

# Boletín

## DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA



SUBDIRECCIÓN GENERAL DE TECNOLOGÍA Y CENTROS  
Boletín de Observación Tecnológica en Defensa nº 20 • 3º Trimestre de 2008

### Conceptos de *middleware*: DDS como tecnología emergente en Defensa

- Vehículos de combate modulares: una perspectiva
- Sistemas de localización y trazabilidad RFID para el análisis de la evacuación del buque de guerra

b  
20

20 NÚMEROS DE BOLETÍN



## Nodo Gestor (NG)

C.F. Ing. José María Riola Rodríguez  
SDG TECEN C/ Arturo Soria 289  
Madrid 28033  
[jriorod@fn.mde.es](mailto:jriorod@fn.mde.es)

## Observatorio Tecnológico de Armas, Municiones, Balística y Protección (OT AMBP)

T.Col. CIP Nicolás Braojos López  
[nbraojos@oc.mde.es](mailto:nbraojos@oc.mde.es)

## Observatorio Tecnológico de Electrónica (OT ELEC)

C.N. Ing. Arturo Montero García  
[amonterog@oc.mde.es](mailto:amonterog@oc.mde.es)

## Observatorio Tecnológico de Energía y Propulsión (OT ENEP)

C.C. Ing. Juan Carlos Huertas Ayuso  
[jchayuso@fn.mde.es](mailto:jchayuso@fn.mde.es)

## Observatorio Tecnológico de Defensa NBQ (OT NBQ)

T.Col. CIP Juan C. Fernández Fernández  
[jcfernandez@oc.mde.es](mailto:jcfernandez@oc.mde.es)

## Observatorio Tecnológico de Materiales (OT MAT)

Cte. CIESO Jesús M. Aguilar Polo  
[jaquilarp@oc.mde.es](mailto:jaquilarp@oc.mde.es)

## Observatorio Tecnológico de Óptica, Optrónica y Nanotecnología (OT OPTR)

Ing. D. Fernando Márquez de Prado Urquía  
[fmarquezu@oc.mde.es](mailto:fmarquezu@oc.mde.es)

## Observatorio Tecnológico de Plataformas No Tripuladas, Robótica y Plataformas Aéreas (OT UAVs)

Cte. CIEA-ETO Manuel A. González López  
[mgonlo2@oc.mde.es](mailto:mgonlo2@oc.mde.es)

## Observatorio Tecnológico de Sistemas Terrestres y Navales (OT STN)

Col. CIP Manuel Engo Nogués  
[mengnog@et.mde.es](mailto:mengnog@et.mde.es)

## Observatorio Tecnológico de Tecnologías de la Información, Comunicaciones y Simulación (OT TICS)

Ing. D. Francisco Javier López Gómez  
[fjlopez@oc.mde.es](mailto:fjlopez@oc.mde.es)

[www.mde.es/dgam/observatecno.htm](http://www.mde.es/dgam/observatecno.htm)



## CONTENIDOS

### 3 Editorial

#### Actualidad

#### Agencia Europea de Defensa (EDA)

4 Iniciativas sobre UAS en la EDA

#### OTAN y Research and Technology Organization (OTAN-RTO)

5 Medalla al Mérito Científico de la RTO: grupo SAS-060 sobre Armas No Letales

6 Laboratorio móvil Movilink-22

#### Otras noticias

7 Análisis in situ en inspecciones de la OPAQ

8 Jornada sobre materiales inteligentes

9 19º Congreso Mundial del Petróleo

### 9 Enlaces

#### Tecnologías Emergentes

10 Vehículos de combate modulares: una perspectiva

12 Sistemas de localización y trazabilidad RFID para el análisis de la evacuación del buque de guerra

#### En profundidad

15 Conceptos de middleware: DDS como tecnología emergente en Defensa

### 19 Agenda

## ***Editorial***

Un tema candente en los últimos años para la Defensa, es el de asentar la política de investigación y tecnología sobre la base más segura y rentable posible, tal que las decisiones tomadas en un momento dado puedan tener los resultados más positivos en un mañana más o menos lejano.

El I+T de la Defensa debe proporcionar conocimientos científicos en todas las tecnologías relevantes a las Fuerzas Armadas, de manera que les permita afrontar sus tomas de decisiones apropiadamente. Esto cobra especial importancia si pensamos en los cambios radicales en materia de seguridad que están ocurriendo en nuestro planeta.

La experiencia insiste en demostrar continuamente que la tecnología toma el papel desequilibrante en cualquier conflicto, y por ello todos los países de nuestro entorno tienen entre sus estructuras la

función de analizar cuál será la evolución de las tecnologías claves para su desarrollo.

Para poder cumplir con dicha función es necesario disponer de sistemas eficientes de información con los que poder realizar un continuo análisis de prospectiva. Esta actividad es desempeñada por organismos que entre sus funciones se podrían incluir una frase similar a la de "vigilancia, prospectiva tecnológica y planeamiento".

La dinámica de las sociedades abiertas hace necesario un proceso continuo que contraste la evolución de los desarrollos tecnológicos con las previsiones futuras. De esta forma se está constantemente preparado para los desafíos que se vayan presentando. Esta es la función actual de la Prospectiva Tecnológica en nuestros Observatorios.

# European Defence Agency (EDA)



## UAS: INICIATIVAS EN LA EDA

Jesús López Pino, OT UAVs

La Agencia Europea de Defensa (EDA) actúa, desde el año 2005, como motor de activación y punto focal en el área de los sistemas aéreos no tripulados (UAS), generando diversas iniciativas desde sus Direcciones de Capacidades, Armamento o Investigación y Tecnología. Estas iniciativas cubren los principales aspectos relativos a los UAS, a través de diferentes propuestas, que se encuentran en distinto estado. Especial mención merecen las propuestas MIDCAS, *UAS Insertion into General Air Traffic* y MTUAS.

La primera de ellas (MIDCAS) es muy significativa por su valoración (entre 40 y 60 M€), por su duración (4 años) y su alcance (desarrollo de soluciones *Sense and Avoid*). Esta propuesta, realizada por los gobiernos de Suecia y Francia, se encuentra en fase de preparación y han sido invitados a participar España, Alemania e Italia.

Por otro lado, la iniciativa "*UAS insertion into General Air Traffic*", desarrollada por el consorcio Air4All (constituído por BAE Systems, Alenia Aeronautica, Dassault Aviation, Diehl BGT Defence, EADS

CASA, EADS Defence & Security Alemania, Galileo Avionica, QinetiQ, Rheinmetall Defence Electronics, SAAB AB, Sagem Defence Systems y Thales Aerospace) y finalizada en julio de 2008, ha proporcionado un informe final que contiene, entre otros, un *roadmap* que ofrece una aproximación paso a paso para la integración total de los UAS. Este *roadmap* representa un punto de inflexión en las, hasta ahora, dispersas actividades y estudios sobre UAS y pretende plasmar de forma realista las tareas para la consecución de la integración de los UAS.

En apoyo de los resultados obtenidos en el estudio de Air4All, el *Steering Board* de la Agencia acordó que se propusieran proyectos *ad hoc* para el desarrollo de cada uno de los aspectos tratados en el informe final. El resultado ha sido la generación de diversos *Business Cases* para el inicio de proyectos comunes en el periodo 2008/2009.

Los proyectos han sido priorizados por la EDA atendiendo a la urgencia de las tareas a realizar y serán lanzados para su contratación de acuerdo a dichas prioridades.

Sobre el primero de ellos, relativo a "*Military Frequency Spectrum Allocations for UAV*", se ha hecho pública la *Contract Notice* que abre el proceso de contratación para la

realización de dicho estudio. Otros *Business cases* relativos a autonomía, estaciones terrestres de control, propulsión etc., están pendientes de aprobación por las naciones antes de la publicación de las correspondientes llamadas.

Por último, cabe destacar el programa del MTUAS (*Maritime Tactical UAS*), generado en el WG2 (Vehículos Aéreos No Tripulados) del *Project Team "Maritime Surveillance"* (PT MARSUR), del que España forma parte. En este 2008, una vez aprobados los CSR (*Common Staff Requirements*) se emitirán diferentes RFI (*Request For Information*) a las empresas en base a cuyas propuestas se contratarán las siguientes fases del Programa, que finalizará con la producción de determinado número de unidades VTOL embarcadas (el inicio de la Fase de Producción se prevé para el 2015).

Aunque el CSR ha sido aprobado por España en mayo de este año, la participación en las sucesivas fases del proyecto no está decidida.

Tabla. 1. Integración paso a paso.

UAVs sin certificación de tipo		UAVs con certificación de tipo		
UAVs experimentales		UAV gubernamentales	UAVs civiles/gubernamentales	
Paso 1 Espacio Aéreo Segregado	Paso 2 Espacio Aéreo No Segregado	Paso 3 Espacio Aéreo No Segregado	Paso 4 Espacio Aéreo No Segregado	Paso 5 Espacio Aéreo No Segregado
Vuelo dentro de frontera nacional Competencia nacional				Mundial OACI

# OTAN y Research and Technology Organization (OTAN-RTO)



## Medalla al Mérito Científico de la RTO: SAS-060 sobre Armas No Letales

Jorge Lega, OT AMBP

El escenario de las operaciones militares actuales, la evolución en las maneras de actuar de los ejércitos y la cada vez mayor voluntad de minimizar los daños colaterales en los conflictos han impulsado en los últimos años el desarrollo de las llamadas Armas o Medios No Letales (ANLs/MNLs) (*Non Lethal Weapons* – NLWs en inglés y otras denominaciones similares).

Estos medios pretenden dotar a las unidades de la capacidad de actuar eficazmente al tiempo que buscan reducir al mínimo posible los daños que se causan tanto a personas como en materiales e incluso en el medio ambiente. Tienen aplicación en casi todo el rango de operaciones militares y de seguridad, como en situaciones de enfrentamiento en las que cada vez es más difícil distinguir entre población civil y potenciales adversarios y fundamentalmente en operaciones no bélicas (por ejemplo en control de multitudes).

