentes del sistema. La supervisión puede realizarse para módulos de hardware y software utilizando SNMP v1, v2, v3.

La supervisión de todos los componentes puede realizarse mediante SNMP, PING, protocolos basados en TCP y la evaluación de los archivos de registro enviados a CNMS. Además del sondeo SNMP, CNMS puede procesar traps SNMP. Todas las trampas recibidas se almacenan en una base de datos.

El sistema se entregará con CNMS preconfigurado para supervisar todos los componentes esenciales. Estos pueden incluir los siguientes: puertos LAN físicos, unidades físicas, fuentes de alimentación, estado del sensor de temperatura, estado del ventilador, estado de la batería de la caché RAID, carga de la CPU, uso del disco y de la memoria (en su caso, estado del software mediante consulta MIB del software).

Los sitios remotos (agentes de usuario y routers) se representan en los mapas del sistema CNMS mediante un icono de estado resumido. El icono de resumen muestra un estado de ADVERTENCIA si al menos un agente de usuario del sitio no está bien (por ejemplo, una interfaz caída o alta carga de CPU). Si uno o más agentes de usuario del sitio están caídos, se muestra un estado CRÍTICO. El cliente puede decidir qué sitios remotos y agentes de usuario serán presentados y supervisados por CNMS.

CNMS es capaz de ejecutar manejadores de eventos. Los manejadores de eventos son comandos opcionales que se ejecutan cada vez que ocurre un cambio en el estado del host o del servicio. Un uso obvio para los manejadores de eventos (especialmente con servicios) es la capacidad de arreglar problemas proactivamente antes de que alguien sea notificado. Otro uso potencial de los manejadores de eventos podría ser registrar eventos de servicio o host en una base de datos externa. Los manejadores de eventos también pueden ser invocados al recibir trampas SNMP. Otra tarea de los manejadores de eventos es filtrar eventos generados a partir de syslogs.

Los eventos del sistema pueden configurarse para alertar al administrador mediante alarma acústica y visual, así como por correo electrónico (requisito previo servidor de correo electrónico corporativo).

CNMS proporciona notificaciones emergentes en el escritorio de las plataformas (servidor y estaciones de trabajo) donde esté configurado. Las notificaciones emergentes muestran, por ejemplo, advertencias o notificaciones de recuperación.

La interfaz de usuario del CNMS está basada en un navegador y se puede acceder a ella desde cualquier punto de una red conectada (es decir, desde cualquier puesto de trabajo). Se instalará un servidor CNMS independiente en el sistema CO-AMHS utilizando la estacione de trabajo OWP Monitoreo Tecnico

CNMS es capaz de enviar Traps SNMP para alarmas configurables. Normalmente, las alarmas se configuran para eventos críticos, por ejemplo, un fallo del hardware del servidor o de un componente de software.

3.3.3 Monitorización de Servidores VM Host

Dado que en los servidores se instala VMWare ESXi en lugar del Sistema Operativo Linux, está previsto utilizar HP iLO para monitorizar los componentes Hardware del servidor. No habrá costes adicionales en cuanto a licencias, ya que la licencia iLO estándar incluida en los servidores es suficiente.

3.4 CCMS

CCMS es la suite de gestión de la configuración de Frequentis Comsoft y ofrece funciones avanzadas para la configuración y gestión centralizadas de las plataformas de hardware y las aplicaciones de software que forman el sistema completo de gestión de mensajes. CCMS se basa en una herramienta ampliamente utilizada de aprovisionamiento de software, gestión de la configuración e implantación de aplicaciones: Ansible. Entre otras, CCMS proporciona funciones para:

- Gestión centralizada de las versiones de software para las distintas aplicaciones de software.
- Asignación de aplicaciones software a plataformas VM / hardware.
- Configuración de un subsistema para que se reinicie automáticamente al detectar un error.
- Distribución de datos de configuración y versiones de software a sitios y sistemas remotos.
- implementar un endurecimiento mejorado del SO, por ejemplo, se habilitará por defecto el control de acceso obligatorio para procesos (SELinux en modo enforcing) y usuarios (Fapolicyd)
- permitir la ejecución de un servidor en modo headless (sin interfaz gráfica de usuario, sin usuario conectado)
- permitir que un subsistema, por ejemplo un OSS AIDA-NG, sea ejecutado por cualquier usuario de Linux con acceso a una interfaz gráfica de usuario (no sólo oper)
- Utilizando el procedimiento de instalación en el que CCMS desempeña un papel central, es posible reinstalar muy rápidamente una plataforma y el sistema completo.

