ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS

ESCUELA SUPERIOR DE GUERRA CONJUNTA DE LAS FUERZAS ARMADAS

CURSO DE ESTADO MAYOR Y PLANEAMIENTO CONJUNTO

Trabajo de Investigación Profesional

Plan de Trabajo

Tema:

Elaboración de los lineamientos de la Norma para la integración de datos radar del AMC.

Titulo:

Consideraciones para la integración de sensores, para la elaboración de un sistema de control y vigilancia aeroespacial conjunta.

Autor: My BAZÁN, Guillermo F.

Tutor: Com. MORESI, Alejandro.

ÍNDICE

Abstracto

El aeroespacio es parte crucial y usado por todos los componentes en los entornos operacionales. Además existe una alta concentración de medios de superficie (terrestres o marítimos) que utiliza este medio para proyectar sus capacidades de poder de combate. Es entonces que el objetivo principal de controlar el aeroespacio, es mejorar la eficacia de los medios conjuntos y aumentar la seguridad de las operaciones aéreas conjuntas.

En este entorno, se debe contar con un sistema que permita la conducción de los medios en forma centralizada, en donde se debe evitarse el fratricidio, aumentar la libertad de acción de las aeronaves y sistemas de armas, tanto de alta y baja velocidad, (tripulados y no tripulados), discriminar de manera rápida y eficaz las aeronaves amigas, enemigas y neutrales, sincronizar las armas superficie-aire de defensa y los aviones de defensa aérea para lograr la máxima eficacia, y garantizar que la red de control del espacio aéreo sobreviva y sea eficaz, frente a un ataque enemigo.

El protocolo de comunicaciones ASTERIX, abreviatura de: **A**ll Purpose **ST**ructured **E**urocontrol Su**R**veillance **I**nformation E**x**change, se creó como solución tecnológica para maximizar los recursos operacionales, alcanzando la **integración**, **interconexión** y **estandarización** de la información de los distintos sistemas y sensores radar aéreo, terrestre y marítimo. La implementación de este protocolo favorecerá y dará ventajas competitivas en la interoperatibilidad, manejo de masa y tiempo, unidad de esfuerzo, y acelera los ciclos de respuesta.

Al tratarse de un estándar de comunicaciones de aplicación a nivel conjunto, se entiende que el órgano responsable de llevar adelante la migración de este proceso será el EMC – C6 - Comunicaciones.

Como es un estándar de aplicación a nivel operacional, se entiende que la responsabilidad de coordinar e implementar esta tecnología estará bajo la responsabilidad del EMC- C6 Comunicaciones,

Antecedentes del sistema de control y vigilancia aeroespacial en la Argentina[1]

La Argentina fue pionera dentro de la región, en la materia, durante los años 50 y 60 constituyendo un sistema de vigilancia y control aéreo orientado a la defensa del llamado "Centro de Poder Buenos Aires", que aplicaba todas las enseñanzas de la II GM y las guerras posteriores. Integraban dicho sistema, además de una serie de radares de largo y corto alcance dispuestos alrededor de Buenos Aires, sistemas de comunicaciones, caza interceptores (Gloster Meteor), artillería antiaérea de alta y baja cota, centros de información y control subterráneos, entre otros.

Con el vertiginoso desarrollo de la aviación en general y de la comercial en particular, el Estado Nacional ha ido impulsando a lo largo de los años, diferentes planes tendientes a lograr la vigilancia y control integral de su aeroespacio, los cuales no llegaron a materializarse por diversas razones.

Así nacieron el Sistema Integrado de Control del Espacio Aéreo (SICEA) en los años '70 y '80; el Plan Nacional de Radarización (PNR) en los años '90 que fuera aprobado por Decreto 145/96; y actualmente el llamado Sistema Nacional de Vigilancia y Control Aeroespacial (SINVyCA) que lo remplazó.

Este sistema está destinado al gerenciamiento integral del aeroespacio para ejecutar tanto la vigilancia y el control del tránsito aéreo, como la defensa de aeroespacio de interés, y fue propuesto por la Fuerza Aérea Argentina y el Ministerio de Defensa. El 14 de octubre de 2004, el presidente Kirchner firmó el Decreto 1407/04 que derogó al 145/96 y creo el SINVyCA.

Entre los fundamentos del nuevo Decreto 1407/04 merece destacarse el párrafo que señala: "dado el incremento que ha tenido la actividad de vuelos ilícitos a nivel mundial y más específicamente a nivel regional, relacionados con el contrabando y el uso del medio aéreo como elemento terrorista, se hace imprescindible poder contar con radares y sistemas que realicen un control efectivo del aeroespacio, de manera de proteger el tránsito aéreo en el ámbito nacional, el desarrollo nacional y la seguridad de sus fronteras".

[1] Vigilancia Aeroespacial en la Argentina - Brigadier Mayor (R) Horacio Rodríguez, socio activo y Vicepresidente del Centro Aeronáutico de Estudios Estratégicos.

Introducción a los sensores radar.[2]

La palabra radar corresponde a las iniciales de "radio detection and ranging", y fue utilizado por las fuerzas aliadas durante la II Guerra Mundial para designar diversos equipos de detección y para fijar posiciones. No sólo indicaban la presencia y distancia de un objeto remoto, denominado objetivo, sino que fijaban su posición en el espacio, su tamaño y su forma, así como su velocidad y la dirección de desplazamiento.

El concepto de funcionamiento del radar es relativamente simple, pero su implementación no lo es. Un Radar es un elemento que irradia pulsos de energía electromagnética y detecta los ecos que se reflejan de los objetos irradiados (targets). Desde este punto de vista podemos decir que el radar se ha convertido en un sensor electromagnético que detecta y localiza el reflejo de objetos. Esta operación puede resumirse en los siguientes pasos:

- El radar irradia energía electromagnética desde su antena propagándola al espacio.
- Parte de esa energía irradiada, es interceptada por el objeto, usualmente llamado “target”, ubicado a cierta distancia del radar.
- La energía interceptada por el target es re-irradiada en varias direcciones.
- Parte de esta energía re-irradiada (eco) retorna y es recibida por la antena radar.

Después de la amplificación de la señal recibida, es procesada por un modulo digital o DSP (digital signal processing), quien decide si la señal recibida se trata de un eco o no. El producto de este proceso, sumado a otros procesos digitales posibilita la representación en pantalla de un objeto y su respectiva información asociada.

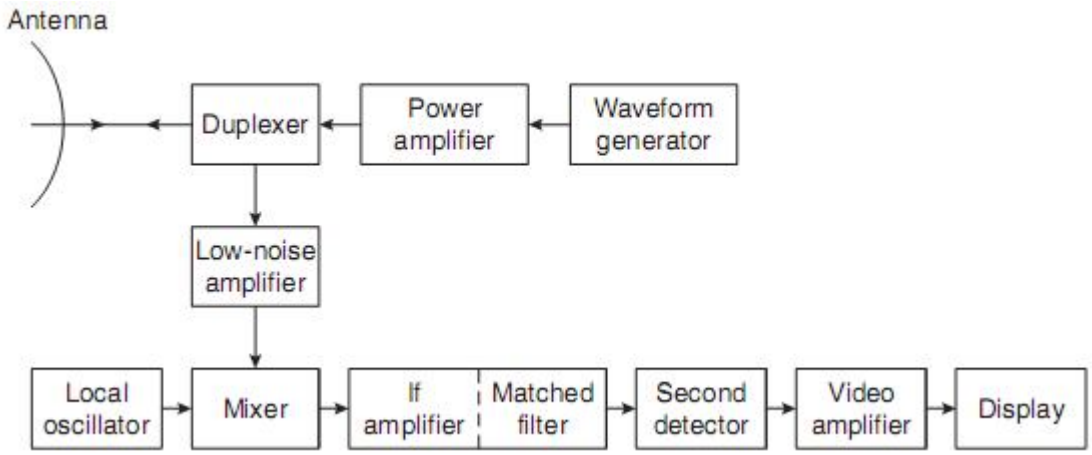
Para ejemplo del lector (o recuerdo) comúnmente la forma de onda irradiada es un conjunto de pulsos cuadrados muy estrechos, estos pulsos una duración en millonésima parte de un segundo (microsegundos), y el tiempo entre la emisión del pulsos y la onda reflejada es del orden de los milisegundos. La potencia radiada del radar es del orden de los kilowatts y la potencia recibida del objeto irradiado es del orden 190dB menos que la potencia irradiada. Los radares pueden detectar aeronaves, barcos o misiles, pero también pueden detectar gente, pájaros, insectos, precipitación, vegetación, hielo, montañas, auroras, meteoritos, satélites, etc.; en relación a los targets, el sensor radar tiene la capacidad de medir la dirección angular, la velocidad relativa, la forma (firma digital), posición (track), o trayectoria, entre los más importantes.

[2] Radar Handbook – Merill Skolnik - Tercera edición - 2008 by The McGraw-Hill Companies – Pag. 1.1

Partes básicas de un sensor Radar[3]

Nuevamente traeremos a colación las partes de un radar tomadas de referencia del Radar Handbook antes mencionado, las que se muestran en la figura 1, con el objeto de posicionarnos en el tema en cuestión. El transmisor, el cual está incluido dentro de la figura de “power amplifer”, el que genera una onda electromagnética en forma de pulso; el “duplexer” permite utilizar una misma antena tanto sea para la transición como para la recepción de señal de onda, en ese sentido este componente tiene como valor agregado, la de proteger a los sensibles receptores electrónicos. La “antenna” que es el dispositivo que permite transmitir la energía y recolectar la energía re-irradiada por los objetos (ecos). Es casi siempre un tipo de antena directiva, tanto como para el direccionamiento del pulso electromagnético, como también para la recepción del mismo; la “antenna” no solo concentra energía, sino que también posee filtros espaciados que permiten proveer resolución sobre el ángulo de la onda recibida y otras capacidades. El receptor amplifica la débil señal recibida del “duplexer”, en la figura de “low-noise amplifier”, este módulo electrónico presenta una solución a los problemas planteados por la baja señal recibida (apenas perceptible) y el ruido del entorno. Luego para demodular la señal recibida se mezcla con el “local oscilator” en el “mixer”. Luego esta señal se introduce en el “if amplifier”, en donde se separa la señal deseada de la señal no deseada, el “matched filter” es la parte en donde se maximiza la señal para diferenciarla del ruido; estos dos módulos están incorporados o integrados dentro de lo que se conoce como el “signal procesor”; sin adentrarnos demasiado en términos de ingeniería, podemos decir que este modulo establece los niveles de detección de la señal que establecerán si la señal recibida se trata de un objeto o producto de otro tipo de fenómeno electromagnético. Como producto final de esta etapa produce la señal de los objetos irradiados. Seguidamente al proceso, el “second detector” le aporta a la señal producida por las etapas anteriores, el valor de la información del análisis propio de la señal del objeto detectado, los cuales se introducen en el “video amplifer” y la señal finalmente es representada en el “display”.

[3] Radar Handbook – Merill Skolnik - Tercera edición - 2008 - by The McGraw-Hill Companies – Pag 1.2.



Información disponible del sensor radar.