Uno de los aspectos novedosos de las ANLs es la dificultad de evaluar su eficacia dado que, por su naturaleza, nos son válidas las metodologías existentes para el armamento convencional. En este sentido, la Subdirección de Tecnología y Centros (SDG TECEN) de la DGAM, a través del Laboratorio Químico Central de

Armamento (LQCA) y del Observatorio Tecnológico de Armamento, Munición, Balística y Protección (OT AMBP), ha participado en el grupo de trabajo OTAN RTO-SAS-060 "*Non Lethal Weapons - Effectiveness Assessment Development and Verification Study*". Este grupo, ha llevado sus trabajos a cabo entre 2004 y 2007, con el objetivo de elaborar la metodología para verificar y evaluar los medios no letales hasta el nivel operativo.

En concreto, España ha llevado a cabo los trabajos para ampliar la metodología desarrollada hasta el momento y estudiar las posibilidades de desarrollo de medidas de eficacia a nivel operativo (MoOEs *Measures of Operational Effectiveness*). Para ello, ha identificado, desarrollado y aplicado una serie de métodos que, sobre los principios de la metodología, permiten valorar cualquier sistema (medida de su eficacia) y realizar comparaciones entre sistemas. Asimismo, ha propuesto un método para evaluar sistemas de ANLs a nivel operativo en una secuencia de fases que se suceden a lo largo de un escenario operativo.

Para desarrollar los trabajos se han empleado métodos matemáticos analíticos, métodos de toma de decisiones multicriterio, redes neuronales y se ha aplicado lógica difusa, así como múltiples simulaciones. Todo ello se ha implementado, a nivel nacional, en una plataforma software de desarrollo.

El alto nivel del trabajo realizado, ha merecido la concesión del **2008 Scientific Achievement Award de la Research and Technology Organization (RTO)** de la OTAN al

grupo de trabajo SAS-060, en reconocimiento a "el esfuerzo excepcional realizado en actividades significativas de la RTO, a la excelencia y originalidad en sus contenidos científicos y técnicos, así como a sus destacados resultados en términos de beneficios para la Defensa".

El resultado de estos trabajos permitirá disponer de medios estandarizados de evaluación para cualquiera de los sistemas y las tecnologías que comprenden las ANLs. Servirán, entre otros, para la elaboración de requisitos, doctrina, evaluación de equipos, como herramienta de selección y/o adquisición, etc., e incluso para su empleo por parte de los investigadores como guía para mejorar las prestaciones de los medios no letales existentes. No obstante, para disponer de estas herramientas, y aunque se ha avanzado mucho, todavía queda trabajo por hacer.

Además, la SDG TECEN, a través de sus expertos en ANLs, participa en el grupo de trabajo de la JUPROAM sobre "Desarrollo de Capacidades militares en la FAS que facilitan el uso no letal de la fuerza".

Este grupo coordina las actividades que se llevan a cabo en este ámbito tanto a nivel nacional como en las participaciones en los diferentes grupos de trabajo internacionales en que España está presente. A nivel internacional se tiene presencia en grupos de la OTAN (entre ellos al grupo SAS-078 que dará continuidad al SAS-060), de la Agencia Europea de Defensa (EDA) y en el seno de la Lol.

Los interesados en este tema pueden encontrar más información en los siguientes Boletines:

- Nº 4 "Armas No Letales".
- Nº 5 "Simposio: Armas No Letales".
- Nº 13 "Evaluación de Eficacia de Armas No Letales".
- Nº 17 "Finaliza el grupo OTAN-RTO-SAS-060 sobre Armas No Letales".

### ¿QUIERE COLABORAR EN EL BOLETÍN?

Envíe sus sugerencias al **Sistema de Observación y Prospectiva Tecnológica** y contactaremos con usted. Puede proponer temas que considere de interés o sobre los que le gustaría ampliar conocimientos, colaborar preparando artículos, presentando estudios y análisis prospectivos,...

**Contacto:** C.F. Ing. José María Riola Rodríguez

Tel.: 913954631; correo electrónico: [jriorod@fn.mde.es](mailto:jriorod@fn.mde.es)

## Laboratorio móvil Movilink-22

M<sup>a</sup> Dolores Ladrón de Guevara Martínez y José Carlos Fortea Marín, Departamento de Electrónica (CIDA-ITM)

El programa internacional NILE (*NATO Improved Link Eleven*) es un proyecto conjunto en el que participan siete naciones (Canadá, Francia, Alemania, Italia, Reino Unido, Estados Unidos y España), cuya misión es el desarrollo de un nuevo enlace de datos táctico, denominado Link-22, que sustituirá al Link-11 y convivirá con el Link-16.

El Link-22 opera, a diferencia de otros, en las frecuencias de HF (2-30 MHz) y UHF (225-400 MHz) en los modos de frecuencia fija y salto en frecuencia. En el modo HF permite interconectar unidades más allá de las 300 millas náuticas sin necesidad de disponer de una unidad que retransmita los mensajes.

Además, una red Link-22 puede estar formada por hasta 8 subredes de radiofrecuencia y cada unidad puede operar de forma simultánea hasta en 4 de estas subredes.

Entre las ventajas que proporciona Link-22 sobre Link-11 se encuentran las siguientes:

- Independencia de un nodo centralizado. La arquitectura utilizada es TDMA (*Time Division Multiple Access*). Esta arquitectura concede periodos de transmisión (*time-slots*) a cada unidad, planificándose su disposición de forma previa a la operación. Implementa además la capacidad de utilizar TDMA dinámico, pudiendo modificarse las asignaciones de *time-slots* durante la operación de la red.
- Mayor protección ante interferencias (*anti-jamming*), debido a la posibilidad de utilizar salto en frecuencia, tanto en HF como en UHF.
- Inclusión de un dispositivo COMSEC (*Communications Security*) para la encriptación de los mensajes.
- Formato de mensajes similar a Link-16, lo que facilita el reenvío de información entre ambos Data Link (*Data-Forwarding*).

- Capacidad de retransmisión automática entre las distintas subredes Link-22, lo que permite el intercambio de mensajes entre unidades que no están conectadas a través del mismo medio físico.
- Gestión de red avanzada, que permite cambiar de forma dinámica los parámetros de funcionamiento de las subredes.
- Posibilidad de incorporar nuevas unidades una vez que la red está iniciada sin interrumpir las operaciones (*Late Network Entry*).

Un sistema Link-22 está formado por los siguientes equipos, algunos proporcionados por la oficina de programa NILE y otros cuyo desarrollo es responsabilidad nacional:

- El *Data Link Processor* (DLP) es un equipo de responsabilidad nacional encargado de independizar los sistemas de la unidad (*TDS – Tactical Data System*) de los distintos Data Link en los que opera. Realiza el cambio de formato entre la información táctica de los sistemas de la unidad y los mensajes Link-22.
- El *System Network Controller* (SNC) es un software común para todos los sistemas Link-22. Ha sido desarrollado por la oficina del programa NILE y se encarga de proporcionar el servicio de entrega de mensajes y de implementar los protocolos de red. Está disponible para los sistemas operativos Windows y Linux.
- El *Link Level Comsec* (LLC) es un equipo desarrollado por la oficina del programa NILE encargado del cifrado de los mensajes Link-22.
- El *Signal Processing Controller* (SPC) es el equipo encargado de modular/demodular la señal según las formas de onda existentes para cada uno de los medios (HF o UHF), así como de la detección y corrección de errores.
- Las radios, que pueden ser HF o UHF, tanto de frecuencia fija como

con salto en frecuencia. Se ha diseñado Link-22 para que se puedan utilizar las radios en uso actualmente para Link-11.

- El TOD (*Time of Day*), encargado de la sincronización de los distintos equipos.

El Centro de Investigación y Desarrollo de la Armada (CIDA) lleva desde finales de los años 90 realizando desarrollos para los nuevos enlaces de datos tácticos (Link-16 y Link-22). Uno de estos desarrollos es el laboratorio móvil Movilink-16, consiste en un *shelter* NATO-II en el que se integra un MIDS-LVT (*Multifunctional Information Distribution System Low Volume Terminal*, equipo de transmisión Link-16) y el software necesario para participar en operaciones Link-16 y para la realización de pruebas. El Movilink-16 ha servido para probar las capacidades Link-16 de distintas plataformas españolas, tales como las fragatas F-100, el buque Castilla y el sistema integrado de mando y control aéreo.

Siguiendo este enfoque, en la actualidad se está desarrollando un laboratorio móvil (Movilink-22), así como la herramienta software de pruebas Evalink-22, que se integrará en el mismo y que implementa la funcionalidad del *Data Link Processor* de Link-22, simulando además las capacidades tácticas de una unidad real.

Este laboratorio móvil permitirá probar las capacidades Link-22 de las unidades españolas a las que se dote en el futuro de dicho enlace de datos táctico, como son los submarinos S-80, los buques BAC y BAM, las fragatas F-100, las LPDs (Castilla y Galicia) y los porta aeronaves (Príncipe de Asturias y Juan Carlos I).

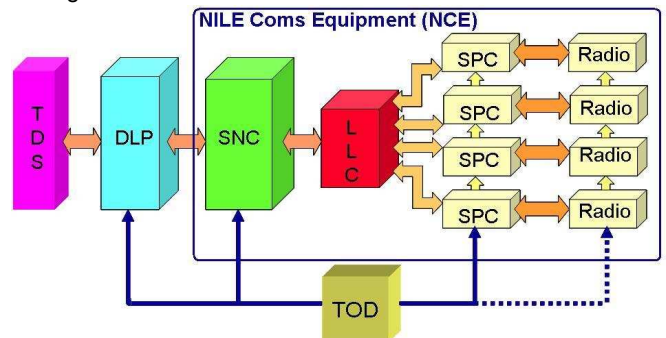


Fig. 1. Arquitectura de los sistemas Link-22.