Se incluye una actualización de la última versión publicada de CCMS compatible con la última versión de Linux 8 admitida por la FCO para la plataforma virtual y física del sistema propuesto.

La nueva versión de CCMS se basa en Ansible, una herramienta ampliamente utilizada para el aprovisionamiento de software, la gestión de la configuración y el despliegue de aplicaciones.

Los principales conceptos conocidos y probados del predecesor se han conservado en gran medida:

- sigue habiendo ubicaciones (ahora denominadas sitios), plataformas (ahora denominadas hosts), configuraciones de plataforma (ahora denominadas configuraciones de host) y sistemas
- siguen existiendo 2 servidores de inicio (ubicados junto a los servidores AIDA-NG)
- la gestión del sistema sigue realizándose a través de una interfaz de usuario basada en web

- una vez desplegados el sistema y la aplicación, CCMS es transparente para el usuario y funciona en segundo plano.
- también es posible controlar de forma remota subsistemas (arranque, parada) y hosts (reconfiguración, reinicio, detención) mediante la interfaz de usuario web

Las siguientes capturas de pantalla de ejemplo ilustran lo anterior (no representan la configuración final).

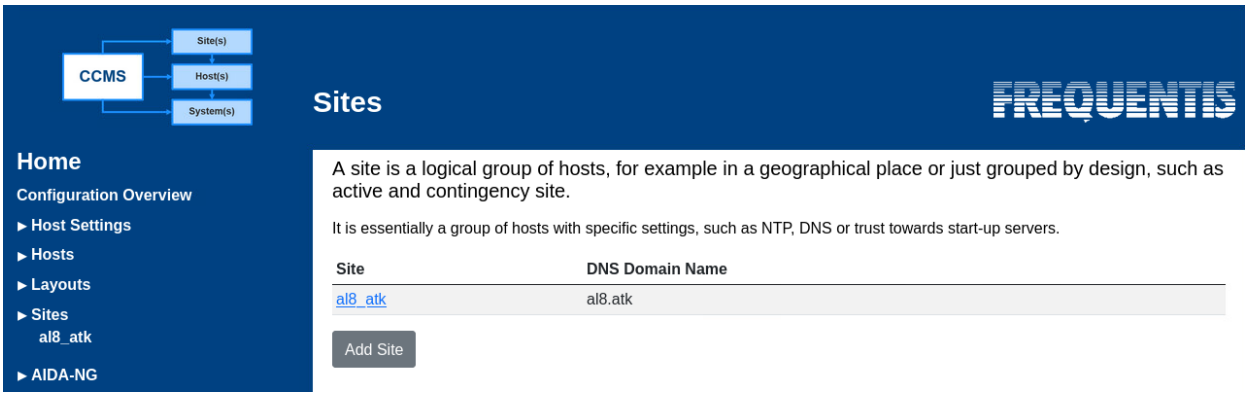


Fig. 6: CCMS web UI: Sites

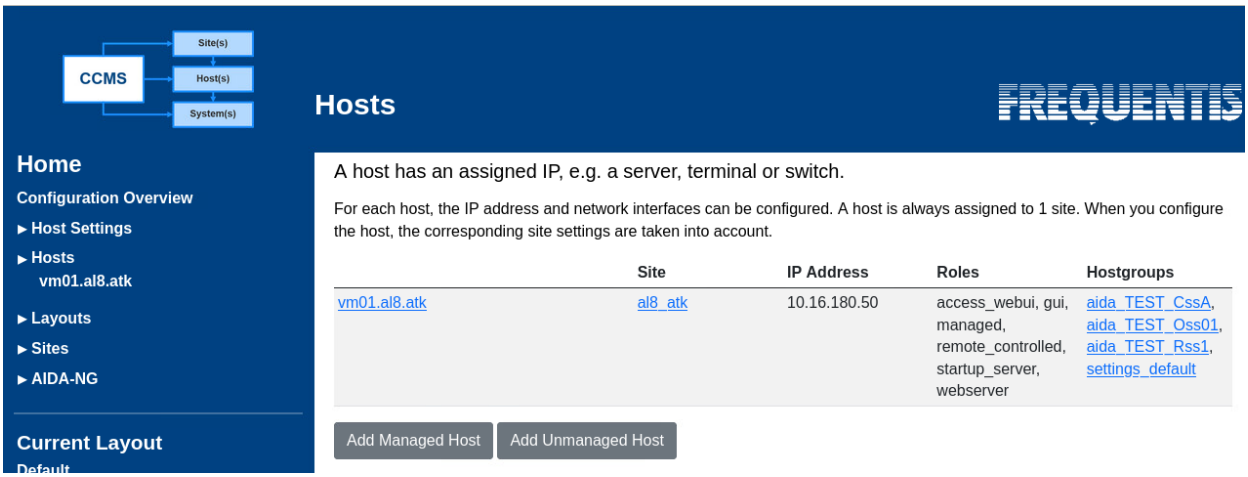


Fig. 7: CCMS web UI: Hosts

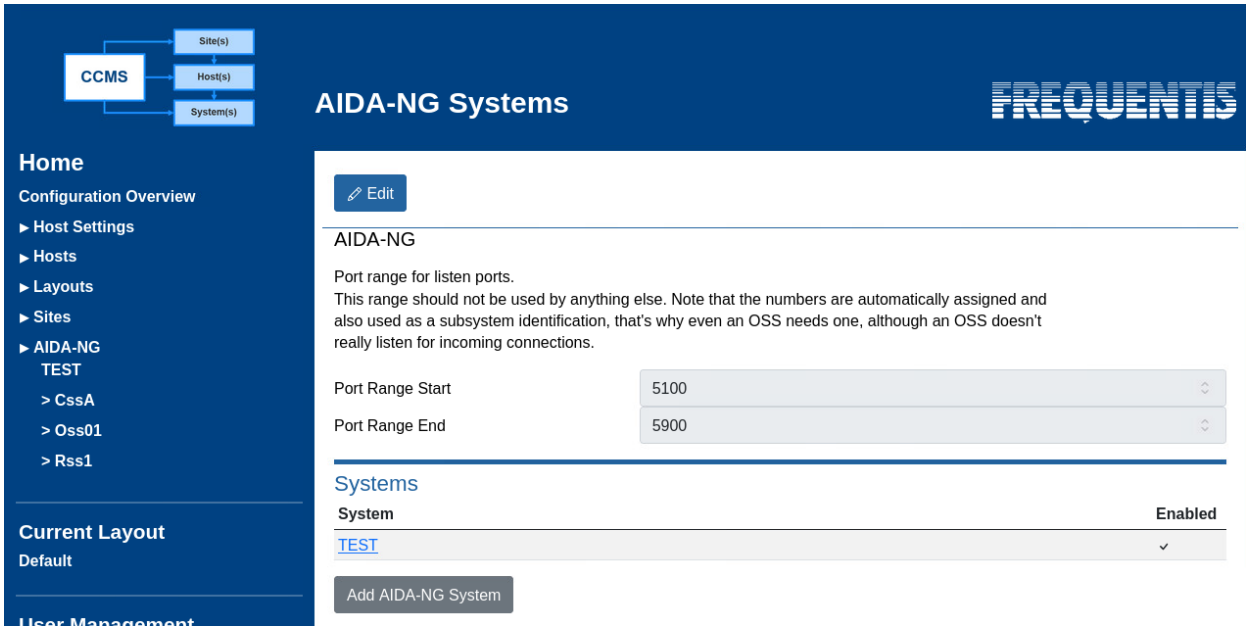


Fig. 8: CCMS web UI: AIDA-NG Systems

La nueva versión de CCMS:

- Mejorará la seguridad del sistema operativo, por ejemplo, se activará por defecto el control de acceso obligatorio para procesos (SELinux en modo enforcing) y usuarios (Fapolicyd)
- permitirá ejecutar un servidor en modo headless (sin interfaz gráfica de usuario, sin usuario conectado)
- permitir que un subsistema, por ejemplo un OSS AIDA-NG, sea ejecutado por cualquier usuario de Linux con acceso a una interfaz gráfica de usuario (no sólo oper como actualmente)

3.4.1 Generación de kickstart

Debido a una importante revisión de cómo se implementa y despliega CCMS, el mecanismo existente para generar un kickstart y la instalación desde un kickstart ha cambiado. No obstante, seguirá siendo posible desplegar kickstart que contengan plataformas específicas para cada uno de los sitios remotos.