La detección de los "targets" tendría poco valor, a menos que se obtenga algo más de información sobre la señal que se ha detectado. Este concepto nos lleva a entender y a aclarar que existe diferencias entre la información vertida propia de la detección de un "target" ("target detection"), como lo son la velocidad, la distancia, etc.; y la información que pueda extraerse de la señal del "target" ("target information"), más relacionada con la capacidad electrónica del radar y su equipamiento, como lo son el tamaño del eco y su firma electrónica, entre otros.

Cambiando el enfoque del análisis que hasta ahora hemos realizado, reflexionemos y observemos al sensor radar ya no como un equipamiento de alta complejidad electrónica, sino como un sistema capaz de producir información.

Sistemas de información genéricos

Introduzcámonos en el tema, y definamos a un sistema de información como un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de uno o varios actores.

Estos elementos se caracterizan por cuatro actividades básicas: entrada, almacenamiento, procesamiento y salida de información.

Entrada de Información: Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos.

Almacenamiento de información: El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos, o también en bases de datos.

Procesamiento de Información: Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones.

Salida de Información: La salida, es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo integrador.

Dada la explicación de cómo un sistema de información funciona, podemos hacer un paralelismo con el sensor radar; el radar es ahora un productor de información, que vierte en un sistema de mayor nivel la información de diferentes sensores y procesos. El valor de la sinergia del sistema estará dado entonces por la cantidad de sensores radar que compongan un sistema de vigilancia. A simple vista, el proceso es lógico y sencillo, pero nuevamente su implementación trae aparejado una serie de consideraciones que desarrollaremos en el presente trabajo.

Radar Primario y Radar Secundario[4]

Los **radares primarios** de los aeropuertos detectan y monitorean el tránsito aéreo dentro del volumen dado por un radio aproximado de unos 110 kilómetros alrededor de cada estación aérea, y una altura que llega a los 20.000 metros. El piloto no puede condicionar ni evitar la reflexión de la energía en el recubrimiento de su aeronave. La aeronave es un blanco pasivo que al recibir el pulso enviado por el Radar lo refleja de acuerdo con las características del material y la forma de su recubrimiento externo.

Por consiguiente la información que colecta el radar primario no depende del conocimiento ni de la voluntad de los tripulantes. El radar primario es independiente o, para ponerlo en términos actuales, es no-dependiente.

Los **radares secundarios** tienen otra finalidad y funcionamiento. Operan dentro de un radio de 360 kilómetros y hasta una altura de 30.000 metros. El radar secundario tiene dos

[4] Fuente: http://www.aviacionargentina.net

componentes activos: el segmento *terrestre*, denominado comúnmente radar secundario y el *aéreo* instalado en las aeronaves denominado transpondedor de a bordo (El radar primario tiene un solo segmento activo: el terrestre). El radar secundario transmite una señal de interrogación que es recibida por todos los transpondedores de las aeronaves que se encuentren dentro de su radio de alcance. Todos los transpondedores que reciben la interrogación responden con una señal codificada que transporta información de identificación de la aeronave (Modo A) y de su altitud barométrica (Modo C). La respuesta del transpondedor se presenta en la pantalla del radar del controlador de tierra, en forma de una etiqueta con la identificación y la altitud barométrica de la aeronave, en la posición relativa de azimut y distancia respecto de la antena del radar.

Si el radar secundario está instalado en el mismo emplazamiento de un radar primario y funcionan complementándose, la etiqueta presentada por el radar secundario se proyecta superpuesta al eco primario (punto luminoso). En la jerga se habla de eco primario y eco secundario. Más allá del alcance, la diferencia fundamental entre ambos tipos de radar es funcional: el primario detecta cualquier avión convencional, al margen de que éste quiera o no ser detectado. El radar secundario, en cambio, no detecta sino que "interroga", y supone una actitud colaborativa del tránsito aéreo.

"Targets": Trafico Cooperativo y no Cooperativo[5]

Es necesario aclarar en esta etapa el concepto de "target" como el objeto de donde "nace" la información y para ello nos adentraremos en los problemas que surgen de la identificación. Para ejercer la soberanía en el espacio aéreo es imprescindible conocer qué, quienes, cómo, cuándo, y por donde se ingresa, se transita, y se abandona el espacio de interés. Este tránsito aéreo ("target") se clasifica en **cooperativo** y **no cooperativo**.

El **cooperativo** es aquel tránsito ordenado por el subsistema ATS (Servicios de Tránsito Aéreo) con el objeto de lograr un coordinado y seguro desplazamiento del mismo, idea vinculada fundamentalmente al concepto de "safety".

El **no cooperativo** es aquel tránsito cuyo movimiento es ajeno al ordenamiento anterior y cuyo desplazamiento puede constituir un riesgo para la seguridad aérea si se aparta de la normativa de tránsito establecida; o atentar contra intereses nacionales y en violación de la propia soberanía, idea vinculada fundamentalmente al concepto de seguridad y defensa nacional. Cabe aclarar que el tráfico **no cooperativo** no es ilegal, pero desde el punto de vista de la vigilancia y control aeroespacial, se presenta como un problema a resolver, en el proceso de identificación.

[5] LA VIGILANCIA AEROESPACIAL EN LA ARGENTINA - Brigadier Mayor (R) Horacio Rodríguez, socio activo y Vicepresidente del Centro Aeronáutico de Estudios Estratégicos – Pag. 7

Tránsito Aéreo[6]

Los tránsitos aéreos internacionales deben ser siempre cooperativos. Un tránsito internacional no cooperativo implica una violación a la soberanía nacional, dado que burla controles migratorios, aduaneros, y de seguridad. Normalmente estos tránsitos están vinculados con actividades delictivas en tiempo de paz; y en tiempo de guerra constituyen vectores enemigos y son objetivos de la defensa aeroespacial. Para distinguir el tránsito no cooperativo del cooperativo, es necesario conocer este último. Por ello el subsistema vigilancia debe tener acceso a la información producida por el subsistema ATS en "tiempo real".

Los subsistemas de control (civil y militar) pueden no pertenecer a una misma organización, en este sentido, el control de tránsito aéreo civil (ATC) es delegado en una organización civil (ANAC - Administración Nacional de Aviación Civil), pero el de vigilancia y control aeroespacial debe necesariamente encontrarse bajo jurisdicción militar por lo anteriormente expuesto

En caso que la situación nacional lo exija (nivel de amenaza o agresión), el sistema permitiría que ambos subsistemas continúen operando bajo un mando unificado a efectos de facilitar la toma de decisiones, ejecutando e impartiendo ordenes y coordinaciones en "tiempo real".

Por otra parte se prevé en el diseño del sistema el concepto de USO FLEXIBLE DEL AEROESPACIO que consiste en considerar que dicho espacio no debe designarse obligadamente como civil o militar, sino que es uno solo y continuo, no así la responsabilidad que se ejerce en el.

El empleo del mismo será asignado atendiendo a las necesidades de los usuarios, sean civiles o militares, sujetos por igual a las normas del Código Aeronáutico; privilegiándose, por sobre todo, la seguridad aérea y la eficiencia operativa.

En síntesis, el aeroespacio es único, continuado, de uso flexible, y requiere, en orden a ejercer eficazmente la soberanía y la defensa en el espacio de interés, de unificación del control en el ámbito aeronáutico militar, sin perjuicio que el subsistema ATS pueda ser administrado por una organización civil.

[6] LA VIGILANCIA AEROESPACIAL EN LA ARGENTINA - Brigadier Mayor (R) Horacio Rodríguez, socio activo y Vicepresidente del Centro Aeronáutico de Estudios Estratégicos. – Pag. 8

El problema tecnológico de los sistemas de vigilancia y control aeroespacial.

Las áreas para controlar el tráfico aéreo son extensas, y esto requiere que para controlar estas áreas se necesiten número de sensores radar (primario y secundario) que van a depender de: el tráfico, la zona geográfica, el tiempo de reacción de los medios defensivos, de los medios ofensivos y de los límites interestatales.

Resuelto el inconveniente de la ubicación y la cantidad de sensores radar para cubrir el área de interés, estos sensores empiezan a producir información sobre los targets de los distintos tráficos aéreos cooperativos y no cooperativos. Toda esta información se transfiere a por medio de enlaces de comunicaciones, al C4I3SR (Comando, Control, Comunicaciones, Computadoras, Inteligencia, Información, Infraestructura, Vigilancia y Reconocimiento) acumulando un volumen de datos tal, que necesariamente se necesitan sistemas automáticos de fusión de datos, para minimizar los tiempos de reacción del sistema.

Es compleja y extensa la problemática, y abarca desde el tipo de emisión del pulso de radar, hasta los sistemas que comparten información para la toma de decisiones. La cantidad de sensores o fuentes de información que realimentan el sistema son variadas, las tecnologías aplicadas, los procesos, los problemas de fusión, las comunicaciones, pero en términos generales podemos agruparlos en dos grandes grupos de problemas que son; la de **integración** y la **interconexión** de datos. Dentro de la integración, haremos abarcativo a todos los procesos de **fusión de datos** independientemente del nivel o tipo de información, y dentro de la interconexión, haremos abarcativo al "**transporte**" de datos entre los sistemas.

Fusión de datos[7]

Primero estableceremos los conceptos de la fusión de datos (DF: Data fusión) tomando como referencia el "Handbook of multisensor data fusion", quien nos introduce a una problemática compleja de tratar. Este tema posee una infinidad de consideraciones, que en el presente trabajo trataremos sin entrar en profundidad matemática.

En los últimos años, se ha centrado la atención en la fusión de datos multisensor para aplicaciones militares y no militares. Estas técnicas de Fusión de datos combinan datos de múltiples sensores y relaciona la información para lograr conclusiones más específicas de las que se podría lograr mediante el uso de un solo sensor.

[7] Handbook of multisensor data fusion - David L. Hall and James Llinas – 2001 - by CRC Press LLC – Pag. 18.

El concepto de fusión de datos multisensor no es nuevo. Como seres humanos y animales han evolucionado, y han desarrollado la capacidad de utilizar múltiples sentidos para ayudarlos a sobrevivir. Por ejemplo, evaluar la calidad de una sustancia comestible que no sea posible utilizando sólo el sentido de la visión; la combinación de la vista, el tacto, el olfato y el gusto es mucho más eficaz. Del mismo modo, cuando la visión se ve limitada por las estructuras y la vegetación, el sentido del oído puede entregar una advertencia avanzada de peligros inminentes. Así, los datos de fusión multisensoriales, naturalmente, realizado por los animales y los seres humanos para evaluar con más precisión el entorno y para identificar las amenazas, mejorando así sus posibilidades de supervivencia.

La fusión de datos de múltiples señores provee varias ventajas sobre los datos de un solo sensor, por ejemplo, si se utilizan sensores idénticos (como por ejemplo, los radares de seguimiento), la combinación de ellos traerá como mejoramiento de la exactitud de los datos obtenidos del “target”, en lo referente a velocidad y posicionamiento. Así también como en la vida animal, la integración de otros tipos de sensores, (infrarrojos, por ejemplo) ayuda a reducir los errores y genera una mayor confiabilidad de los datos producidos.

Definición

Hecha ya la introducción sobre fusión de datos de múltiples fuentes, podemos definirla como un compendio de técnicas multidisciplinares, análogas al proceso cognitivo que realizamos los humanos, para integrar los datos de múltiples sensores (sentidos) con el fin de realizar inferencias sobre el mundo exterior, convergiendo en un conjunto de resultados (reacción).