## Otras noticias

### ANÁLISIS IN SITU EN INSPECCIONES DE LA OPAQ

Esther Gómez Caballero, Departamento NBQ (FNM-ITM)

La Organización para la Prohibición de Armas Químicas (OPAQ) realiza la ingente labor de controlar a miles de industrias químicas en todo el mundo para garantizar que los productos químicos, a partir de los cuales se pueden sintetizar armas químicas, se utilicen en su totalidad para fines legales (actividades declaradas).

Para realizar esta labor, la OPAQ dispone de una amplia plantilla de inspectores encargados de realizar periódicamente inspecciones rutinarias y, en casos excepcionales, inspecciones debidas a denuncias. Para analizar las muestras tomadas por los inspectores, la OPAQ dispone de laboratorios de alta cualificación de países colaboradores a los que examina todos los años. Uno de estos laboratorios se encuentra en España, el LAVEMA.<sup>1</sup>

Pero en algunas ocasiones puede ser necesario un análisis preliminar de las muestras *in situ*, durante la inspección y dentro de la propia planta química. Esta operación supone dificultades no fáciles de superar, como son:

- Empleo de equipos analíticos muy sofisticados no disponibles en la planta química.
- Utilización de equipos analíticos robustos para resistir el transporte.
- Imposibilidad de transportar por vía aérea gran parte de los equipos y consumibles.
- Intervención de expertos en química analítica y espectrometría de masas.

Un punto crítico para la OPAQ es garantizar la confidencialidad y no dejar al descubierto los componentes de la formulación no relacionados con las armas

químicas, siendo ésta una exigencia fundamental en las inspecciones.

Para solucionar el problema del transporte del equipo analítico y los consumibles (entre los que se encontraban gases de cromatografía en cilindros a presión) se realizan transportes especiales por carretera.

Para determinar la operatividad de este procedimiento en las inspecciones rutinarias, la OPAQ ha comenzado a realizar ejercicios de este tipo y España ha sido uno de los países en los que se ha realizado este tipo de inspección.

En el mes de mayo del presente año, unos días antes de realizarse la inspección a una planta química situada en Cataluña, la OPAQ comunicó a la Autoridad Nacional Española (ANPAQ), dependiente del Ministerio de Asuntos Exteriores e Industria, que debería incluir un análisis *in situ* durante la semana que duraría la inspección.

La Autoridad Nacional organizó su equipo de personas, que en este caso, además de la composición habitual, incluyó un experto del laboratorio de verificación de la Marañosá (LAVEMA) en cromatografía y espectrometría de masas con amplia experiencia en la analítica de compuestos químicos clasificados como agentes químicos de guerra.

Su misión consistió en, además de prestar apoyo a los analistas de la OPAQ, actuar como defensor de los intereses nacionales y de la industria

española en el hipotético caso de que existiese conflicto en la identificación de algún agente no declarado. La Organización envió dos expertos analistas que trabajaron junto con el experto español y el personal técnico de la planta inspeccionada.

Es importante destacar que, frente a un problema que pudiese aparecer en una industria española, el primer responsable es el gobierno de España, que tendría que hacer frente a las elevadas multas económicas o consecuencias legales que correspondan.

El conflictivo tema de la confidencialidad de la información se resolvió instalando un programa informático especial en los equipos analíticos. Para la identificación de los compuestos presentes en las muestras se utilizó el software de deconvolución AMDIS, el cual dispone de una amplia base de datos, pero que el operador sólo puede ver en pantalla si se identifica algún compuesto clasificado, quedando oculto el resto de componentes que constituyen la muestra analizada.

El equipo inspector de la OPAQ decidió los lugares de la toma de muestras y la naturaleza de las mismas. Se recogieron dos muestras de aspecto aceitoso.

Los químicos analíticos de la OPAQ junto con el experto nacional, como observador del tratamiento, obtuvieron las diferentes alícuotas, analizaron las muestras y emitieron un informe final con los resultados obtenidos, confirmando la ausencia de compuestos clasificados no declarados. El resultado de la experiencia, tanto la inspección de la industria como el método de análisis "in situ" aplicado, se consideró muy positivo.



Fig. 1. Personal del LAVEMA durante el análisis de muestras.

<sup>1</sup> Boletín nº 3 "Designación OPAQ del LAVEMA".

# JORNADA SOBRE MATERIALES INTELIGENTES

Luis Miguel Requejo Morcillo, OT MAT

El día 26 de junio se celebró en el Centro Nacional de Investigaciones Metalúrgicas (CENIM) la jornada "Nuevos Materiales para la Seguridad y la Defensa", organizada por la Fundación Círculo de Tecnologías para la Defensa y la Seguridad.

Durante la jornada se impartieron una serie de conferencias por parte de expertos en el área de tecnología de materiales, dando una visión del estado del arte de los materiales definidos como "inteligentes" y de sus aplicaciones en el sector de defensa, aunque muchas de ellas también pueden ser adoptadas por el civil.

Por parte de la Subdirección General de Tecnología y Centros, el Cte. Jesús M<sup>a</sup> Aguilar Polo, que expuso la ponencia "Prospectiva y Aplicaciones en Defensa de los materiales Inteligentes". En ella, se identificaron las principales áreas de interés tecnológico para Defensa en el ámbito de la tecnología de materiales y la relación o posible aplicabilidad de los materiales inteligentes en las mismas, tanto en la actualidad como en un futuro próximo. Estas líneas tecnológicas has sido identificadas y consideradas relevantes por el Observatorio de Materiales.

## EL PAPEL DE LOS MATERIALES INTELIGENTES EN DEFENSA

En general, para la industria es muy importante realizar una correcta selección de materiales a la hora de fabricar cualquier tipo de vehículo o

instrumento. Las nuevas plataformas e instrumentos a utilizar en Defensa requieren cada vez materiales más resistentes y ligeros y sistemas capaces de prever su mal funcionamiento y su deterioro con atención especial a la capacidad de protección que ofrece ante amenazas explosivas, balísticas y también NBCR.

Tradicionalmente, para estos fines se han empleado materiales metálicos, aunque el empleo de polímeros, materiales cerámicos y compuestos es cada vez mayor. Desde hace unos años se vienen estudiando y desarrollando una serie de materiales que son capaces de responder de una manera determinada ante un estímulo externo, modificando sus propiedades o incluso su forma, de manera variable y controlable. Son los conocidos como materiales inteligentes, los cuales pueden llegar a ser una alternativa válida (lo cierto es que actualmente ya se están utilizando en gran cantidad de dispositivos) y llegar a ser imprescindibles para la fabricación de equipos.

Existen numerosos tipos de materiales de los denominados "inteligentes" y muchas maneras de clasificarlos. La clasificación presentada en este artículo viene determinada tanto por su naturaleza como por el fundamento físico que los caracteriza. Se pueden distinguir los siguientes:

- Los **materiales con memoria de forma** son capaces de modificar su forma por medio de cambios de temperatura y tensiones. Este tipo de materiales presentan un elevado número de aplicaciones implicadas al campo de la defensa, como por ejemplo en la fabricación de determinadas piezas de motores, actuadores, en

aplicaciones médicas, en la inserción en sistemas inteligentes, etc.<sup>1</sup>

- Los **materiales electro y magnetoactivos** cambian sus propiedades físicas cuando se someten a una campo eléctrico y magnético respectivamente. Este tipo de materiales pueden ser empleados en actuadores, sistemas de control y sensores. Los fluidos magnetorreológicos son motivo de estudio para el desarrollo de los nuevos blindajes endurecibles y de sistemas de control de vibraciones.<sup>2</sup>
- Los **materiales cromoaactivos** son aquellos materiales en los que se producen cambios de color por la acción de algún fenómeno externo como la corriente eléctrica, radiaciones, etc. En los **materiales fotoactivos**, bien tienen lugar cambios de distinta naturaleza por la acción de la luz o bien son capaces de emitir luz como consecuencia de algún fenómeno externo. Estos materiales se aplican en el desarrollo de sistemas ópticos y optoelectrónicos, en el procesado de películas delgadas (fabricación de pantallas planas), etc.<sup>3</sup>

## SISTEMAS INTELIGENTES

Es importante hacer mención en este artículo a la existencia de **sistemas inteligentes**, que son heterogéneos desde el punto de vista del material, pero que presentan capacidad multifuncional gracias a la integración de microestructuras de diversos tipos, logrando un comportamiento inteligente desde el punto de vista macroscópico. Algunos de estos sistemas inteligentes con cabida en las prioridades de Defensa son:

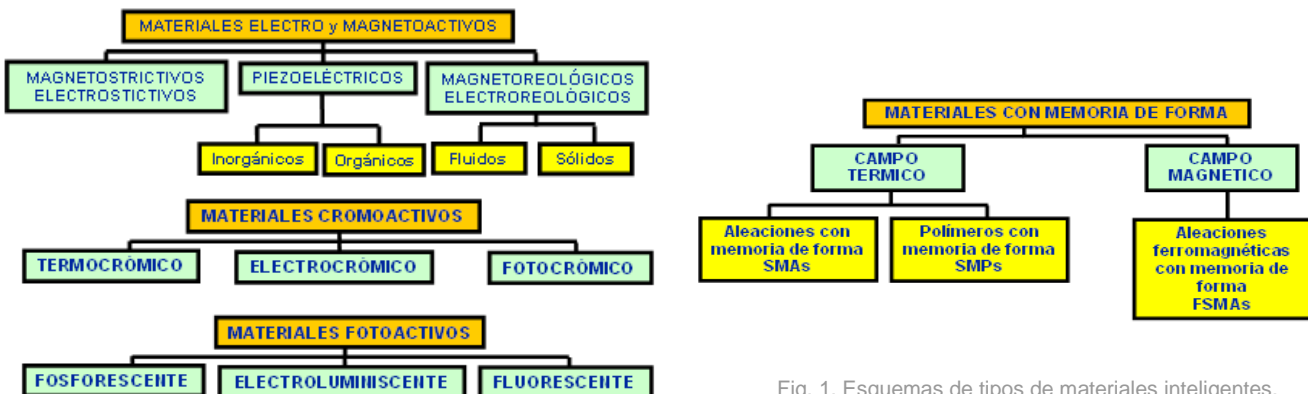


Fig. 1. Esquemas de tipos de materiales inteligentes.