3.5 Sistema Operativo

Las máquinas virtuales del servidor, así como las estaciones de trabajo, requieren la última versión del sistema operativo Linux publicado por FCO. Para el sistema propuesto, actualmente está previsto utilizar AlmaLinux 8 en tecnología de 64 bits.

El sistema operativo utilizado contendrá los últimos parches de software disponibles en el momento de la producción del sistema. Antes de la entrega del sistema propuesto, FCO realizará

un escaneo de seguridad Nessus que comprobará los componentes de software del sistema en busca de vulnerabilidades.

El sistema operativo Linux se instalará en todas las plataformas (máquinas virtuales y estaciones de trabajo) que entregue FCO.

4 Seguridad del Sistema

4.1 General

El Cliente será el único responsable de salvaguardar el Sistema y de controlar el acceso físico y virtual al mismo. Esto incluye, entre otras cosas, la protección del Sistema contra virus, troyanos, malware, gusanos y ataques de piratas informáticos. El Cliente está obligado a cambiar todas las contraseñas de administrador después de la instalación.

El Cliente tiene derecho a conceder acceso en línea a FCO o a cualquier empleado de FCO previa solicitud por escrito y por un tiempo limitado. El acceso concedido será cancelado inmediatamente una vez cumplido el propósito para el que se ha concedido el acceso o en cualquier momento anterior si así lo solicita FCO o si el Cliente tiene conocimiento de una amenaza causada por este acceso.

4.2 Características de seguridad de aplicaciones / software

4.2.1 Seguridad del sistema operativo

Se aplicarán los últimos parches de seguridad de software en el momento de la producción. El sistema operativo Linux que se utilizará en el capítulo 3.5 se reforzará de acuerdo con las pruebas de referencia estándar del sector, como el perfil CIS RHEL Benchmark.

Además, SELinux estará activado por defecto en el sistema operativo. Se aplicará la política SELinux y se denegará el acceso basándose en las reglas de la política SELinux. Todas las aplicaciones de Frequentis Comsoft proporcionarán un conjunto de reglas de política SELinux para garantizar la compatibilidad funcionando con el modo de aplicación.

Antes de entregar el sistema propuesto, FCO realizará un escaneo de seguridad Nessus que comprueba los componentes de software del sistema en busca de vulnerabilidades.

4.2.2 Seguridad X.400/AMHS

Tanto en AIDA-NG como en CADAS-ATS, se implementará el grupo funcional SEC del servicio ampliado AMHS de acuerdo con las especificaciones aplicables de la OACI.

5 Red (Network)

5.1 Red del Sistema

La LAN redundante del sistema garantizará que los componentes que conforman el sistema central puedan comunicarse entre sí, incluso en caso de fallo del hardware.

Todos los hosts VM y los puestos de trabajo de los sistemas CO-AMHS estarán conectados a esta LAN de sistema.

Para la comunicación externa (p. ej. AFTN/TCP, X.400 P1, X.400 P3, HTTP) los conmutadores LAN del sistema estarán conectados a la REDDIG / ATN gestionada por la UAEAC. La dirección IP operativa para AIDA-NG y CADAS-ATS será definida por el usuario final, siendo posible usar el mismo direccionamiento actual. Con ello se pretende minimizar la configuración necesaria y garantizar una transición fluida durante el despliegue operativo.

Puede ser posible reconfigurar los routers IP existentes para ser utilizados además del sistema.

Todo el diseño de la red y el direccionamiento IP para las plataformas virtuales y físicas se coordinará con la UAEAC.

El sistema se interconectará a la RED ATN de la UAEAC a través de una conexión redundante.

5.2 Red de Servicios

La Red de Servicio virtual gestiona el tráfico de servicio iniciado o causado por los operadores o por los ingenieros. Esto incluye la exportación/importación de la configuración, la supervisión SNMP de los servidores host, iLO y el hipervisor ESXi.

Las conexiones existentes de todas las plataformas que necesiten utilizar la LAN de servicio utilizarán el etiquetado VLAN y se definirán dos interfaces VLAN en el mismo dispositivo físico de las plataformas. Cada una tendrá su propia dirección en diferentes rangos de direcciones. El enrutamiento estático garantizará la separación del tráfico de servicio del tráfico operativo.