Niveles de fusión

En general se concibe la fusión como un proceso integral de tratamiento de datos, subdividido en niveles que van desde la captura de los datos, hasta el resultado final, incluyendo la interacción de dichos resultados con el receptor y/u operador.

Nivel 0: Pre-proceso de las fuentes

Los datos de las fuentes son habitualmente pre-procesados para una fusión posterior, filtrando datos o alineándolos temporalmente u otras acciones previas. Este proceso lo lleva a cabo, por lo general, el software asociado a cada uno de los sensores de forma independiente del resto de sensores. Se puede considerar así una pre-fusión. Es a este nivel donde cada uno de los sensores aporta sus datos obtenidos de forma independiente del resto.

Nivel 1: Evaluación del objeto

Combinación de los datos de los sensores para obtener posición, velocidad, atributos y características de la entidad. Siendo la entidad, en transporte, por ejemplo un vehículo, un incidente de tráfico o la congestión. Los algoritmos de este nivel son:

- *Alineación de datos*: Ajustes espacio-tiempo y de unidades para posibilitar un procesamiento posterior
- *Correlación Dato/Objeto*: Asociación y correlación de datos para cada individuo. Para permitir la correcta agrupación de los datos
- *Estimación de posición, cinemática y otros atributos del objeto*: Mediante la combinación de modelos físicos y supuestos estadísticos para la obtención del Vector de Estado.
- *Estimación de la identidad del objeto*: Obtención de la entidad mediante métodos paramétricos (Bayes, Dempster-Shafer), no paramétricos (redes neuronales) o de lógica difusa.

Nivel 2: Evaluación de la situación

Interpretación de los resultados del nivel anterior, en nuestro caso si se determina en el paso anterior que las velocidades son bajas podemos interpretar que estamos en un estado de congestión.

Las técnicas más adecuadas para este nivel son la Inteligencia artificial (IA) y el razonamiento automático. Los algoritmos de este nivel son:

- *Agregación de objetos*: Agregar los datos de cada una de las identidades para una visión global de la situación.
- *Interpretación contextual*: Tener en cuenta los factores externos al estudio que pueden afectar de forma indirecta (En nuestro caso principalmente los factores climatológicos)
- *Evaluación multiperspectiva*: Observación global del problema, desde el exterior e interior.

Nivel 3: Evaluación del futuro

Proyección de futuro de la entidad analizada a partir de la situación actual. Los modelos utilizados para este nivel son la inteligencia artificial, los modelos predictivos, el razonamiento automático y la estimación estadística.

Los algoritmos de este nivel son:

- *Estimación/Agregación de capacidad de fuerza*: Agregación de la información de diversos subsistemas para determinar sus interrelaciones y la robustez del sistema.
- *Estimación de implicaciones*: Resultados de una hipotética acción sobre el sistema
- *Evaluación multiperspectiva*: Análoga al del nivel 2, observación del sistema desde el exterior e interior.

Nivel 4: Proceso refinamiento

Metaproceso que monitoriza todo el proceso de DF para mejorar el rendimiento del proceso en tiempo real, mediante la optimización de la utilización de recursos, la modelización sensorial y la computación de medidas de perfeccionamiento. Este nivel se considera parcialmente fusionado al proceso de fusión, ya que este refinamiento es necesario para el correcto funcionamiento de la fusión y de las operaciones a la que este destinada la DF.

Los algoritmos de este nivel son:

- *Gestión de la misión*: Dirección de los recursos existentes con el fin de obtener los resultados deseados.
- *Predicción de Entidad*: Definir que entidades especificas debe reconocer el Proceso
- *Requerimientos de las fuentes*: Definir la infraestructura necesaria de las fuentes para que puedan identificar las entidades
- *Modelización del rendimiento del sistema*: Definir la estructura del sistema de fusión de datos, la relación entre fuentes, los componentes de procesamiento, etc.
- Control del sistema: Tal como control de multiobjetivos y optimización.

Nivel 5: Refinamiento cognitivo

Mejora del sistema de fusión a partir de la relación Sensor-Procesamiento-Persona. Proyectando modelos en los que la representación de los resultados (ya sean intermedios o finales) permitan al operador identificar posibles errores en el

procesamiento, y que este previamente haya podido detectar errores en los datos suministrados por los sensores. Sin considerar que tienen la entidad de los niveles antes mencionados hay que tener en cuenta también:

- *La gestión de la base de datos*: Es un punto clave dada la gran cantidad de datos que se manejan durante el proceso. Para desarrollar esta función será necesario un considerable esfuerzo computacional, destacando que el software comercial habitual es incapaz de gestionar el problema completo de fusión

- *Interacción de la persona con el ordenador*: Este elemento, considerado externo a la fusión, es importante en el proceso de fusión. Ya que una correcta interfaz del sistema, será clave para el refinamiento cognitivo.

Ventajas y desventajas de la Fusión de datos

Las ventajas de la fusión son:

- **Robustez operacional**: Ya que un sensor puede aportar información cuando los otros no están operativos o solo parcialmente operativos.

- **Cobertura espacial extendida**: La correcta fusión de los datos de los sensores distribuidos por el espacio dan una mejor resolución que uno solo de ellos.

- **Cobertura temporal extendida**: Un sensor puede obtener información cuando otros no o de forma más continua.

- **Aumento fiabilidad**: Un buen proceso de fusión puede confirmar la veracidad de una información, dada la inherente redundancia de los datos de las fuentes.

- **Reducción ambigüedad**: La fusión de la información de múltiples sensores permite reducir el número de hipótesis a realizar

- **Mejora de detección**: Una correcta fusión facilita la detección de un suceso, gracias a la redundancia de los datos.

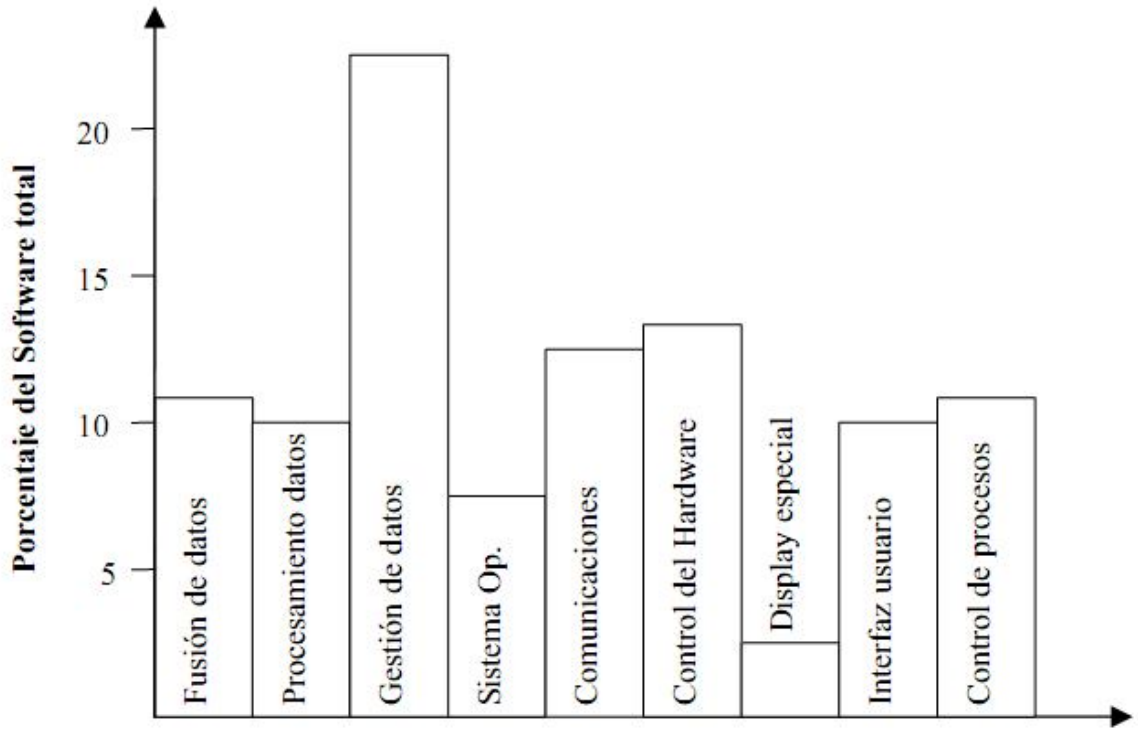
Sus limitaciones:

- **Calidad y número de sensores**: Como hemos visto anteriormente, la calidad del sensor y su número determinará de forma importante la calidad del resultado final de la DF.

- **Imposibilidad de corregir errores de base**: El proceso de DF no puede corregir errores en el pre-procesamiento de los datos. Es decir no hay corrección aguas arriba de la inferencia, si bien el Nivel 4 procederá a un refinamiento de los resultados, pero ya a partir del nivel 1.

- **La calidad de la información sobre los sensores**: Si la información que tenemos sobre los sensores (su rendimiento, datos que pueden aportar) es pobre o incorrecta, también lo serán los resultados de la DF.
- **Inexistencia del algoritmo de DF ideal:** Cada algoritmo tiene sus fortalezas y debilidades debiendo el gestor elegir el más apropiado para el fin deseado.
- **Falta de datos de entrenamiento:** Nunca habrá suficientes datos para entrenar al sistema, es decir los recursos son limitados.
- **Dificultad de cuantificación del rendimiento**: No existen parámetros claros y globales para determinar si un sistema de DF es mejor que otro. Queda así en manos del gestor una correcta valoración
- **Dinamismo del proceso**: Es imposible analizar el proceso como algo estático, siendo así difícil de valorar su rendimiento de forma generalizada, ya que dependerá de su grado de aprendizaje y de los datos disponibles en ese momento.

También hay que considerar el esfuerzo de cálculo y memoria que supone la gestión de un sistema de múltiples fuentes de datos y su consiguiente fusión. Si bien, según Hall y McMullen (2004), la mayor parte del esfuerzo se emplea en la gestión de los datos.



Multi-Radar Tracker (MRT)

El proceso de fusión de datos, es producto de tecnología de vanguardia, y seguramente será una ciencia en constante crecimiento. Esta ciencia, trata de procesos de software de alta tecnología, y para mantener una referencia a esto, diremos que si la computadora (COTS - commercial-off-the-shelf) que corriera este software capaz de integrar estos datos costara unos U$S 20M, el software valdría alrededor de unos U$S 300M. En la figura desmitificamos un poco este tipo de equipamiento, producido por Northrop Grumman[8]. Solo para tener en cuenta las capacidades de un MRT diremos que tiene capacidad de integrar unos 32 radares, procesar hasta 1000 "targets", esto nos da una idea aproximada de la capacidad de procesamiento.