- **Sistemas de monitorización estructural (SHM)**, capaces de proporcionar información en tiempo real y a corto plazo del estado de una estructura.<sup>4</sup>
- **Materiales compuestos autorreparables**. Son materiales capaces de actuar ante ciertas condiciones, desencadenando reacciones químicas que reparen grietas o defectos producidos en una estructura.
- **Textiles inteligentes**. Son materiales textiles que presentan funcionalidades distintas a las del textil base, o incluso que pueden cambiar sus propiedades en función del medio ambiente en el que se encuentren. Esto es posible

por medio de la integración de microdispositivos en los tejidos.<sup>5</sup>

- **Músculos artificiales y actuadores biomiméticos**. Son sistemas inteligentes bio-inspirados.

Aunque algunos materiales inteligentes ya son conocidos desde hace mucho tiempo (como es el caso de los piezoeléctricos), muchos de ellos son muy novedosos y requieren de investigación y desarrollo y de la coordinación de ambos con el fin de ampliar su campo de aplicabilidad. Más específicamente para Defensa, la aplicación de materiales y sistemas inteligentes, tendrá un impacto positivo en la logística operativa: aumentar la supervivencia y la disponibilidad del

sistema, reducir su peso, disminuir su coste del ciclo de vida, etc.

<sup>1</sup> Boletín Nº 12, "Materiales con Memoria de forma".

<sup>2</sup> Boletín Nº 6, "Sistemas de protección flexible: presente y futuro".

<sup>3</sup> Boletín nº 13, "Materiales activos orgánicos"

<sup>4</sup> Boletín nº 5, "Sensores embebidos".

<sup>5</sup> Boletín nº 7, "Smart textiles".



## Congreso Mundial del Petróleo

Luis Miguel Requejo Morcillo, OT ENEP

Entre los días 29 de junio y 3 de julio de 2008, tuvo lugar en IFEMA Feria de Madrid el 19º Congreso Mundial del Petróleo. El Consejo Mundial del Petróleo organiza cada tres años este evento, que agrupa a 60 países miembros que representan el 95% de la producción y consumo mundial.

El 19º Congreso Mundial del Petróleo se ha caracterizado principalmente por la situación económica actual debida al elevado precio del barril de petróleo. Los temas a tratar se dividieron principalmente en cuatro bloques.

El primero de los bloques (*upstream*) trató sobre las últimas novedades en materia de recuperación de gas y petróleo de los yacimientos, así como nuevos medios de exploración y obtención de hidrocarburos. En el

segundo bloque (*downstream and petrochemicals*) se abordaron temas relacionados con la mejora de la eficiencia y optimización energética en refinerías. El tercer bloque (*natural gas and renewables*) se centró en cuestiones relacionadas con la mejora en la obtención de gas natural (fuentes no convencionales, transporte, oferta y demanda), y las relacionadas con las tecnologías de fuentes de energía renovables (eólica y solar). El cuarto bloque (*managing the industry*) trató sobre asuntos de sostenibilidad, la situación actual del mercado, aspectos de salud y seguridad para el medio ambiente y también para el mantenimiento de la propia industria petroquímica.

Además, se llevaron a cabo sesiones extraordinarias en las que se abordaron importantes cuestiones como las perspectivas a largo plazo para la obtención y la demanda de agua o la responsabilidad social.

Para Defensa, las decisiones que se tomen y que puedan repercutir tanto al consumo de petróleo como a la

aparición de nuevos combustibles, afectan de manera muy importante. Esto se debe a que dichos combustibles, que por sí mismos juegan un papel estratégico en la economía mundial, para el sector militar son aún más relevantes debido a la existencia de una serie de problemas adicionales, basados principalmente en la logística y en la seguridad de suministro de los mismos.

Tal es su importancia, que la OTAN tiene un órgano asesor en materia logística relativa al petróleo militar, el NPC (NATO Petroleum Committee).<sup>1</sup>

En definitiva, ha sido una buena ocasión para la búsqueda de soluciones a los actuales problemas del sector, relacionadas con los elevados precios del crudo y con la necesidad de encontrar fórmulas más sostenibles y respetuosas con el medio ambiente.

<sup>1</sup> Más información en el Boletín nº 16, "El Reto de los Combustibles en el Sector Militar".

## enlaces de interés

### The Industrial Research and Innovation Website

Página Web sobre la I+i del Joint Research Centre (JRC), de la Comisión Europea. En esta página se puede encontrar información sobre la I+D+i industrial y sus relaciones con el desarrollo económico. Además, se presentan los principales resultados de las actividades llevadas a cabo por el JRC's Institute of Prospective Technological Studies.

<http://iri.jrc.ec.europa.eu/>



# tecnologías emergentes

## VEHÍCULOS DE COMBATE MODULARES: UNA PERSPECTIVA

Col. CIP. Manuel Engo Nogués, OT STN, y Manuel P. Pindado Puerta (Isdefe)

*Large producers of military vehicles frequently use the word “modular” however there can be diverse concepts and grades of “modularity”.*

*The first concept of modularity can be applied to the ease of capacity of adaptation of military vehicles with minimal stress during various missions or operative scenes. The clearest example of this first concept of modularity is the shield addition based on distinct panel types that can be mounted on a basic shield.*

*The second concept of modularity, relates to the modular techniques of manufacturing civil and military vehicles. A modular design facilitates the assembly of the different elements to form the various versions (combat, transport, ambulance, combat engineer, transmissions) reducing cost and time.*

*The third concept or grade of modularity is the newest and most complex. The idea of a modular vehicle is that a large portion of the final configuration can be modified in the operations field facilitating the quick and easy adaptation to the assigned mission. E.g a VCI can convert into a command vehicle by connecting a different mission module to the common module.*

### 1. EL CONCEPTO DE VEHICULO MODULAR

En la publicidad de los principales fabricantes de vehículos militares del mundo aparece frecuentemente el adjetivo modular. Sin embargo, el término modular no siempre tiene el mismo significado o, por expresarlo de otra manera, existen diversos conceptos de modularidad en la oferta actual de vehículos militares,

que podrían también calificarse como “grados de modularidad”.

Un primer concepto de modularidad sería el que aplica el adjetivo modular a la capacidad de adaptación de los vehículos militares, con facilidad y mínimo esfuerzo, a las diferentes misiones y escenarios operativos. Quizás, el ejemplo más claro de este primer concepto de modularidad sea el blindaje añadido, basado en distintos tipos de paneles que se montan sobre el blindaje básico (el casco) en anclajes previstos a tal efecto. Los paneles se diseñan en función del vehículo concreto y las diferentes amenazas y, en consecuencia, así varían sus espesores, diseño y materiales. Esta modularidad del blindaje permite adaptar la protección<sup>1</sup> del vehículo a la amenaza esperada en el escenario en que deba desarrollar su misión, configurando también su peso y su gálibo teniendo en cuenta la influencia de ambos en la movilidad del mismo. Igualmente, esa modularidad permite reemplazar los paneles de blindaje dañados por otros nuevos, renovando así el blindaje en poco tiempo y con poco coste en la propia zona de operaciones. Otro ejemplo de este primer concepto de modularidad lo encontramos en el armamento que puede elegirse en función de la misión. Este es el caso de las modernas torres RCWS<sup>2</sup>, que permiten montar uno o varios diferentes sistemas de armas, tales como

<sup>1</sup> Un ejemplo de sistema moderno modular de blindaje es el AMAP (Advanced Modular Armor Protection), desarrollado por la empresa IBD Deisenroth, aunque existen multitud de otros ejemplos.

<sup>2</sup> RCWS: Remote Controlled Weapon Station, Estación de Armas con Control Remoto.

ametralladoras de diferentes calibres, lanzagranadas automáticos, misiles anticarro, etc.

Un segundo concepto de modularidad es el relativo a las técnicas modulares de fabricación de vehículos civiles y militares. Así, un diseño modular del vehículo facilita enormemente el montaje en fábrica de los distintos elementos para configurar las diferentes versiones (combate, transporte, ambulancia, zapadores, transmisiones, etc.), reduciendo costes y tiempos. En este caso, algunos elementos dependen de la versión del vehículo pero otros muchos son comunes, reduciéndose costes, facilitándose la logística y el mantenimiento. Una vez que el vehículo sale de fábrica su estructura permanece “fija”. Este concepto de modularidad no es nuevo, y todos los fabricantes actuales lo utilizan en mayor o menor medida,

por las ventajas citadas.

Por último y siendo el objetivo principal de esta perspectiva, existe un tercer concepto o grado

de modularidad, que es el más complejo y novedoso, y para el que quizás debiera reservarse el término “vehículo modular”. En

él, la modularidad consiste en que un gran porcentaje de la configuración final del vehículo puede modificarse en el propio campo de operaciones con objeto de adaptarlo a la misión asignada, de forma relativamente rápida y fácil. De esta manera, un VCI (Vehículo de Combate de Infantería) puede convertirse en un vehículo de mando conservando la parte común, llamada “módulo común” o “módulo de conducción”, y acoplando uno específico para esas funciones denominado “módulo de misión”. En



Fig. 1. Boxer 8x8 (ARTEC), mostrando claramente los módulos de conducción y de misión. El módulo de conducción está ocupado por el conductor y el jefe del vehículo y el módulo de misión es intercambiable. ([www.artec-boxer.com](http://www.artec-boxer.com))

estos vehículos el “módulo común” suele estar integrado por la planta motriz, los puestos del conductor y del jefe del vehículo, así como por un chasis portante. El “módulo de misión” se monta sobre dicho chasis, fijándolo y conectándolo de manera apropiada. Esta operación de montaje del módulo de misión debe hacerse con medios disponibles en el teatro de operaciones y en tiempos aceptablemente cortos. Además, no debe olvidarse que la modularidad de esas diferentes versiones significa también que puedan seguir admitiendo, cada una, diferentes sistemas menores, por ejemplo, de blindaje o de armamento, lo que hace al vehículo aún más flexible y configurable.