5.3 Servicio de acceso remoto

Las herramientas remotas de FCO permiten un acceso completo a todos los recursos del sistema, por ejemplo, a los parámetros del sistema y a las funciones de diagnóstico y seguimiento. Además, las nuevas versiones de software pueden descargarse, probarse y activarse a petición del usuario.

El acceso remoto al sistema proporcionado por el Cliente estará totalmente bajo su control. El ancho de banda de la conexión remota debe ser de al menos 512 Kbps o mejor. Si el ancho de banda proporcionado es de velocidad analógica, FCO es capaz de dar sólo un apoyo limitado (por ejemplo, la visualización de archivos LOG, etc.)

FCO considera que el acceso remoto al sistema es una herramienta importante para proporcionar al cliente un soporte rápido y fiable. FCO, gracias a su experiencia con otros sistemas, está convencida de que la utilidad de soporte remoto es una herramienta adecuada para manejar casi todos los problemas de mantenimiento no relacionados con el hardware y proporciona al cliente un soporte óptimo. La herramienta de acceso remoto se basa en "VNC". El servidor VNC se instalará en una plataforma dedicada (normalmente un OWP). FCO se conectará a través del cliente VNC a este servidor a una pantalla separada.

Por razones de seguridad, FCO establecerá la conexión remota mediante una conexión de túnel VPN.

Acceso proporcionado por el cliente

FCO se conectará a un punto de acceso existente proporcionado por el cliente. El cliente es responsable de entregar toda la información y/o herramientas necesarias.

5.4 Seguridad de la red

UAEAC se encargará de la configuración de Firewalls, proxys inversos, routers y otros elementos de red que permitan el tráfico, puertos, IPs, para un correcto funcionamiento del sistema.

6 Hardware

El sistema utiliza productos COTS de los principales proveedores que siguen las normas internacionales o las mejores prácticas ampliamente aceptadas. Este documento describe los componentes del sistema disponibles actualmente en el mercado.

El sistema se basa en una arquitectura de servidor estándar montable en bastidor, equipado con una CPU de alto rendimiento en una única placa base.

El sistema tiene un diseño modular que facilita el mantenimiento, la configuración y las pruebas por parte de un solo técnico. Todos los dispositivos son fácilmente accesibles desde su parte frontal y trasera. Todos los elementos están sujetos mediante tornillos. El cableado está claramente dispuesto y es fácil de manejar. Todos los dispositivos pueden protegerse contra el acceso no autorizado gracias a las puertas con cerradura del armario. Todas las etiquetas y controles están en inglés. El equipo puede funcionar 24 horas al día, 7 días a la semana.

Cada parte del equipo lleva un número de serie que se mencionará en el Documento Central de Identificación (CID).

El sistema se despliega de forma redundante, todos los componentes redundantes pueden sustituirse sin interrupción de los servicios operativos.

El sistema se fabrica de acuerdo con la norma europea EN 62368-1.

FCO utiliza cables de instalación CAT6 o CAT7 para sistemas de cableado genéricos con las siguientes especificaciones:

- S/FTP (Par trenzado apantallado/enrollado)
- 4x2 AWG23/1
- Libre de halógenos (LSZH)

Los cables están etiquetados con un número para identificar el tipo, la longitud y la ubicación del cable.

El sistema consta de los siguientes componentes principales:

- Dos (2) Servidores
- Cinco (5) Workstations con pantalla
- Dos (2) Servidores de Tiempo NTP
- Dos (2) Switches de Red

6.1 Servidores

Manufacturer	Hewlett Packard Enterprise
Model	**ProLiant DL380 Gen10**

Type	19" rack mountable, 2 U, Telescopic bars for easy replacement,
Processor	**1x Intel Xeon Gold 5215** Processor (10 Cores/ up to 3.4 GHz)
RAM	**64 GB**
Video	Integrated video standard 1280 x 1024 (32 bpp) 1920 x 1200 (16 bpp)
RAID Controller	**Smart Array P408i-a SR/2GB with 96W Smart Storage Battery**
Storage	**4x 600GB**: HPE 600GB SAS 12G Mission Critical 10K SFF SC 3-year Warranty Multi Vendor HDD
Optical drive	**DVD/CD RW SATA**
LAN	4x RJ45 10/100/1000 BaseTx ports on-board **1x 4-port PCIe-based 10/100/1000 BaseTx LAN:** - **HPE Ethernet 1Gb 4-port BASE-T I350-T4V2 Adapter**
Power Supply	Redundant, **2x 800W Platinum**, hot plug
USB 3.0 ports	1x front, 2x rear, 2x internal
PCI	3x PCI Express

Tab. 6: Especificación del Servidor

El calculo de RAID5 se realiza de la siguiente manera:

*Almacenamiento bruto: 2,4 TB / 2400,0 GB
*Almacenamiento utilizable: 1,6 TB / 1676,4 GB
RAID 5 utiliza un disco para Paridad y requiere al menos tres discos para ser utilizado.