9

¿Qué hace un MRT? Es la pregunta a responder, a la que nos limitaremos a comentar el siguiente caso a título de ejemplo, para dar una idea más clara sobre el tema. Imaginemos lo siguiente, tenemos un "target" el que es captado por dos radares en distintos lugares al mismo tiempo, en tiempo real. Estos transmiten los datos referidos al mismo "target", y esta información llega al MRT, quien a través de un proceso de fusión, determina que se trata de un mismo "target". A la salida del MRT, tendremos integrada la información de los dos radares. ¿Podemos decir que el MRT es un integrador de señal? Si, a modo de entendimiento, pero es algo más complejo. Igualmente pensemos que el MRT solo es un escalón la Fusión de Datos, en la integración de un sistema de control y vigilancia aeroespacial, que más adelante ubicaremos dentro de un esquema. La siguiente pregunta para seguir escalando en la comprensión, será, ¿Qué datos necesita el MRT para realizar la integración? ¿Y cómo se conecta el MRT con el sensor radar? Pasemos ahora a la segunda problemática del trabajo.

[8] Fuente: http://www.es.northropgrumman.com/index.html

[9] Fuente: http://www.es.northropgrumman.com/solutions/multiradartracker/

Interconexión

Ya definimos interconexión, como el "transporte" de datos entre sistemas. Esta definición necesita seguramente responder algunos interrogantes tales como: ¿Que información debería canalizarse sobre los vínculos que enlazan el sistema? ¿Qué protocolos de comunicación son los que se necesitarían para que la red funcione?, son algunos de los interrogantes que trataremos de responder, para clarificar el tema de la interconexión.

En principio, en la Argentina se desarrolló el PRU (siglas de **P**rotocolo de **R**adar **Ú**nico), un protocolo diseñado para responder el problema del transporte de datos entre sistemas de radar y las consolas remotas. Este protocolo fue uno de los primeros en funcionar y explotar las capacidades de controlar un sector radar, a través de un vínculo digital. Pero a medida que se empezó a escalar e integrar, se vió que se necesitaba un estándar mas probado y escalable, que permitiera la interconexión de más de un nodo, de más de una consola, de más de un sistema de integración y que posea la flexibilidad de embeber sistemas militares y sistemas civiles que potencien el sistema de control y vigilancia aeroespacial manteniendo costos y la eficacia adecuada para trabajar en el ambiente aeroespacial.

De aquí el debate y las preguntas, tales como ¿es necesario crear dos sistemas independientes que funcionen para administrar (aplicación civil) y controlar (aplicación militar) el espacio de jurisdicción nacional? ¿Cuales serian los beneficios o los problemas que suscitarían este tipo de sistemas? Sin adentrarnos mucho en los pormenores del análisis, diremos que por una cuestión meramente económica es más rentable para el Estado Nacional que los dos sistemas (civil y militar) convivan en un mismo espacio. Este problema no era excluyente a la Argentina, así que se realizaron estudios de cómo otros países habían solucionado este inconveniente.

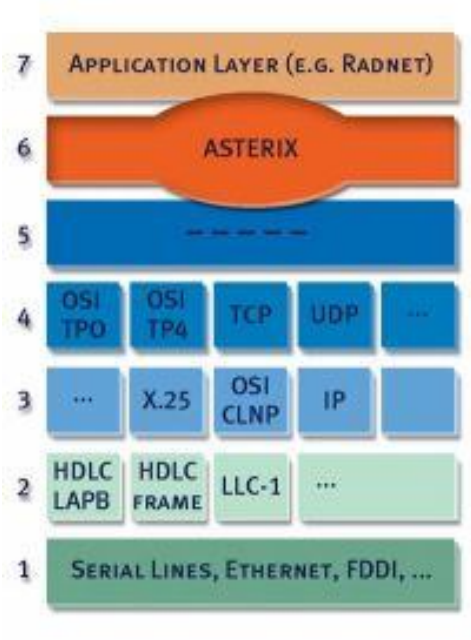
Para ese entonces la Comunidad Europea poseía un estándar abierto de comunicaciones que permitía interconectar sus sistemas civiles y militares, al que denominó ASTERIX,

¿Qué es Asterix?

ASTERIX es un protocolo estándar, abreviatura de: **A**ll Purpose **ST**ructured **E**urocontrol Su**R**veillance **I**nformation E**X**change[10], creado por Eurocontrol, para la estandarización del intercambio de información. Esta información se intercambia a través del formato de datos de mensajes binario, entre sistemas de vigilancia y control aeroespacial, permitiendo la transmisión de información "viaje" entre sistemas automatizados. ASTERIX define

[10] EUROCONTROL STANDARD DOCUMENT FOR SURVEILLANCE DATA EXCHANGE (Part 1) - SUR.ET1.ST05.2000-STD-01-01 - EUROPEAN AIR TRAFFIC MANAGEMENT - Edition : 1.30 Edition Date : November 2007 – Fuente: http://www.eurocontrol.int/asterix/public/subsite_homepage/homepage.html

entonces, la estructura de los datos que se intercambian, sobre el medio de comunicación, codificando cada bit de información, y la organización de la estructura de datos intercambiados, definido como block de datos. Especificando un poco más en el área de comunicaciones, ASTERIX es un protocolo de capa de presentación, del modelo OSI[11] (International Standards Organization (ISO) Standard 7498).



Esta característica nos da una flexibilidad importante, ya que puede trabajar sobre cualquier protocolo de comunicaciones, ya sea para redes Local Area Network (LAN), o Wide Area Network (WAN), independientemente de la tecnología CORE[12] que usemos.

Consideremos que hay información común a todos los sistemas (por ejemplo, la posición en Modo-A y Modo-C del trasnponder[13]), ASTERIX especifica el requerimiento mínimo de información para que los datos puedan ser intercambiados entre sistemas heterogéneos. Esto permite que la comunicación entre dos sistemas diferentes (incluso ubicados en diferentes países) sea realizable; ejemplo de ello, y en el marco regional podemos

[11] El *modelo de referencia de Interconexión de Sistemas Abiertos* (OSI, Open System Interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

[12] Building the Carrier-Class IP Next-Generation Network – CISCO SYSTEMS (White Paper) - C11-331938-00 02/06

[13] Fuente: http://es.wikipedia.org/wiki/Transpondedor

mencionar el MEMORANDO DE ENTENDIMIENTO PARA LA INTERCONEXIÓN DE LOS SISTEMAS AUTOMATIZADOS DE ARGENTINA Y BRASIL.[14]

Cabe aclarar que para simplificar la transmisión de información entre sistemas, y hacerla más sencilla, el RDE-TF (Surveillance Data Exchange Task Force[15]) estandarizó la información en "data ítems", necesarios para que el sistema funcione, a la agrupación de estos "data ítems", la definió como categorías. Estas categorías están agrupadas en 256 categorías distintas, definidas en la tabla del ANEXO 2 para una mayor comprensión.

Alcance del ASTERIX

Asterix ha sido desarrollado para un fácil intercambio de información entre los sistemas de vigilancia aeroespacial de distintos países. Por tanto el principal usuario de ASTERIX han sido los Centros de Control de Tráfico Aéreo (Air Traffic Control - ATC). Pero ASTERIX es también usado para ayudar a las industrias a estandarizar y madurar las nuevas tecnologías contribuyentes a el control y vigilancia aeroespacial, integrado nuevos sensores y automatizando sistemas tales como el ARTAS (ATM suRveillance Tracker And Server[16]), RMCDE (Radar Message Conversion and Distribution Equipment[17]). Asterix, es también un estándar evolutivo, diseñado así, para absorber el incremento de volumen de trafico aéreo permitiendo la incorporación de nuevas tecnologías, absorbiendo, y coexistiendo con los sistemas actuales, sin que con ello decaigan las prestaciones del servicio con una alta seguridad en el empleo de información.

Reseña histórica de ASTERIX

Hasta la década de los 80, cada Administración Nacional Europea, desarrolló su propio formato para la distribución de los datos entre los centros de control de tráfico aéreo, y el resultado de duplicar el esfuerzo en el intercambio de datos radar, fue un tema complicado de resolver durante muchos años. La necesidad de un formato común europeo de datos se hizo evidente entonces y un ejemplo de la presentación de un formato estándar presentada por el UAC de Maastricht a la ex Panel de Especialistas en Sistemas de Radarl (RSSP) en 1984, fue allí donde nació el ASTERIX. En 1988, fue presentado el manual de Asterix, con

---

[14] MEMORANDO DE ENTENDIMIENTO PARA LA INTERCONEXIÓN DE LOS SISTEMAS AUTOMATIZADOS DE ARGENTINA Y BRASIL - Fecha de efectividad: 17 SEP. 2009 - **Por Argentina**: Eduardo Rodino (Director Nacional de los Servicios de Navegación Aérea) ANAC - **Por Brasil**: Murilo Albuquerque Loureiro (Adjunto División Coordinación Técnica) DECEA Fuente: http://www.lima.icao.int/

[15] EUROCONTROL Fuente: http://www.eurocontrol.int/working_arrangements/public/standard_page/surt_rde_tf.html

[16] EUROCONTROL Fuente: http://www.eurocontrol.int/artas/public/subsite_homepage/homepage.html

[17] EUROCONTROL Fuente: http://www.eurocontrol.int/working_arrangements/public/standard_page/surt_rug.html

estructura similar actual con aplicaciones para radares monopulso y radares meteorológicos.

En 1991, la RSSP. De allí en adelante, los distintos equipos de trabajo que se vieron involucrados en el trabajo de este protocolo, fueron integrados y estandarizando, en lo que hoy se conocemos.

La filosofía del protocolo Asterix puede ser descripto en dos frases cortas:

“Distribuir todo lo que se requiera” y

“No transmitir mas de lo necesario”.

Bajo este miramiento, el protocolo Asterix ha sido diseñado como una forma flexible de codificación de información de vigilancia, para el intercambio de información. Y como característica distintiva principal, es la agrupación de la información en categorías de datos y la generación de mensajes flexibles con el fin de ahorrar ancho de banda en la transmisión.

Esta categorización permite a los diseñadores de sistemas, implementar exactamente lo que necesitan, sin sobrecargar las redes de comunicaciones con información innecesaria. Existen 256 categorías de datos, los cuales están agrupado en:

- Data Categories 000 to 127 for standard civil and military applications;
- Data Categories 128 to 240 reserved for special civil and military applications;
- Data Categories 241 to 255 used for both civil and military non-standard applications.

PMF – Principio Militar Fundamental.

Pretendemos que el Asterix sea aceptado como el protocolo ideal para la integración de los sensores radar en el accionar militar conjunto. Ahora bien, para interiorizarnos más en la problemática de la interconexión, desde un punto de vista militar, aplicaremos el Principio Militar Fundamental (PMF), a este protocolo, para observar los distintos enfoques. ¿Que es entonces el PMF?, “del estudio de la historia de la guerra, se han extraído innumerables principios se la conducción, luego de haberlos analizado, se ha adoptado para el análisis integral de las operaciones aéreas en la Fuerza Aérea Argentina el Principio Militar Fundamental (PMF), el que contempla todos los factores contenidos en los otros principios

y todas las condiciones conocidas vinculadas con las operaciones".[18]. Apliquemos este principio a las comunicaciones.

Acción eficaz y dirigida contra OOMM Correctos.