## 2. VEHICULOS MILITARES MODULARES EN EUROPA

Como se ha adelantado, esta perspectiva se centra en el tercer concepto de modularidad, es decir, en vehículos militares proyectados como suma de un “módulo común” y un “módulo de misión”, por ser el más novedoso. En la actualidad y a nivel europeo existen pocos programas que incorporen este concepto de modularidad, algunos de los cuales se describen a continuación.

### 2.1. PROGRAMA BOXER (ARTEC)

El Boxer es un vehículo 8x8 desarrollado por el consorcio ARTEC para los ejércitos alemán y holandés, cuyas primeras entregas están previstas para mediados del 2009, siendo así el primer vehículo con este concepto de modularidad que entraría en servicio en los ejércitos. Los fabricantes indican un tiempo de cambio entre módulos de menos de una hora.

### 2.2. PROGRAMA SEP (BAE Systems – Hägglunds)

El SEP<sup>3</sup> es un programa sueco con dos versiones: vehículo de cadenas y vehículo de ruedas. La situación actual del programa es incierta. Aparte de la modularidad, también dispondrá de una planta motriz híbrida diesel-eléctrica y de un sistema de transmisión eléctrica. La versión de cadenas tiene previsto montar un nuevo material elástico-

<sup>3</sup> SEP: Splitterskyddad Enhetsplattform o Sistema Blindado Táctico Modular, programa también conocido como Thor.

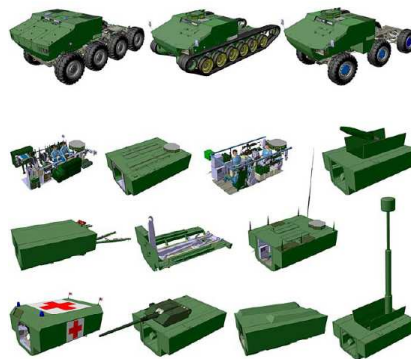


Fig. 2.- Visión esquemática de la familia SEP. Fila superior: tres tipos de módulo común: 8x8, de cadenas y 6x6. Tres filas inferiores: diseños de diferentes módulos de misión. ([www.baesystems.com](http://www.baesystems.com))

mero que mejora las prestaciones de zapatas y ruedas de rodaje.

### 2.3. PROGRAMA GeFaS (Rheinmetall)

De los proyectos conocidos, este es el que parece más ambicioso, aunque también es el previsto a más largo plazo, siendo una iniciativa privada de un grupo de empresas, encabezado por Rheinmetall. El vehículo GeFaS<sup>4</sup> está constituido por tres módulos principales diferentes: un primer módulo que constituye un eje motriz; el segundo módulo que es el paquete de potencia, y un tercero que es el módulo principal. Según Rheinmetall, estos tres módulos se pueden combinar de maneras diferentes sobre el terreno para configurar vehículos de diferentes tipos, llegando a poder montarse el vehículo como 4x4, 6x6 u 8x8 en función del número de módulos de eje utilizados. Las uniones mecánicas y funcionales están normalizadas entre los diferentes módulos para facilitar el ensamblado. La propulsión propuesta es del tipo híbrido diesel-eléctrica<sup>5</sup>, lo que tiene la ventaja de que, al no existir ejes o piezas similares que recorren el suelo del vehículo, dichos ejes no

<sup>4</sup> GeFaS: Geschützttes Fahrzeugsystem o Sistema de Vehículo Protegido.

<sup>5</sup> La implantación de este tipo de propulsión híbrida en vehículos militares está siendo estudiada por los principales fabricantes mundiales de vehículos blindados. Véase, por ejemplo, el programa AHED de General Dynamics.



Fig. 3. Izquierda: vehículo GeFaS en configuración 4x4. Derecha: módulo correspondiente a un eje del GeFaS, donde todos los ejes son motrices e independientes. ([www.rheinmetall-detec.de](http://www.rheinmetall-detec.de))

constituyen un peligro adicional para los tripulantes en el caso de una explosión, que los lanzaría hacia arriba. Aparte de reducir el consumo y aumentar la autonomía, otra ventaja de esta propulsión híbrida es que las baterías permiten el funcionamiento del vehículo sin usar el motor de combustión, bien porque esté dañado, o bien para operar en silencio.

## 3. VENTAJAS E INCONVENIENTES DE LOS VEHICULOS MODULARES

Sin entrar a hacer una valoración, las ventajas atribuidas a este tipo de vehículos modulares por sus fabricantes son las siguientes:

- Mejor transportabilidad, al poderse trasladar los distintos módulos por separado y luego montarse en el escenario de operaciones.
- Mayor adaptabilidad, al poder configurar el tipo de vehículo que sea adecuado a la misión a desempeñar. Los tiempos aproximados que publicitan los fabricantes para la operación de cambio de módulo de misión son de una hora.
- Facilidad de mantenimiento, por varias razones. Primero, al haber un módulo común a todas las versiones la formación del personal de mantenimiento es más sencilla y existe un número mucho mayor de elementos comunes, lo que a la vez facilita

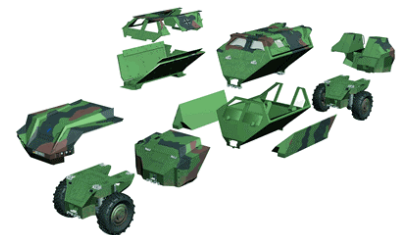


Fig. 4. Despiece de la versión 4x4 del vehículo GeFaS. ([www.rheinmetall-detec.de](http://www.rheinmetall-detec.de))

la gestión de repuestos. Segundo, si un vehículo ha sufrido daños graves en uno de sus módulos, existe la opción de cambiar ese módulo por otro nuevo y enviar el vehículo de nuevo al campo de operaciones, mientras se procede a reparar la parte averiada.

- Facilidad de actualizar el vehículo según vayan apareciendo avances tecnológicos en el futuro, que pueden irse incorporando a los módulos en que sea necesario, pudiendo así alargar la vida en servicio de la plataforma.
- Mejora de la protección contra minas y artefactos explosivos. Esto se consigue porque el módulo de misión es de una sola pieza, independiente del módulo de conducción, y puede montarse a él a través de medios de atenuación de las ondas de choque, e incluso se puede prever que la unión entre ambos módulos se rompa en el caso de una explosión, absorbiendo parte de la energía esa rotura e independizando el módulo de misión del de conducción, que ha recibido la explosión.

No obstante, es de suponer que el diseño de estos vehículos modulares lleve acarreadas una serie de

dificultades potenciales, por ejemplo:

- Complicación en el diseño. La unión del módulo de misión al módulo de conducción no sólo debe ser mecánica, sino que también requiere unir de forma rápida y fiable sistemas tan complejos y variados como son los de comunicaciones, informáticos, electrónicos, hidráulicos, neumáticos, etc.
- Dificultad de la integración de partes móviles entre los diferentes módulos.
- No aplicable a vehículos en servicio. El concepto de modularidad sólo es aplicable, en su máxima extensión, a vehículos nuevos que se diseñen desde cero, por lo que queda reservado para la siguiente generación.
- Requiere un personal muy especializado para realizar el cambio de módulos en la zona de operaciones o un diseño de conexiones "plug and play" muy complicadas.
- Riesgo de que el ataque a un módulo dañe gravemente las conexiones con los demás, dificultando o impidiendo el reemplazo del módulo dañado.
- Riesgos de aumento de peso de los sistemas modulares

frente a los sistemas tradicionales.

- Un mayor coste de adquisición de estos vehículos.
- Dificultad para definir la correcta composición del "parque" de módulos que debe adquirirse o trasladarse a una misión concreta, corriendo el riesgo de sobreestimarlo e incurrir en costes mayores de lo realmente necesario.

## 4. CONSIDERACIONES FINALES

Parece clara la tendencia de algunos fabricantes de vehículos europeos a aplicar en sus futuros diseños el concepto de modularidad descrito en estas líneas.

Resulta difícil, dado lo novedoso del concepto y la escasez de información técnica detallada, valorar si es realmente ventajoso desde los puntos de vista operativo y económico. Habrá que seguir la evolución de estos programas en los años futuros y de los vehículos que se pongan en servicio.

## Sistemas RFID: análisis de la evacuación del buque de guerra

C.F. Ing. José María Riola Rodríguez (SDG TECEN) y C.C. Ing. Francisco J. Pérez Villalonga (GIMO)

*The construction of a warship is an important economic investment for any nation, and can be seen as a demonstration of its technological and Industrial capability. The loss of a naval unit is very difficult and costly to replace, hence a war ship*

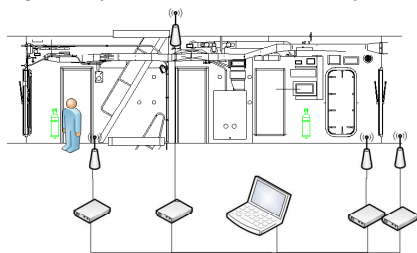


Fig. 1. Sistema de registro de paso

*must maximise its capacity for survival in hostile environments alongside increasing the possibilities of completing assigned missions with success.*

*Although the women and men that serve aboard war ships know the risks, their safety has always been a prime concern when building and operating war ships in service.*

*For most navies, their warships are a limited resource and require an important force in formation and training in order to manage increasingly complex systems.*

*It must be demonstrated from the beginning that the warship has done*

*everything possible to avoid the number of crew casualties aboard a war ship, not just reduce the number of casualties.*

*The Cabinet of Military Investigations of the Navy of Spain (GIMO) together with companies that specialize in control access systems, have developed a System of localization and traceability through radio-frequency identification, that enables an important part of the crews safety, that being the moment of evacuation of the ship, to be analysed.*

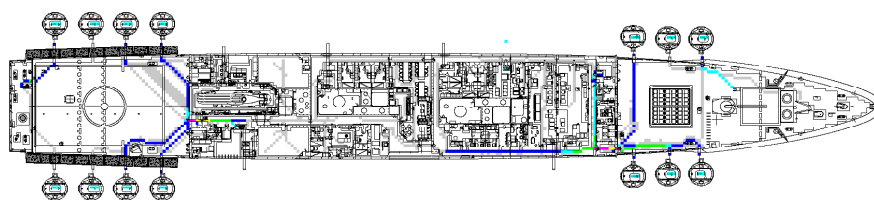


Fig. 2. Representación de las salidas de abandono.