6.2 Workstations

Las siguientes especificaciones se utilizarán para las estaciones de trabajo de Operador/Supervisión, Supervisión Técnica y Agente de Usuario.

Manufacturer	Hewlett Packard
Model	Z2 Gen9 SFF
Processor	Intel® Core™ i7-12700
Memory	16 GB

Manufacturer	Hewlett Packard
Storage	1TB SSD
DVD	DVD/RW
LAN	1 x Ethernet 10/100/1000 Base Tx, on-board 1 x Ethernet 10/100/1000 Base Tx, NIC, PCIe
Sound	On-board
USB	2.0, 3.0
Keyboard	USB, US-international-Layout
Mouse	USB, Optical Scroll Mouse

Tab. 7: Especificación de la Workstation

6.3 Display para Supervisión y Workstations de Monitorización

Manufacturer	Hewlett Packard Inc.
Brand Name	P24h G4
Model	23.8” IPS
Resolution	1920x1080, 16:9
Contrast ratio	1000:1
Response time	maximum 5 ms
Dot pitch	0.274 mm
Brightness	250 cd/m²
Input	1x VGA, 1x HDMI, 1x DisplayPort
Viewing angle	from centre for left/right and up/down: 178°/178° total
Speakers	integrated
VESA Mount	Yes, 100mm x 100mm

Tab. 8: Especificación del Technical Monitoring Display

6.4 Equipamiento de Red

Manufacturer	CISCO
Model	C9200L-48T-4G-E
Ports	• 48 RJ45 Gigabit Ethernet • 4 GB SFP All ports auto-negotiation
Features	Manageable, Network Essentials Perpetual License

Power Supply	Redundant Power Supply
Form Factor	19”

Tab. 9: Especificación del System LAN Switch

6.5 Receptor GPS/ Servidor horario NTP

Dos (2) Receptores de GPS. El sistema de temporización se compone de dos módulos receptores GPS independientes con servidor NTP integrado, uno de ellos alojado en el interior de cada uno de los Gabinetes AMHS. Un reloj de tiempo real integrado mantiene un tiempo de alta precisión en caso de falta de la señal GPS. Se usan dos antenas GPS independientes para recibir la señal de tiempo GPS. A fin de proporcionar protección contra sobretensiones del sistema GPS, un protector contra rayos pasivo está instalado en cada una de las trayectorias de las antenas de recepción.

La especificación del sistema GPS es como sigue o similar:

Manufacturer	HOPF
Model	8029HEPTA-V2/GPS
Tipo	Receptor GPS/Servidor de tiempo NTP/Sistema de tiempo, 19" slim line 1U
Features	• Pulso PPS interno: < +/- 100ns • Regulación del VCO: +/- 0,1ppm, después de 30min. Recepción GPS • Deriva para T= +20oC (const.) después de 1h: 0,36mseg. • Precisión de la rueda libre: después de 24h: 8,64mseg • Salida: 1x Ethernet 10/100Mbit RJ45, 1x puerto USB para recuperación Salida del estado de sincronización a través de un acoplador óptico • Protocolos: SNMP, HTTP/HTTPS-WebGUI, Telnet, NTPv4 • Antena Activo: IP65, compacto con cable RF y protector contra rayos
Power Supply	AC Power Supply

Tab. 10: Especificación Reloj GPS

La información del tiempo se distribuirá a través del protocolo NTP a cada una de las LAN del sistema.

7 Disponibilidad, fiabilidad y mantenimiento

Debido al tiempo de funcionamiento requerido de 24 horas al día durante todos los días del año, todos los componentes del sistema relevantes para la seguridad están como mínimo duplicados para proporcionar la altísima disponibilidad que presenta una de las características más decisivas del sistema.