En este caso para que la acción sea eficaz por parte del protocolo, debe primero ser capaz de transportar la información de los sensores radar a los nodos de fusión de datos, para ello se deberán tener en cuenta a los siguientes aspectos: El Rendimiento, la Disponibilidad, la Escalabilidad, y las normas de compatibilidad. El rendimiento estará asociado a como el Asterix, transporte la información de un punto a otro, y en este sentido la flexibilidad del Asterix está siempre optimizada, ya que solo transporta la información necesaria, como ya describimos anteriormente dentro de sus características. El problema radicará en el estudio del entorno en el cual el Asterix estará trabajando. En ese aspecto habrá que estudiar los distintos servicios que en el nodo radar existan (canales de voz, datos para el manejo de la estación, datos para el servicio de seguridad físico, telemando, entre otros), a fin de que el rendimiento del Asterix no decaiga, o se vea comprometido. De esto se deriva que la red debe entonces soportar QoS[19]. QoS o Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

Otro aspecto derivado del rendimiento, es el requerimiento de ancho de banda BW, que necesite el protocolo Asterix para su funcionamiento. El protocolo Asterix, en comparación a las viejas transmisiones de video que se necesitaban para transportar información de los datos radar (256k o más), está dentro del 2% al 10% de este Bw; siempre dependiendo de la aplicación y de la información que se necesite. En lo que se refiere a la disponibilidad, estará asociado pura y exclusivamente a los medios de enlace, y la vulnerabilidad que estos tengan en referencia a la seguridad. Respecto de la Escalabilidad, el Asterix, no posee limitación en cuanto al servicio ya que es un protocolo flexible e integrador de nuevas tecnologías.

---

[18] Curso de Comando y Estado Mayor (CCEM – FAA) Edición 2008. Estado Mayor - ParteII tomo I – Capitulo V.

[19] QoS : El avance progresivo de las redes convergentes ha hecho que nuestras redes de datos brinden soporte de conectividad a tráfico con requerimientos de performance muy diferentes: VoIP, videoconferencias, navegación web, transacciones sobre bases de datos, sistemas de soporte de la operación de la empresa, etc. Cada uno de estos tipos de tráfico tiene requerimientos diferentes de ancho de banda, condiciones diferentes de delay, pérdida de paquetes, etc. Poder dar respuesta a diferentes requerimientos de performance sobre una misma infraestructura de red supone la implementación de Calidad de Servicio (QoS). – .- Internetworking Technologies Handbook, Third Edition – Cisco Systems - Cisco Press – Febrero 2001 – Capítulo 49 Pag 699

Correcta Distribución del poder combativo.

La correcta distribución del poder combativo, entendemos que estará enfocada en dos capacidades importantes:

La Capacidad que se posea para modificar la red y su funcionalidad en tiempo real, que habla de la capacidad que se posea para modificar la estructura de red o modificar sus patrones de trafico si un componente de red se ve afectado. Ya que el protocolo Asterix cumple los estándares OSI, esta capacidad estará enfocada a la elección del protocolo de capa de red, que utilicemos. Esta característica nos da otro punto de diseño importante para la los criterios de construcción de la red y es el diseño teniendo en cuenta las posibles caídas de los distintos nodos que lo componen no debe afectar al su normal funcionamiento.

Capacidad que se posea para integrar sensores de otras fuentes. Integrar un nuevo sensor no es un inconveniente menor, si no se realizó el estudio y se realizó el trabajo de integrarlo electrónicamente. Pero si el equipamiento posee la interfaz adaptada o dentro de su descripción técnica la interface y soporta el protocolo Asterix, teniendo en cuenta el bajo ancho de banda que insume, será fácil enlazarlo e integrarlo a la red. De este análisis sacamos en conclusión que debe existir un estándar a nivel operacional de todos los sensores que contribuyan en la vigilancia y control aeroespacial.

Desde posiciones relativas favorables.

¿Qué posición relativa favorable tiene que tener este tipo de protocolo, para absorber las exigencias de la integración de los distintos sensores? Desde el punto de vista tecnológico, debería poseer un porcentaje de las redes con capacidad ociosa para absorber los requerimientos de ancho de banda necesarios para poder integrar uno o mas sensores, sin que con ello afecte su capacidad. Ya que el ancho de banda es despreciable en comparación con otros servicios (servicios de voz o video), no será necesario guardar importantes anchos de banda para la integración. Otro punto a analizar es la ubicación de los sensores (aéreo, marítimo y terrestres) (móviles o fijos), lo más prudente de instalar sin que genere mucha servidumbre son los enlaces satelitales, ya que poseen una fuerte movilidad, no generan una cadena de servicio ni estructura para mantener la red como las redes de medios físicos, siempre y cuando la red sea extensa, o el sensor se encuentre en una posición comprometida (cerros, mares interiores, etc.).

Otro punto a desarrollar es que los nodos cuenten con la infraestructura y flexibilidad suficiente como para poder absorber el tráfico que generen los nuevos sensores, y la posibilidad de poder manejar QoS en la red. Actualmente la mayoría de las redes poseen esta característica, y la estructura para hacerlo, si bien este servicio es propietario tecnológico de la capa de red, actualmente existen tecnologías (aun no masivas) que

trabajan la QoS, a nivel capa de enlace como lo son las tecnologías MPLS[20]. Trabajar con este tipo de protocolos presenta una serie de consideraciones en cuanto a la infraestructura y su diseño matricial, y no deberían ser consideradas maduras como para implementarlas como redes de integración de sensores radar.

Adecuada libertad de acción.

"Bien se sabe, que la necesidad tiene cara de hereje…". Existe una fina línea entre la capacidad libertad de acción dentro del ámbito de las comunicaciones y la posibilidad de introducir nuevos focos de conflicto y problemas en la red, no solo asociados a los problemas seguridad (un tema bastante profundo y por lo general poco atendido), sino además los inconvenientes de integración de tráfico, compatibilización de interfaces, asociados a los recursos humanos y materiales necesarios para mantener esta libertad. Un tema de debate es el acceso de datos a través de medios como internet (la mala palabra…) como vinculo asociado a poder transportar por este medio datos que por la red establecida no podría hacerse. La historia militar está llena de casos en donde la red de internet y no convencionales (que son civiles) se utilizaron para transmitir datos o comunicaciones de operaciones militares, cuando los nodos CIC3 fueron destruidos. Uno de los autores que estudia y manifiesta esto fue Robert Pape[21], en la guerra de Kosovo. Siempre existe la posibilidad de poder transmitir datos por otra vía que la formal. Lo que nadie cuenta es que para mantener "formalmente" este tipo de redes no convencionales, se necesita una estructura humana de recursos y medios de importancia, sumado a ello la educación y el entrenamiento constante.

Por mucho tiempo se han desarrollado políticas restrictivas que en su sano juicio, prohibieron el acceso o duplicaron las redes con tal de no integrarlas, por el miedo a la seguridad en el manejo de la documentación. Pero el avance de las tecnologías de internet y el cada vez más económico acceso a internet, parecen pasar demoledoramente este tipo de prejuicios. Lo que hace unos 10 años nos parecía imposible o de tecnología de un mundo de ciencia ficción e inalcanzable, esta hoy a nuestro alcance, producto de la evolución de procesos masivos. Esto hace que dada la necesidad de integrar un sensor a nuestra red en situaciones marginales, nos sea más fácil acceder por vías no formales a nuestros nodos formales.

---

[20] MPLS (Multi-Protocol Label Switching) es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay o ATM. Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red.- Internetworking Technologies Handbook, Third Edition – Cisco Systems - Cisco Press – Febrero 2001 – Capitulo 28 Pag 433

[21] Bombing to Win: Air Power and Coercion in War (Cornell Studies in Security Affairs) – Robert A. Pape. – Cornell University Press - 1996

Un punto de importancia en el tema de la seguridad, es la capacitación de los recursos humanos, en su entrenamiento, conocimiento, capacitación innovadora, y motivación, para darle flexibilidad a la red y sus accesos, sin ellos la adecuada libertad de acción estará atada a la teoría de caos.

Consideraciones sobre seguridad (Adecuada libertad de acción)

Nadie puede discutir hoy en día que la seguridad de las Tecnologías Informáticas es un componente necesario de los sistemas de información y tanto los entes públicos como los privados, empiezan a dedicar recursos materiales y humanos cada vez más significativos a esta área.

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. Ejemplo de ello es lo que sucedería si en la pantalla donde se plasma la información sobre la vigilancia aeroespacial, fallara en medio de las operaciones, o lo que sucedería si el sistema no presentara la confiabilidad suficiente para tomar decisiones en un marco de conflicto. La falta de medidas de seguridad en las redes es un problema que está en crecimiento, y cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red. A la hora de plantearse en qué elementos del sistema se deben de ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

Protección de los sistemas de transferencia o transporte. En este caso, el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura al usuario final de la información de forma lo más transparente posible.

Aplicaciones seguras extremo a extremo. Si pensamos, por ejemplo, en el correo electrónico, consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío. De esta forma, el mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos.

En ambos casos, un problema de capital importancia es la gestión de passwords. Este problema es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro.

Las políticas de seguridad informática (PSI) como base de la administración de la seguridad integral.

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos. Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado[22] que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí mismas no constituyen una garantía para la seguridad de la organización.

Al crear una política de seguridad de red, es importante entender que la razón para crear tal política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger y que algunos recursos son más importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A pesar de la cantidad de publicidad sobre intrusos en una red, varias encuestas indican que para la mayoría de las organizaciones, la pérdida real que proviene de los "**miembros internos**" es mucho mayor (tal cual se ha explicado anteriormente).

El análisis de riesgos implica determinar lo siguiente:

- Qué se necesita proteger
- De quién protegerlo
- Cómo protegerlo

Otro tipo de ataque es el de "fuerza bruta", que consiste simplemente en realizar todas las combinaciones posibles de caracteres hasta hallar el password. En el siguiente cuadro podemos ver el tiempo de búsqueda de una password de acuerdo a la longitud y tipo de

[22] Grafico: Anexo 5

caracteres utilizados. Se supone una velocidad de búsqueda de 100.000 passwords por segundo.

Long. En caracteres	26 letras (minúsculas)	36 letras y dígitos	52 (mayúsculas y minúsculas)	96 Todos los caracteres
6	50 minutos	6 horas	2.2 días	3 meses
7	22 horas	9 días	4 meses	23 años
8	24 días	10.5 meses	17 años	2287 años
9	21 meses	32.6	881 años	219.000 años
10	45 años	1159 años	45.838 años	21 millones de años

Como la información que maneja el SINVyCA está ajustada a valores temporales muy cortos (del orden de 5 minutos), entendemos que de nada serviría al actor beligerante tener información de un movimiento de aeronaves 5 horas tarde de realizada la operación. "Robar" información del sistema, tal vez no sea la forma más rentable de vulnerar al sistema de control y vigilancia aeroespacial. Es por ello que se entiende que de realizarse un ataque al sistema, estará más fuertemente vinculado a interrumpir las comunicaciones o un ataque de denegación de servicio[23] (DoS), que la ruptura del encriptado.

Interconexión de sensores de las distintas fuerzas. Un problema del EMC – C6.