**Introducción**

La construcción de un buque de guerra es, para toda nación marítima, una importante inversión económica y la demostración de su capacidad tecnológica e industrial. La pérdida de una unidad naval, de difícil y costoso reemplazo a corto plazo, puede llegar a suponer una importante merma en su capacidad defensiva. Es por ello que el buque de guerra se proyecta, opera y mantiene para maximizar su capacidad de supervivencia, especialmente en un entorno hostil, e incrementar las posibilidades de cumplir la misión con éxito.

La probabilidad de supervivencia del buque suele depender de los siguientes parámetros:

- Susceptibilidad, es la probabilidad de recibir un impacto,
- Vulnerabilidad, es la probabilidad condicional de no sobrevivir habiendo recibido un impacto,
- Recuperación, es la probabilidad de reparar el buque.

No obstante, nunca será posible asegurar la completa invulnerabilidad del buque ante un ataque. Es el momento de dar por perdido el buque y ordenar el “abandono del buque” para poner a salvo a su dotación. Aunque los hombres y mujeres que sirven a bordo de los buques de guerra conocen y asumen los riesgos que su profesión les exige, su seguridad siempre ha sido un aspecto primordial en el modo de proyectar y operar este tipo de buques mientras están en servicio.

Para la mayoría de marinas occidentales, las dotaciones de sus buques son un recurso escaso, difícil de captar, que requiere un importante esfuerzo en formación y adiestramiento para manejar sistemas cada vez más complejos y que es necesario preservar.

El problema de la seguridad de las dotaciones de los buques de guerra no consiste, hoy en día, en minimizar el número de bajas sino que hay que demostrar, incluso desde las primeras fases del proyecto del buque, que se ha hecho todo lo posible para evitarlas.

El Gabinete de Investigación Militar Operativa de la Armada (GIMO), en colaboración con una empresa especialista en sistemas de control de

acceso, ha desarrollado un sistema de localización y trazabilidad por medio de identificación radiofrecuencia (RFID - *Radio Frequency IDentification*) que permite analizar un aspecto muy importante para la seguridad de las dotaciones como es la evacuación del buque.

**Antecedentes**

Tradicionalmente han sido las grandes catástrofes marítimas y la presión de la opinión pública alarmada por la pérdida de vidas en la mar la que ha impulsado a los gobiernos de las principales naciones marítimas a un esfuerzo legislador que mejore la seguridad de sus buques. Este fue el caso de la primera Convención Internacional para la Seguridad de la Vida en la Mar (SOLAS) celebrada en Londres en 1914, dos años después del hundimiento del *Titanic*. Desde entonces las distintas convenciones celebradas con posterioridad y las resoluciones de la Organización Marítima Internacional (OMI) ha sido el marco regulador por el que se rige la navegación marítima.

A pesar del esfuerzo técnico y legislativo llevado a cabo por OMI, con la notable mejora en la seguridad marítima que esto supone, los buques de guerra están exentos del cumplimiento de esta normativa y no existe en su ámbito ninguna organización equivalente a OMI que en-

tienda a nivel internacional de su seguridad.

No por esto los buques de guerra deben ser considerados menos seguros que los buques de carga y pasaje, solo que queda a juicio de cada nación el nivel de seguridad que ofrece a sus dotaciones.

La falta de un criterio común en materia de seguridad de los países miembros de la OTAN supone una limitación en un contexto en el que es cada vez más frecuente que estos buques sean construidos por astilleros situados en otros países y operen en agrupaciones navales internacionales llevando a cabo misiones conjuntas.

Conscientes de esta limitación, las principales sociedades de clasificación fundan en 2002 la *Naval Ship Classification Association* (NSCA) con el objetivo de promover la seguridad en la mar de los buques de guerra armonizando los distintos estándares. Tras la constitución de la NSCA, el *Naval Armament Group* (NG/6) de la OTAN ofreció un acuerdo de cooperación para elaborar un conjunto de regulaciones similares a las establecidas por la OMI, pero en el ámbito militar.

Este acuerdo marcó el comienzo de los trabajos para la elaboración del *Naval Ship Code* (NSC), inicialmente conocido como Naval SOLAS, y que será el referente en materia de seguridad para construir y operar sus buques de guerra del mismo modo que la Convención SOLAS y la normativa OMI lo es para los buques mercantes.

**La Evacuación del Buque de Guerra**

El NSC dedica el capítulo VII a establecer las normas que deben regir el proyecto, construcción y mantenimiento de los medios que debe disponer un buque de guerra para facilitar el Escape, la Evacuación y posterior Rescate de todas las personas embarcadas (EER). Todo el proceso de abandono debe transcurrir de un modo eficiente y para demostrar que esto es así sugiere emplear la misma metodología que se emplea para el análisis del proceso de evacuación de los buques de pasajeros y que queda recogida en la OMI MSC Circular 1033 *“Interim Guidelines for*

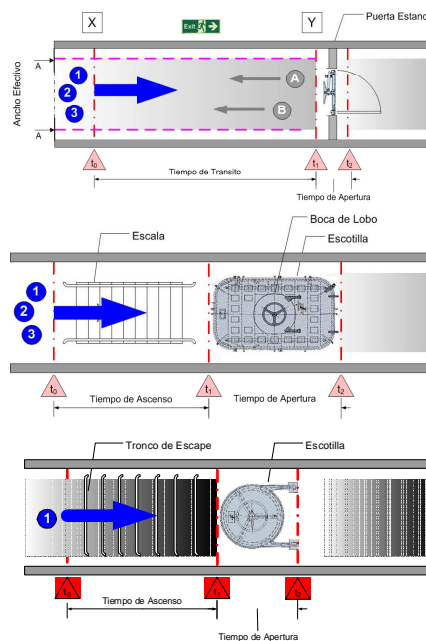


Fig. 3. Esquema de: pasillo con contraflujo; escalera y escotilla, y tranco de escape.

## Evacuation Analysis for New and Existing Passenger Ships

En esta circular quedan perfectamente definidos los parámetros, muchos de ellos derivados del campo de la edificación, que se deben emplear para analizar el proceso de evacuación de un buque de pasajeros por medio de herramientas de simulación.

Sin embargo y a pesar de que existen semejanzas entre ambos tipos de buques, aspectos como las características físicas y el adiestramiento de las dotaciones de los buques de guerra, el procedimiento que siguen durante el abandono e incluso las diferencias de configuración como puede ser el ancho de los pasillos, la inclinación de las escalas o la presencia de puertas y escotillas estancas para garantizar la estanqueidad, hacen pensar que el proceso de evacuación de un buque de guerra puede llegar a diferir notablemente del que tiene lugar en un buque de pasajeros.

El GIMO, con el apoyo de la DGAM, inició a finales de 2007 un programa para el estudio del proceso del abandono del buque de guerra y, en especial, la determinación de las características del movimiento de las dotaciones de estos buques en situaciones de emergencia.

Existen en la actualidad numerosas referencias sobre las características del movimiento de las personas y los factores que en ella influyen, desde los primeros experimentos de Predtechenskii y Milinskii hasta las investigaciones de J. Pauls o Fruin cuyas conclusiones se incorporaron a los estándares técnicos de edificios y que, posteriormente, han influido en la normativa OMI para buques de pasajeros.

### Ensayos a Escala Real

Llegado este punto cabía preguntarse si las características del movimiento de las dotaciones, la velocidad a la que se desplazan por los pasillos y escalas de los buques de guerra, era similar al de las personas que evacuan un edificio de oficinas o, debido principalmente a su edad y adiestramiento, era distinto.

Para ello se llevó a cabo una batería de experimentos a bordo de la Fragata "Asturias", atracada en Ferrol, en los que participaron los

hombres y mujeres de su dotación para los que se contó con la colaboración de la empresa INZACARD, S.L., especializada en sistemas de control de accesos e identificación por radiofrecuencia.

Sobre la cubierta de seguridad interior se definieron tres zonas de ensayos (pasillo, escala y tronco de escape) y se instalaron antenas receptoras RFID de tipo activo, que trabajan en la frecuencia de 125Khz y tienen un alcance de hasta 3m, conectadas a un ordenador portátil.

A cada uno de los participantes se le entregó un tag RFID activo en formato tarjeta lo que permitió registrar el momento de paso e identificar al individuo. Los mejores resultados se obtuvieron por medio de antenas receptoras tipo *loop* situadas sobre la cubierta del buque.

La primera batería de experimentos estuvo encaminada a determinar la velocidad de avance por tramos de pasillo horizontales, la influencia en esta velocidad de las características físicas de los individuos y del número de personas que forman el grupo de evacuados. Adicionalmente se registró el tiempo necesario para abrir y cerrar una puerta estanca.

Una segunda batería de experimentos se realizó en una escala de 60° de inclinación, que permite acceder a la cubierta superior por medio de una escotilla estanca. Los participantes debían ascender por la escala y abrir una boca de lobo para atravesar la escotilla.