El diseño redundante del sistema permite reparar o sustituir una pieza defectuosa en paralelo al funcionamiento del sistema. Además, el diseño del sistema - junto con los mecanismos de supervisión incorporados - no impone la necesidad de actividades de mantenimiento periódicas. Por lo tanto, no se producen interrupciones regulares del servicio.

En caso de fallo de hardware del servidor operativo, el servidor de reserva se hará cargo automáticamente del servidor en un plazo no superior a 10 segundos en condiciones normales de funcionamiento (sin colas excesivas, sin carga excesiva del sistema, etc.).

Tras el encendido, el sistema puede reiniciarse automáticamente (es decir, pasa a estar operativo sin intervención del operador) en 10-15 minutos.

Es muy poco probable que el sistema no pueda reiniciarse automáticamente tras un error de hardware o software. Debido al hecho de que todos los componentes de hardware esenciales están al menos duplicados, esto sólo puede ocurrir si, por ejemplo, dos fuentes de alimentación o todos los servidores fallan simultáneamente. Debido al corto MTTR (incluyendo MRT), es muy poco probable que esto ocurra si los eventos se consideran estadísticamente independientes. Sin embargo, si esto ocurriera, al menos uno de los dos componentes defectuosos debe ser sustituido para permitir el reinicio del sistema. El cambio de una pieza de hardware defectuosa es una acción de mantenimiento que debe llevar a cabo el personal de mantenimiento de primera línea.

Lo mismo ocurre con los errores de software de aplicación. Además, el software está duplicado y es extremadamente improbable que dos servidores fallen simultáneamente. Sin embargo, si a pesar de todo esto ocurriera debido a un mal funcionamiento de la aplicación, el almacenamiento de múltiples versiones de software permitirá al administrador volver a la última versión de software fiable en menos de cinco minutos. El cambio a una versión de software anterior es una acción de mantenimiento que debe realizar el personal de mantenimiento de primera línea.

El fallo simultáneo de todos los componentes de hardware redundantes podría deberse a un fallo de causa común. Las estadísticas de eventos que causan fallos de modo común no se conocen y no pueden tenerse en cuenta en los cálculos de la disponibilidad del hardware.

La aplicación supervisa su propio estado y lo muestra al administrador. Los componentes de hardware pueden supervisarse mediante SNMP utilizando una estación de supervisión externa.

Los mecanismos descritos anteriormente garantizan que la disponibilidad del sistema (tanto calculada como observada a lo largo de muchos años de experiencia operativa) superará el valor de 99,99%.

7.1 Clasificación de la gravedad de los fallos

Las clasificaciones de gravedad de los fallos se definen como sigue:

- Categoría 1 - Fallo catastrófico

Fallo inherente al Sistema que provoca la pérdida total del mismo. El sistema no puede cumplir su misión: Se ven afectadas partes importantes del Sistema y no puede garantizarse su funcionamiento. No existen soluciones alternativas ni sistemas de reserva para compensar la ausencia del sistema.

- Categoría 2 - Fallo crítico

Fallo inherente al Sistema que provoca la pérdida de las principales funciones del mismo. La función del sistema se ve comprometida: El sistema no puede desempeñar su misión, pero puede restablecerse mediante la reconfiguración del sistema o el uso de instalaciones de reserva.

- Categoría 3 - Fallo marginal

Fallo inherente al Sistema que provoca la pérdida de funciones menores del Sistema. El funcionamiento del sistema se ve parcialmente comprometido: La capacidad del Sistema para desempeñar su Misión se degrada, pero puede mantenerse por otros medios.

- Categoría 4 - Fallo insignificante

Fallo inherente al Sistema que no ocasiona ninguna pérdida de sus funciones. No se degrada la capacidad del sistema para cumplir su misión.

8 Anexo A: Artículos suministrados por el cliente (CFI)

8.1 Equipo suministrado por el cliente / Usuario Final

Item	Descripción del ítem	Fecha requerida	Comentarios
1	El Cliente será responsable de proporcionar acceso remoto al sistema.	Listo para la instalación del sistema	Acceso remoto para FCO
2	El cliente será responsable de proporcionar, configurar y dar soporte a la red LAN ATN subyacente.	Listo para la instalación del sistema	El cliente debe configurar la red para que admita la interconexión de sitios remotos, sistemas internos y sistemas externos.
3	Cuando se requieran nuevos cableados, el cliente será responsable del suministro de todo el cableado desde la red LAN ATN hasta el nuevo Sistema AMHS-COL, así como de los distintos terminales.	Listo para la instalación del sistema	
4	En los puestos de operador en los que se sustituirán los puestos de trabajo por los nuevos, el cliente deberá asegurarse de que se dispone de espacio suficiente y preparado para la instalación.	Transición	
5	El Cliente deberá suministrar el cable de alimentación para la sala de equipos donde se instalará el servidor de acuerdo con las necesidades de consumo del Sistema. Así como las conexiones a los sistemas de protección de descargas	Listo para la instalación del sistema	