Describimos anteriormente que la problemática del SINVyCA, podía agruparse en dos áreas (interconexión e integración), y entendemos que la sinergia de la integración de los sensores de las distintas fuerzas contribuye positivamente en el manejo y administración de los medios en el aeroespacio. Ahora bien si la integración de los datos es ámbito de competencia de la FAA, como órgano entendido y legalmente competente en la evaluación de la información, pendiente queda entonces el tema de la interconexión entre los distintos sensores en el ámbito conjunto. El EMC es responsable de todas aquellas actividades que se realicen entre las distintas fuerzas con distintos grados de participación, por lo que derivamos que será competencia del EMC –C6 "la de Fijar los conceptos doctrinarios y las normas básicas que gobiernan a las comunicaciones conjuntas para facilitar el ejercicio del comando" [24] en base a la experiencia y competencia de la Fuerza Aérea, y de este modo

[23] Fuente: http://es.wikipedia.org/wiki/Ataques_de_denegación_de_servicio

[24] La publicación "COMUNICACIONES PARA LA ACCIÓN MILITAR CONJUNTA", PC 16-01 (Confidencial)

integrar otros sensores; además de participar en forma activa en los procesos de compra de sensores radar que en un futuro se adquieran, para poder integrarlos al SINVyCA.

¿Pero en base a que necesidades especificas se realiza la integración? [25]

- En la necesidad de que cada componente dentro de la fuerza conjunta, pueda operar una variedad de aviones y sistemas de armas, tanto de alta y baja velocidad, giratoria y de ala fija (tripulados y no tripulados).
- En la necesidad de que cada componente pueda utilizar el espacio aéreo con la máxima libertad.
- En la necesidad de que las actividades de control del espacio aéreo se realicen en congruencia con las operaciones de defensa aérea, y se puedan integrar y sincronizar con las armas superficie-aire de defensa y los aviones de defensa aérea para lograr la máxima eficacia.
- En la necesidad de discriminar de manera rápida y eficaz operaciones aéreas de: amigo, enemigo y neutrales.
- En la necesidad de que el sistema de control del espacio aéreo que responda a las necesidades de la fuerza conjunta a través de las redes del sistema de control del espacio aéreo, con capacidad para soportar el tráfico de alta densidad y el aumento de las operaciones cuando sean requeridos por el comandante de la fuerza conjunta.
- En la necesidad de una estrecha coordinación e integración de las operaciones de las fuerzas de superficie, el apoyo a los incendios, las operaciones aéreas, operaciones de defensa aérea, operaciones especiales, y actividades de control del aeroespacio.
- En la necesidad de reconocer los niveles de saturación y las limitaciones de las redes de control del espacio aéreo.
- En la necesidad de incorporar, en detalle, un plan integrador de los medios de guerra electrónica, aviones de combate y misiles, para asegurar que los elementos defensivos no inhiban o degraden las capacidades ofensivas de los propios componentes
- En la necesidad de garantizar que la red de control del espacio aéreo de control conjunto sobreviva y sea eficaz, frente a un ataque enemigo.

[25] Joint Publication 3-52 - Joint Airspace Control - 20 May 2010

- En la necesidad de ofrecer las máximas oportunidades para emplear medidas de engaño.

- En la necesidad de estandarizar los datos de las comunicaciones, el formato y los requisitos, en las operaciones multinacionales para reducir la posibilidad de diferencias de interpretación, de traducción, o la aplicación de los procedimientos de control del espacio aéreo durante las operaciones multinacionales.

- La necesidad de apoyar las operaciones de 24 horas en bajo todo tipo de climas y condiciones ambientales.

Además, una de las principales razones de una estrecha coordinación entre el control del espacio aéreo (FAA), control del tráfico aéreo civil (ANAC – OASI), y elementos de defensa aérea (terrestres o marítimos), en lo referente a las comunicaciones en tiempos de conflicto, es reducir el riesgo de fratricidio y aumentar la eficacia de la defensa aérea integral. Los requisitos de identificación para el control del espacio aéreo deben ser compatibles con los de la defensa aérea. El control del espacio aéreo, la defensa aérea, el control del tráfico aéreo civil, el apoyo a los procedimientos, los equipos, y la necesidad de una terminología en común, buscan ante todo, un manejo del poder aeroespacial conjunto de forma integrada e interoperable.

Debemos agregar que si bien es un tema relativamente nuevo, tanto como para la F.A.A., en la relación con el A.N.A.C (Administración Nacional de Aviación Civil) ex Comando de Regiones, el EMC – C6 deberá absorber en el corto plazo, la responsabilidad de interactuar con el ente recientemente creado, en todo lo referente a la integración de la red de control de tráfico civil con la red propia.

Esto abre un interrogante serio, ya que los medios de control aeroespacial se basan en la información brindada por el ANAC, a fin de establecer una correcta identificación de los tráficos cooperativos, por lo que el atentado o afectación a las redes civiles en caso de conflicto podrían interferir en los sistemas de control y vigilancia aeroespacial. ¿Es esto una responsabilidad del EMC – C6 en caso de conflicto? ¿Qué medidas paliativas podrán tomarse para evitar esto? Lamentablemente lo ocurrido el 11 de septiembre en la historia aeronáutica, suma como ejemplo que los absurdos, deben ser tratados como suposiciones, y no descartadas con una visión simplista.

CONCLUSIONES

Con el avance de la tecnología, principalmente el software y la conectividad, se han desarrollado una importante cantidad de aplicaciones a costos significativamente por debajo de los beneficios que trae aparejado su aplicación. En lo referente a la Integración, los procesos de fusión de datos se muestran maduros y ya poseemos en el mercado

comercial y regional antecedentes sólidos de este desarrollo de ingeniería. En lo referente a la Interconexión, el protocolo Asterix, es sin duda, un punto de apoyo a la estandarización de los medios de detección en el ámbito específico, conjunto y nacional. La planificación para la migración de la actual situación a una situación en donde se integren todos los sensores con capacidad de reconocimiento aeroespacial es vital. Respecto al problema de las asignaciones de las responsabilidades por parte del EMC – C6, olvidado como un elemento clave en el accionar militar, es de valor ponderante en la integración de esta propuesta, es por ello que se lo ha tratado en el presente trabajo.

Las ventajas presentadas, muestran un conjunto de puntos que habrá que desarrollar para implementar esta tecnología, (que no requiere inversiones importantes) como lo es la estandarización de este protocolo, que ayudara a converger la información para trabajar en un modelo de dirección conjunta. Otro punto importante es que la aplicación de este estándar, no solo favorecerá al ámbito de conducción específico de la F.A.A., sino que también en el ámbito de responsabilidad de la Armada en el trabajo del Control Aéreo Táctico para una Operación Aeronaval. Desde este miramiento la transferencia de medios compatibles con esta tecnología, permitirán a la Armada la posibilidad de integrar estos medios a su operación.

Además, actualmente a nivel nacional se llevan adelante proyectos a través del INVAP de una envergadura significativa, como para mostrarnos una clave importante en el desarrollo tecnológico nacional de los próximos 20 años; no aprovecharla sin duda alguna, será dejar pasar una oportunidad de volver a insertarnos no como instrumento militar, sino como valor patrimonial de la Nación Argentina.

Bibliografía y Referencias.

- ✓ An Introduction to Multisensor Data Fusion / DAVID L. HALL, SENIOR MEMBER, IEEE, AND JAMES LLINAS. PROCEEDINGS OF THE IEEE, VOL. 85, NO. 1, JANUARY 1997
- ✓ Cobb, A. (1998). Thinking About the Unthinkable: Australian Vulnerabilities to a High-Tech Risks. Research paper 18 1997-98. Department of Australian Parliamentary Library, Canberra.
- ✓ Handbook of multisensor data fusion / David L. Hall and James Llinas. (Electrical engineering and applied signal processing).
- ✓ Hall D L 1992 Mathematical techniques in multisensor data fusion (Boston: Artech House)
- ✓ Information Warfare: Using the Viable System Model as a framework to attack organisations / Bill Hutchinson School of Management Information Systems , Edith Cowan University Western Australia.
- ✓ JP 3-16, Joint Doctrine for Multinational Operations.
- ✓ JP 3-30, Command and Control for Joint Air Operations.
- ✓ JP 3-60, Joint Doctrine for Targeting.
- ✓ Organización de Aviación Civil Internacional -Grupo Regional de Planificación y Ejecución CAR/SAM (GREPECAS) Tercera Reunión del Grupo de Tarea sobre Vigilancia (SUR/TF/3) Ciudad de México, México, 10 al 11 de septiembre de 2009.
- ✓ Pohl, C.; Van Genderen, J.L. Multisensor image fusion in remote sensing: concepts, methods and applications. Int. J. Remote Sens. 1998, 19, 823–854.
- ✓ Proyecto FAS 1232 / 1230 – Dirección General de Investigación y Desarrollo – F.A.A.
- ✓ RADAR HANDBOOK / Merrill I. Skolnik Editor in Chief, Third Edition.
- ✓ Tracking filter and multi-sensor data fusion / G GIRIJA, J R RAOL , R APPAVU RAJ, and SUDESH KASHYAP.

ANEXO1

Clasificación de los sistemas de radar

Se puede hacer una clasificación general de los radares en función de una serie de aspectos básicos:

Según el número de antenas

- **Monoestáticas jp**(jump ping): una sola antena transmite y recibe.
- **Biestático**: una antena transmite y otra recibe, en un mismo o diferentes emplazamientos.
- **Multiestático**: combina la información recibida por varias antenas.

Según el blanco

- **Radar primario**: funciona con independencia del blanco, dependiendo solamente de la RCS del mismo.
- **Radar secundario**: el radar interroga al blanco, que responde, normalmente con una serie de datos (altura del avión, etc). En el caso de vehículos militares, se incluye el identificador amigo-enemigo.

Según la forma de onda

- **Radar de onda continua (CW)**: transmite ininterrumpidamente. El radar de la policía suele ser de onda continua y detecta velocidades gracias al efecto Doppler.
- **Radar de onda continua con modulación (CW-FM, CW-PM)**: se le añade a la señal modulación de fase o frecuencia con objeto de determinar cuando se transmitió la señal correspondiente a un eco (permite estimar distancias).
- **Radar de onda pulsada**: es el funcionamiento habitual. Se transmite periódicamente un pulso, que puede estar modulado o no. Si aparecen ecos de pulsos anteriores al último transmitido, se interpretarán como pertenecientes a este último, de modo que aparecerán trazas de blancos inexistentes.

Según su finalidad

- **Radar de seguimiento**: es capaz de seguir el movimiento de un blanco. Por ejemplo el radar de guía de misiles.
- **Radar de búsqueda**: explora todo el espacio, o un sector de él, mostrando todos los blancos que aparecen. Existen radares con capacidad de funcionar en ambos modos.