Finalmente se llevó a cabo una serie de ensayos en troncos de escape, estructura que permiten la salida desde cámaras de máquinas y compartimentos situados en cubiertas inferiores cuando la salida principal queda inutilizada.

### Conclusiones

Los datos obtenidos en estos ensayos gracias al empleo de lectores y tarjetas RFID han puesto de manifiesto que la velocidad a la que avanzan los miembros de la dota-

ción de un buque de guerra ante una situación de emergencia es muy superior a la que cabe esperar en buques de pasajeros y sugerida en la metodología OMI para el empleo en este tipo de buques.

Estos ensayos han permitido también obtener datos y parámetros sobre los que no existían referencias al ser estructuras típicas de buques de guerra como es la velocidad de ascenso por escalas de 60°, troncos de escape o el tiempo necesario para abrir puertas y escotillas estancas.

La información obtenida fue empleada para establecer las rutas de escape óptimas y simular el proceso de evacuación del futuro Buque de Acción Marítima (BAM) y de las Fragatas "Álvaro de Bazán" reduciendo de este modo las zonas de congestión que retrasan el proceso de abandono del buque.

La tecnología RFID, que ya se está implantando en algunos buques para el control de accesos, ha demostrado su utilidad en el campo de la evacuación permitiendo recopilar datos sobre las características del movimiento de los evacuados y mejorando, en definitiva, la seguridad de las dotaciones de los buques de la Armada.

Esta tecnología permitirá, en el futuro, continuar con el programa de adquisición de datos en situaciones de navegación o baja iluminación sin interferir en el desarrollo de la actividad del buque o el establecimiento de rutas de escape en función de la situación real del personal a bordo.

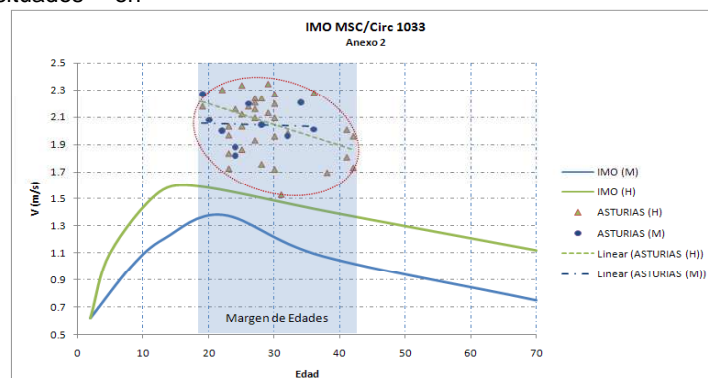


Fig. 4. Tabla de datos de velocidades de la dotación.

# Tecnología en Profundidad

## Conceptos de *middleware*: DDS como tecnología emergente en Defensa

Fernando Cases, OT TICS, Jaime Martín (eProxima) y Gerardo Pardo (RTI)

*This paper introduces the middleware technologies, a sample of an emerging technology, the Data Distributed Service (DDS), and its potential uses in the Defence market.*

*The first section of the paper explains what middleware actually is: a tool for programmers to communicate distributed applications. Further on, it exposes the resources the middleware uses and a classification based on its functionality, offering samples in each category.*

*The second section presents the DDS, a middleware that was designed to work on real time systems. The main features of the DDS are described as well as its conceptual model based on the publish/ subscribe paradigm and the large amount of quality of service (QoS) offered.*

*The last section is dedicated to the illustration of how the DDS fits in to the defence market based on its features. It also shows DDS technology in defence systems all around the world, including within Spanish companies.*

### Qué es un *middleware*

Las aplicaciones informáticas de hoy en día no se ejecutan en un ordenador donde se tiene toda la información necesaria para su ejecución, sino que necesitan información que está presente en otros ordenadores, o bien es información que generan otras aplicaciones situadas en ordenadores remotos. De esta forma surge la necesidad de que diferentes ordenadores se comuniquen con otros.

Las comunicaciones de datos entre ordenadores suelen ser complejas debido a varios factores, entre otros:

- los datos que se quieren enviar son codificados por los diferentes

sistemas operativos (Windows, Linux, Mac,...) de diferente manera.

- los medios de transmisión son de múltiples naturalezas (tarjetas de red, radios, puertos serie,...)
- los lenguajes de programación son diferentes en cada ordenador.
- dos aplicaciones pueden ser desarrolladas por diferentes grupos de programadores.

Por este motivo, la organización de estándares ISO<sup>1</sup> creó una tabla de referencia para enmarcar las comunicaciones de datos en 7 capas. De este modo, la capa 1 denominada "física", trata de encuadrar a las comunicaciones de datos desde un punto de vista de cables, señales eléctricas para codificar bits, frecuencias, etc.; la capa 7 denominada de "aplicación" trata de los datos que usa directamente la aplicación. Este marco se denominó ISO's *Open System Interconnect* (ISO-OSI).

Desde el punto de vista de un programador, cada vez que se encuentre la tarea de realizar un programa que necesite datos de otros ordenadores remotos tendrá que solucionar las comunicaciones en todos los niveles ISO-OSI. Afortunadamente la evolución de las comunicaciones nos ha permitido aislar las capas de más bajo nivel (capas 1 a 4) de tal modo que ese programador no tenga que reprogramar su aplicación en función del medio físico a utilizar, haciendo uso de los protocolos estandarizados que ocultan la naturaleza física. Los protocolos más usados actualmente son los mismos que se usan en la red Internet, o "pila IP"<sup>2</sup> (protocolos que se pueden situar en las capas 3 y 4). El medio físico más usado en un ordenador es la tarjeta de red, la cual está bastante estandarizada, por lo que si se tiene otro medio físico se tendrá que escribir código que adapte su uso a estos protocolos (una capa de comunicaciones físicas).

Una vez fijados los niveles 1 a 4, quedan pendientes los niveles superiores relacionados con la representación de los datos y con las comunicaciones de alto nivel. Aquí es donde surge la idea

de *middleware*. Los *middleware* son desarrollos que se enmarcan en las capas de "presentación" y "aplicación" (6 y 7) dentro de la arquitectura de referencia ISO-OSI (el uso de la capa 5 queda oculto al programador).

El término *middleware*<sup>3</sup> se acuñó en el ámbito de las TIC (Tecnologías de la Información y las Comunicaciones) fusionando las palabras *middle* (medio) y *software*, queriendo hacer referencia a un software especial que se colocaba entre las aplicaciones informáticas y los recursos de comunicaciones (tarjetas de red, radios, módems,... o alguna capa que los represente). En definitiva, se entiende por *middleware* a una herramienta software que ayuda al programador a conectar aplicaciones y/o componentes entre sí, y que puede añadir una serie de herramientas que facilitan el desarrollo de aplicaciones colaborativas y/o distribuidas. En general, los *middleware* sirven para integrar sistemas de información.

### Qué implica un *middleware*

Se indican a continuación las funcionalidades y herramientas comunes que suelen incorporar los *middleware*, aunque no siempre los proveedores proporcionen todas:

1.- Lenguajes de Definición de Datos y Operaciones (LDDO): Una necesidad

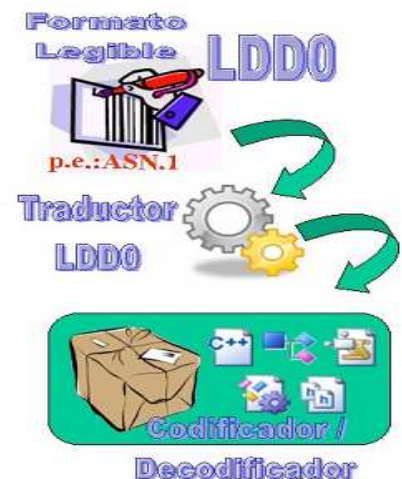


Fig. 1. Proceso de definición de Datos y Operaciones para generar código.

<sup>1</sup> ISO: International Standard Organization.

<sup>2</sup> Internet Protocol.

<sup>3</sup> Se va usar el término *middleware* desde el punto de vista de las comunicaciones, no entrando en otros posibles usos.

común en las comunicaciones entre sistemas / aplicaciones es la definición de los datos que se van a intercambiar y las operaciones entre aplicaciones que se quieren ofrecer. Por este motivo se definen los tipos de datos y las operaciones formalmente mediante un lenguaje de descripción de alto nivel, donde se definen las reglas para la creación de nuevos datos estructurados. Se listan a continuación varios ejemplos de diferentes lenguajes de definición de datos: ASN.1 (*Abstract Syntax Notation #1*), IDL (*Interface Definition Language*), WSDL (*Web Service Definition Language*).

2.- Traductores de LDDO a código fuente: cada tipo de dato definido mediante un LDDO se mapea a los tipos soportados por los diferentes lenguajes de programación, siendo los más usados el C/C++, Java y C#. Estos traductores también se encargan de escribir en cada uno de los lenguajes, las rutinas o procedimientos de alto nivel que el programador usará, así como la traducción de los datos a *wired format*.

3.- Traducción a datos de red (*wired format*): el objetivo es representar los datos en una forma neutra de tal forma que puedan ser interpretados por cualquier plataforma o lenguaje. Un objetivo secundario es mejorar la eficiencia de la transmisión, para ello los datos se formatean y comprimen de

BER (*Packed / Basic Encoding Rules*), XML (*eXtensible Mark-up Language*).

4.- API (*Application Programming Interface*): Funciones y procedimientos propios del *middleware* que al ser usados por el programador envían y reciben información de una forma independiente de los niveles de comunicación inferiores. Cada tecnología y cada fabricante suele definir su propio API, aunque aquellas tecnologías que son estándares fijan sus procedimientos para disminuir la curva de aprendizaje.