Item	Descripción del ítem	Fecha requerida	Comentarios
6	El cliente será responsable de la entrega e instalación de las estaciones de trabajo UA en sus destinos previstos. FCO entregará las estaciones de trabajo únicamente en el CGAC en las oficinas de Centrocom.	Después del SAT	
7	El cliente proporcionara un espacio adecuado para la instalación del sistema dentro de un gabinete de su Sala técnica	Listo para la instalación del sistema	
8	El Cliente/Usuario Final será responsable de suministrar los certificados válidos y vigentes para un correcto acceso vía HTTPS en el sistema CADAS-ATS	Antes de FAT	

Tab. 11: Equipo Suministrado por el Cliente/Usuario Final

8.2 Datos e información facilitados por el cliente/Usuario Final

Item	Descripción del ítem	Fecha requerida	Comentarios
1	Lugar de instalación	Kick-Off	

Item	Descripción del ítem	Fecha requerida	Comentarios
2	Documentos e información que no se enviaron junto con la solicitud de propuestas, especialmente, pero sin limitarse a ellos: • Documentos de control de interfaz (DCI) y • Cualquier otro dato/información necesaria para que FCO pueda finalizar el diseño del sistema y el análisis de requisitos más reciente en la revisión del diseño.	Fecha del contrato	Si hiciera falta alguna información importante en la oferta, esta definición deberá llevarse a cabo durante la fase final de negociación. A partir de estos requisitos funcionales, FCO elaborará los documentos necesarios para poner en marcha el sistema.
3	Asignación de todos los permisos necesarios para entrar en los locales y ubicaciones de los clientes cuando sea necesario.	Fecha del contrato +2 Semanas	Dicho permiso debe estar en vigor durante la inspección del emplazamiento, la supervisión de la instalación y la prueba de aceptación del emplazamiento, como mínimo..
4	Publicación del destino del envío de la documentación (un depósito central)	6 Semanas antes del envío	
5	El cliente proporcionará a FCO una copia de seguridad de los parámetros y la configuración del sistema para las pruebas	6 semanas antes del envío	

Tab. 12: Datos e información facilitados por el cliente/Usuario Final

8.3 Servicios prestados por el cliente/Usuario Final

Ítem	Descripción	Fecha requerida	Comentarios
1	Revisión y aprobación de la información relevante del Proyecto o diseño (hardware y software) proporcionada por FCO para revisión y aprobación del Cliente en un plazo de diez (10) días laborables.	Entrega de documentos + 10 días laborables	
2	Revisión y aprobación del plan de pruebas FAT y la especificación de pruebas FAT.	Entrega de documentos + 10 días laborables	Antes de FAT.
3	Revisión y aprobación del informe de pruebas FAT y del certificado FAT.	1 semana después de FAT	
4	Revisión y aprobación del plan de pruebas SAT, las especificaciones de las pruebas SAT y las hojas de datos.	Entrega de documentos + 10 días laborables	Antes del SAT.
5	Revisión y aprobación del informe de la prueba SAT y del certificado SAT.	1 semana después del SAT	
6	Revisión y aprobación del procedimiento de transición.	Entrega de documentos + 10 días laborables	Antes de la transición.
7	Facilitar al equipo de instalación y SAT de FCO el acceso a los emplazamientos.	Instalación / SAT	
8	Presencia y apoyo durante las actividades in situ (instalación del sistema, pruebas in situ, transición, según sea necesario).	Instalación / Transición	
9	Realización del SAT junto con el FCO de conformidad con el plan de pruebas SAT y los procedimientos de prueba SAT acordados.	SAT	
10	Apoyo en la transición del sistema al servicio operativo de acuerdo con el plan de transición.	Transición	

Tab. 13: Servicios prestados por el cliente/Usuario Final