Según su frecuencia de trabajo

Nombre de la banda	Frecuencias	Longitudes de onda	Observaciones

HF	3-30 MHz	10-100 m	Radares de vigilancia costera, vigilancia OTH (over-the-horizon)
P	< 300 MHz	1 m+	'P' de "previo", aplicado de forma retrospectiva a los sistemas radar primitivos
VHF	50-330 MHz	0.9-6 m	Vigilancia a distancias muy elevadas, penetración en el terreno
UHF	300-1000 MHz	0.3-1 m	Vigilancia a distancias muy elevadas (ej: detección de misiles), penetración en el terreno y a través de la vegetación
L	1-2 GHz	15-30 cm	Distancias elevadas, control de tráfico en ruta
S	2-4 GHz	7.5-15 cm	Vigilancia a distancias intermedias. Control de tráfico en terminales. Condiciones meteorológicas a largas distancias
C	4-8 GHz	3.75-7.5 cm	Seguimiento a distancias elevadas. Meteorología
X	8-12 GHz	2.5-3.75 cm	Guía de misiles, meteorología, cartografía de resolución media, radares de superficie aeroportuarios. Seguimiento a distancias cortas
K_u	12-18 GHz	1.67-2.5 cm	Cartografía de alta resolución. Altímetros para satélites
K	18-27 GHz	1.11-1.67 cm	Absorción del vapor de agua. Se usa para meteorología, para detectar nubes. También para control de velocidad de motoristas.
K_a	27-40 GHz	0.75-1.11 cm	Cartografía de muy alta resolución vigilancia de aeropuertos. Usado para accionar cámaras para fotografíar matrículas de coches infractores
mm	40-300 GHz	7.5 mm - 1 mm	Banda milimétrica, se subdivide como sigue. Nota: la denominación de las bandas no está unánimemente aceptada.
Q	40-60 GHz	7.5 mm - 5 mm	Comunicaciones militares

V	50-75 GHz	6.0-4 mm	Absorbido por la atmósfera
E	60-90 GHz	6.0-3.33 mm	
W	75-110 GHz	2.7 - 4.0 mm	Se usa como sensor para vehículos autónomos experimentales, meteorología de alta resolución y tratamiento de imágenes.

Fuente:

http://es.wikipedia.org/wiki/Radar

Tipos de radar (según su funcionamiento)

Sin entrar en detalle en una descripción de los diferentes tipos de radares y sus características de diseño y capacidades (descriptas en el Anexo 1), haremos una mención de los tipos de radares de uso convencional para la vigilancia y control aeroespacial.

Radares 3 D: Los radares 3 D, permiten determinar la distancia, azimut y altura de las aeronaves, y su información puede ser utilizada para realizar la vigilancia y el control del transito aéreo, sea civil o militar, permitiendo las tareas de interceptación e identificación de vuelos ilícitos.

Radares 2 D: Los radares 2 D, permiten determinar solo la distancia y azimut (no la altura).Al no disponer de información de altura no son aptos para apoyar tareas de interceptación a otras aeronaves.

Ambos tipos de radares se conocen como radares primarios, porque obtienen información de las aeronaves por si solos. La determinación de la presencia de un avión, es independiente de la colaboración que preste la tripulación o el equipo de a bordo de la aeronave; de allí que se pueda denominar a estos radares que detectan a todo blanco como “no cooperativo”.

Radar Secundario: Los radares secundarios o “cooperativos” permiten determinar la distancia, azimut, y altura a condición que la aeronave emita una señal predeterminada por medio de un dispositivo de abordo denominado “transponder”. Básicamente un respondedor a la señal del radar que provee información de ubicación, distancia, altura, código de vuelo, y velocidad. De ahí su designación de “cooperativos”. Estos radares no permiten detectar vuelos “no cooperativos”.

Si el avión no tiene, tiene fuera de servicio o el piloto apaga el “transponder”, el radar secundario no se entera de la presencia del avión.

ANEXO 2

Choosing the adequate ASTERIX Category

The following table will give you indication on how to choose the relevant ASTERIX Category, according to the type of Surveillance related Data to transmit.

Transmission of (Surveillance related Data)	From (Data Source)	ASTERIX Category to use
Monoradar target reports	PSR radar SSR radar M-SSR radar Mode-S station	Cat 048
Monosensor target reports	ADS-B ground station	Cat 021
Monoradar target reports	Surface movement radar	Cat 010
Monoradar service messages	PSR radar SSR radar M-SSR radar Mode-S station	Cat 034
Mode S surveillance coordination function messages	Mode-S station	Cat 017
Mode S datalink function messages	Mode-S station	Cat 018
Ground station service messages	ADS-B ground station	Cat 023
Monoradar service messages	Surface movement radar	Cat 010
Directed Interrogation Messages	Mode-S station	Cat 007
Monoradar weather information	Monoradar	Cat 008
TIS-B Management messages	ADS-B ground station	Cat 022
A-SMGCS data (target report, flight plan data, holdbar status)	SMGCS system	Cat 011
System track data	SDPS system	Cat 062
Sensor Status messages	SDPS system	Cat 063
SDPS Service status messages	SDPS system	Cat 065
Safety Nets Alarms	Safety Nets Server	Cat 004

Multilateration data	Multilateration ground stations	Cat 020
Multilateration System Status Messages	Multilateration ground stations	Cat 019
Digitised Raw Video Information	Rotating Radar	Cat 240
ASTERIX Version Information	Any system	Cat 247
Monoradar Target Reports	Precision Approach Radar (PAR)	Cat 012 (Reserved)
Monoradar Service and Status Messages	Precision Approach Radar (PAR)	Cat 013 (Reserved)
Monoradar Weather Reports	Precision Approach Radar (PAR)	Cat 014 (Reserved)
Monosensor Target Reports	ADS-C Ground Station	Cat 024

http://www.eurocontrol.int/asterix/public/standard_page/how_to_choose.html

ANEXO 3

Capacidades del MRT, descripción técnica.

Capacities

Up to 32 radar inputs
1000 tracks per radar
2000 tracks in the surveillance area
500 plots per second per radar
1000 plots per second total
10,000 tentative tracks per radar

Interfaces/Protocols Supported

EIA-232
EIA-449 (422)
EIA-530
MIL-STD-188-114A
V.11
V.21 bis V.35
Asynchronous
HDLC
SDLC
X.25
TCP/IP
CD-2/CD-2A
BISYNC Radar
9-bit Radars
ASTERIX
Other front end interfaces can be provided

Performance

Maneuver Limits
- Lateral acceleration to ±8g
- Axial acceleration to ±2g

Target Velocity: 4,000 knots, max
Track Initiation:
- Track initiation within two antenna scans in clear areas using IFF data
- Track initiation within eight scans in high false-report areas with no IFF data

Less than 10 false track reports per hour with 2000 clutter and noise plots per scan
Low-Speed Filter: 0 to 160 knots, selectable

Accuracy

For non-accelerating targets, MRT track data typically provides:
- A 200% improvement in track-to-input plot position accuracy
- Velocity within ten (10) Nautical Mile (NM)/hr
- Heading accuracy better than five (5) degrees

Automatic Sensor Registration
- Azimuth correction value <0.1 degree
- Range correction value <0.1 NM

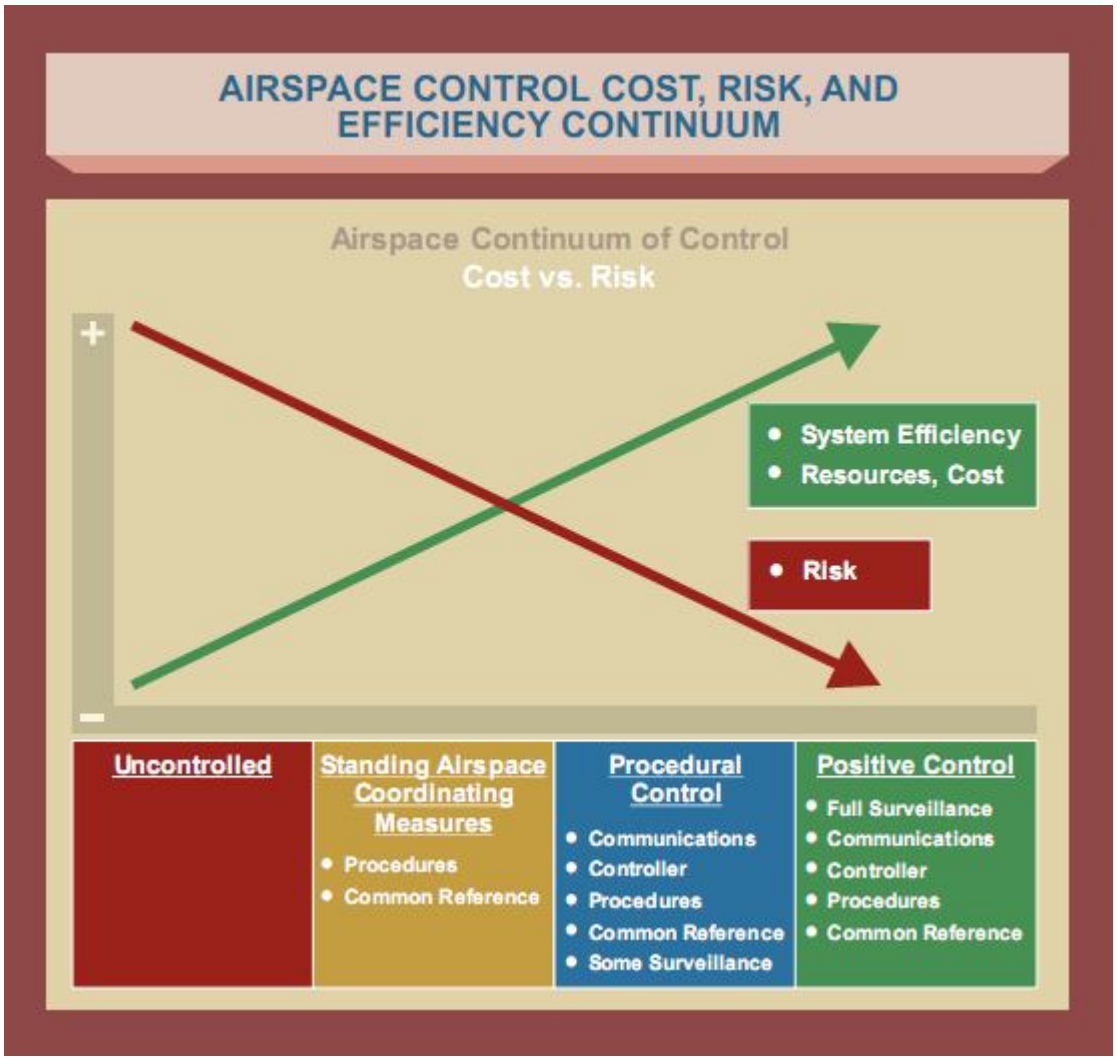
Physical

Dimensions 22.2 in.W x 18.4 in. H x 39.8 in. D
(56.3 cm x 46.8 cm x 101.1 cm)
Weight 150 lb (68 kg)
Power 500 Watts, 115-240 VAC 50/60 Hz

ANEXO 4

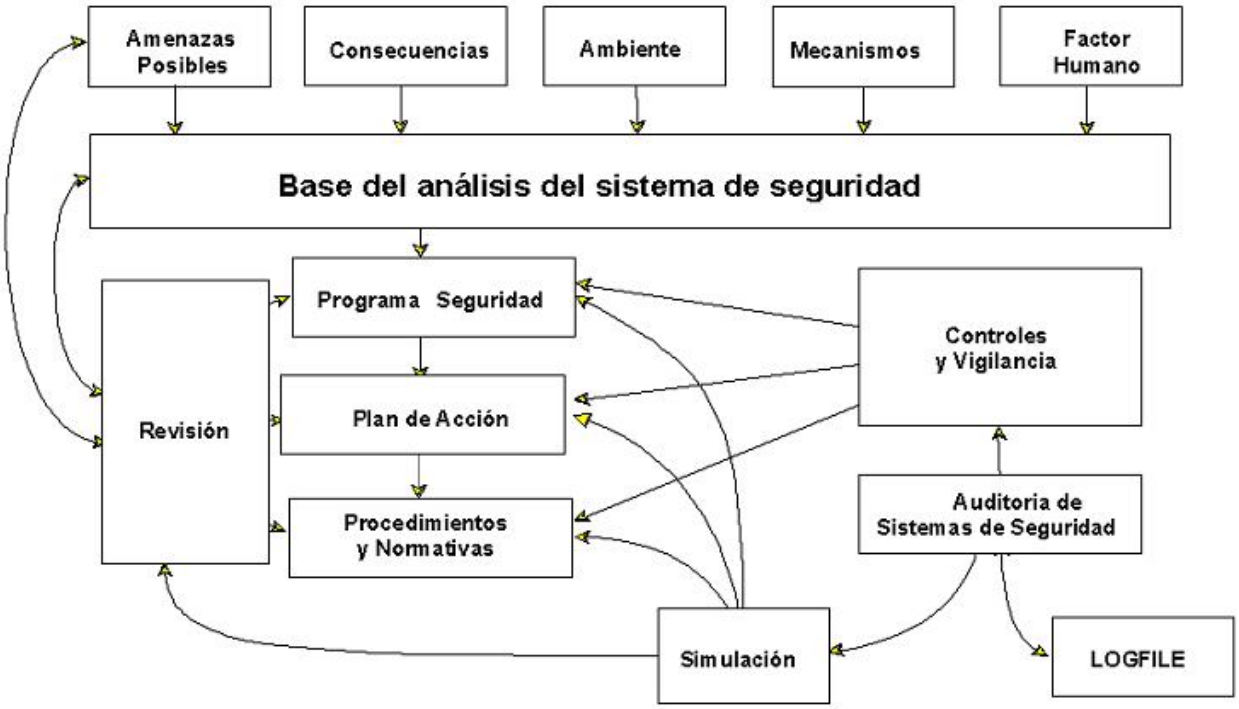
BASIC PRINCIPLES OF AIRSPACE CONTROL

- Reducir el riesgo de fratricidio y optimiza la eficacia de la defensa aérea.
- La planificación centralizada facilita la reunión conjunta del espacio aéreo prioridades comandante de la fuerza.
- La ejecución descentralizada da comandantes subordinados la flexibilidad necesaria para ejecutar sus misiones con eficacia
- Mantener una estrecha relación y coordinación entre todos los usuarios del espacio aéreo.
- Requerir de supervivencia, integradas y sistemas redundantes para el control del espacio aéreo.
- Responder a las condiciones de amenaza en desarrollo y despliegue de la operación.
- funciones de control del espacio aéreo se basan en los recursos de gestión del espacio aéreo, pero son diferentes que el ambiente de control de tráfico.
- Hacer hincapié en la flexibilidad y la simplicidad.
- Los sistemas de control del espacio aéreo deben ser integrados a la medida de lo práctico.
- Apoyar a las 24 horas las operaciones en todas las condiciones climáticas y ambientales.
- Requerir de formación adecuados para las operaciones de control eficaz y seguro del espacio aéreo.


AIRSPACE CONTROL COST, RISK, AND EFFICIENCY CONTINUUM
Airspace Continuum of Control
Cost vs. Risk
+
−
System Efficiency
Resources, Cost
Risk
Uncontrolled
Standing Airspace Coordinating Measures
Procedures
Common Reference
Procedural Control
Communications
Controller
Procedures
Common Reference
Some Surveillance
Positive Control
Full Surveillance
Communications
Controller
Procedures
Common Reference

ANEXO 5

Seguridad integral

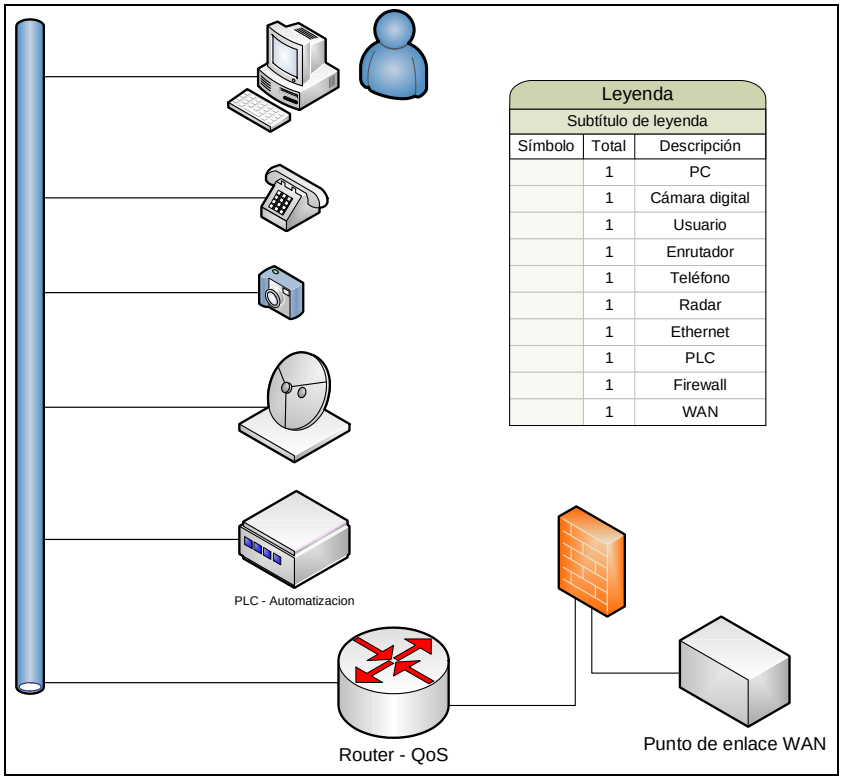


ANEXO 6

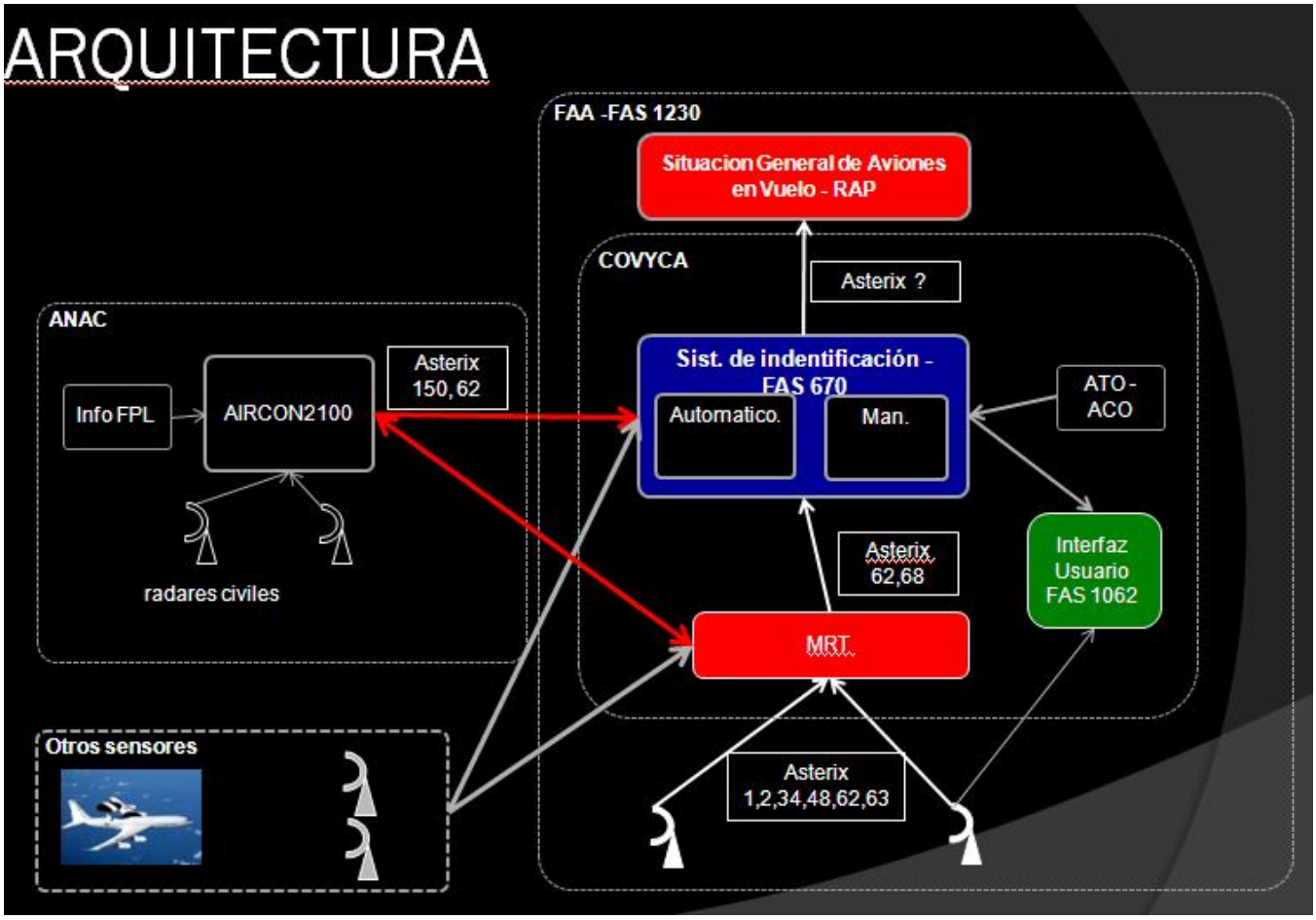
Nodo Radar

Durante este trabajo hemos hablado del sensor radar en forma figurativa, pero no hemos descripto un nodo radar, en el siguiente grafico he colocado lo que sería en términos teóricos un nodo radar tipo. El sensor radar, ya no se concibe en forma aislada, sino que está fuertemente enlazado a la parte energética, la de seguridad física, a la infraestructura, al enlace de comunicaciones, al soporte técnico (mantenimiento), entre los más importantes, con el objeto de asegurar la máxima disponibilidad de servicio.

Desde el punto de vista de las comunicaciones, el radar, posee una interfaz digital de extracción de datos, los que variara según el tipo de radar. Esta interfaz se conecta al nodo radar para transmitir los datos a un enlace WAN, junto con otros servicios como los que figuran en la figura, ellos son telepuertos para la administración remota de: el nodo radar, el router, el firewall; el enlace de telefonía IP, el servicio de seguridad de cámaras, el servicio de seguridad de los automatismos del radar y nodo radar (control de generadores eléctricos, control de accesos, control de temperatura, control de los niveles de combustible, etc) y todo otro servicio que se considere necesario como los son la posible inclusión de la una R.E.A.V.A. (red de estaciones de VHF de avanzada) para la comunicaciones de las aeronaves con el centro de control, o los data link para la transmisión de datos.



ANEXO 7


ARQUITECTURA
FAA -FAS 1230
Situacion General de Aviones en Vuelo - RAP
COVYCA
Asterix ?
ANAC
Info FPL
AIRCON2100
Asterix 150, 62
Sist. de indentificación - FAS 670
Automatico.
Man.
ATO - ACO
radares civiles
Asterix 62,68
Interfaz Usuario FAS 1062
MRT
Otros sensores
Asterix 1,2,34,48,62,63