5.- Protocolos de aplicación: son la parte de las comunicaciones que implementa mensajes de alto nivel entre aplicaciones, bien sean mensajes de control o de datos. Ejemplos de este tipo son: HTTP (*Hyper Text Transport Protocol*) + SOAP (*Single Object Access Protocol*), IIOP (*Internet Inter-Orb Protocol*), SNMP (*Simple Network Management Protocol*) y CMIP (*Common Management Information Protocol*).

Por debajo de este nivel, los *middleware* hacen uso de las pilas de protocolos de transporte, siendo la más usada (pero no única) la pila IP (UDP, TCP, UDP multicast, ...).

6.- Herramientas de ayuda: aplicaciones gráficas para la realización amigable de las tareas anteriores. Además existen herramientas de más alto nivel para el diseño de *workflows*.

procedimiento o servicio) y le devuelva información. Su uso se realiza bajo el paradigma de cliente / servidor. Ejemplos de este tipo son: las RPC (*Remote Procedure Call*), los *Web Services* y las RMI (*Remote Method Invocation de Java*).

2.- Orientado a Objetos: los objetos son entidades de aplicaciones informáticas que encapsulan datos y agrupan procedimientos sobre esos mismos datos. Las aplicaciones hacen uso de estos objetos locales o remotos mediante el paradigma de cliente / servidor. Ejemplos de estas tecnologías son las EJB (*Enterprise Java Beans*) y el CORBA (*Common Object Request Broker Architecture*).

3.- Orientados a mensajes: las entidades de intercambio de información son publicadores y suscriptores desacoplando la comunicación y enviando mensajes previamente definidos. Como ejemplos de este tipo se pueden nombrar a: JMS (*Java Message Service*), los servicios de eventos y notificación de CORBA, TIBCO *Rendezvous™*, las *IBM MQ Series™* y *Microsoft Message Queues™*, entre otros.

4.- Orientados a datos: variante de la anterior en la que se usa el mecanismo de publicación / suscripción para mantener una memoria compartida en red, en la que los publicadores son los encargados de escribir las variables compartidas y los suscriptores de leerlas. Ejemplos de este tipo son JGroups, DDS (*Data Distribution Service*) del OMG y HLA (*High Level Architecture*), usado en simulación militar.

5.- Mixtos: son tipos de *middleware* que se basan en variantes de los anteriores y también en paradigmas y usos diversos. Por ejemplo: el CORBA *Component Model* (CCM) incluye orientación a objetos y mensajería; las soluciones *Enterprise Application Integration* (EAI) centralizan servicios de llamadas de diferente naturaleza; los *Enterprise Service Bus* (ESB) forman un bus de mensajería para la transmisión de información pero haciendo uso extensivo de adaptadores de las diferentes tecnologías a su bus.

Las necesidades de integración entre los sistemas y la naturaleza de los recursos de comunicaciones dirigirán la elección de un determinado *middleware* basándose en las características descritas anteriormente.

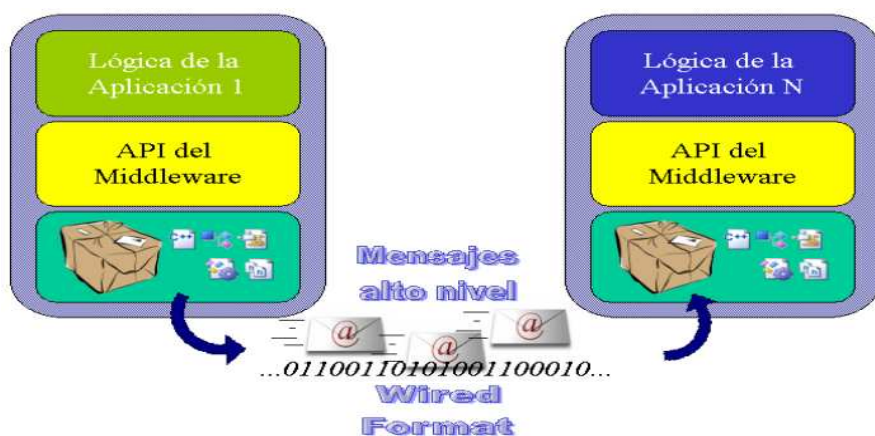


Fig. 2. Dos aplicaciones comunicándose mediante el código generado por el middleware.

manera que la comunicación sea óptima en criterios de tamaño de paquetes y por consiguiente en velocidad de transferencia. De este modo se pueden encontrar: XDR (*eXternal Data Representation*), CDR (*Common Data Representation*), PER y

## Tipos y ejemplos de middleware

Por su naturaleza funcional se pueden clasificar los *middleware*, en un sentido amplio, según la siguiente taxonomía:

1.- Llamadas a procedimientos remotos: su función radica en pedir a otra aplicación que realice una tarea (el



## Distributed Data Service (DDS)

DDS son las iniciales de *Data Distribution Service for Real-time Systems*, una estándar del OMG (*Object Management Group*) publicado en junio del 2003. Es la especificación del API de un *middleware* basado en el modelo de publicación-suscripción, que tiene como objetivo principal los sistemas de tiempo real y es ampliamente utilizado en los sectores de defensa y aeroespacial.

El término "tiempo real" no solo significa alto rendimiento, sino determinismo y predictibilidad. Multitud de operaciones comunes de programación, como reservas de memoria, bucles de espera, sincronización de hilos de ejecución, etc. pueden resultar en un sistema no predecible.

Por tanto, los sistemas distribuidos de tiempo real necesitan un *middleware* de mensajería que proporcione alto rendimiento (baja latencia y alta tasa de transferencia) con un comportamiento predecible y determinista (bajo *jitter*, consumo de recursos de memoria y procesador acotados, etc.)

Por otra parte, un *middleware* predecible y determinista no debe resultar rígido, sino que debe disponer de un buen conjunto de posibilidades de configuración o calidades de servicio que ofrezca flexibilidad y potencia en el diseño del sistema distribuido.

DDS fue diseñado para cumplir esos objetivos: alto rendimiento, predictibilidad y determinismo, altas posibilidades de configuración, y por tanto es la elección más recomendable en los sistemas distribuidos de tiempo real crítico.

El modelo de publicación-suscripción permite una comunicación asíncrona, mejorando la latencia y la tasa de transferencia frente a los sistemas síncronos, que deben hacer una petición síncrona de los datos. Esto es especialmente interesante a la hora de transmitir eventos, comandos o alarmas.

Por otra parte, el diseño del API de DDS, está pensado para hacer que las diferentes implementaciones sean predecibles y deterministas, aportando un conjunto de parámetros de configuración que permiten fijar con exactitud los recursos que consumirá DDS, tanto en

términos de memoria, como en términos de CPU.

DDS dispone de un rico conjunto de calidades de servicio (QoS), que permiten regular, priorizar y dar forma a los flujos de datos en una red, haciendo sencillo resolver los problemas más comunes de diseño que se presentan en un sistema distribuido.

DDS usa el protocolo RTPS (*Real Time Publish-Subscribe Protocol*), también

en el *topic*, que sirvan de clave, DDS usará esta clave para ordenar los datos, posibilitando que una aplicación pueda pedir al *middleware* los datos que coincidan con una clave determinada, para tratarlos de forma independiente al resto. Por ejemplo, el *topic* puede ser la posición de un vehículo, y la clave el identificador del vehículo, de forma que no es necesario crear un *topic* para cada vehículo.



Fig. 3. Modelo simplificado de comunicaciones ofrecido por el API de DDS

estándar del OMG y del IEC (*International Engineering Consortium*). RTPS está pensado para escenarios con pérdidas de paquetes y conectividad, y define su propio sistema de control para garantizar la fiabilidad de las comunicaciones. Al ser una especificación pública y abierta, RTPS sirve como protocolo de interoperabilidad entre distintas implementaciones, posibilitando la comunicación entre ellas.

### Modelo Publicación-Suscripción

DDS usa el concepto de espacio de datos global (véase la Figura 3), en este espacio de datos se definen "asuntos" o *topics* (posiciones de distintos objetos, alarmas, comandos, mediciones de sensores, etc.), y los distintos participantes en el sistema distribuido simplemente declaran su interés en publicar o suscribirse a dichos *topics*. Es posible que distintas aplicaciones coexistan aisladas en el mismo sistema, usando diferentes espacios de datos o dominios para cada aplicación.

La estructura de los datos de los *topics* se define usando un lenguaje de definición de datos estándar del OMG, denominado IDL, cuya sintaxis es muy similar a la definición de datos en C++. Es posible definir uno o varios campos

Una cualidad importante de este modelo, es el hecho de que las suscripciones están desacopladas de las publicaciones en varias dimensiones:

- **Localización:** Los publicadores no necesitan conocer la localización de los suscriptores y viceversa, es decir, no se necesita configurar las direcciones de los nodos, independizándolo de la topología de la red, y permitiendo un sistema "plug & play" al que se pueden añadir participantes "en caliente": el descubrimiento de los distintos participantes es automático, no siendo necesario una configuración previa o un servidor de descubrimiento.
- **Redundancia:** Es posible que se suscriban a los mismos datos diferentes suscriptores, así como que se escriban desde distintos publicadores. Esto se controla de forma transparente por parte del *middleware* posibilitando configurar los escenarios típicos de redundancia de forma sencilla.
- **Tiempo:** La recepción de los datos es asíncrona, no es necesario que el suscriptor realice una petición por cada dato que quiere recibir, sino que se le avisa cuando hay

## tecnología en profundidad

datos disponibles. Incluso un suscriptor puede, si se le configura a tal efecto, recibir datos que fueron escritos incluso antes de que este suscriptor se añadiera a la red.

- **Plataforma:** Las aplicaciones no se tienen que preocupar de la representación de los datos, la arquitectura del procesador, el sistema operativo, o incluso el lenguaje de programación usado en el otro lado de la comunicación. Es posible por ejemplo publicar en un nodo de tiempo real (por ejemplo VxWorks, QNX, Integrity) en C, y suscribirse desde un nodo en Linux usando Java, y/o otro en indows usando C# bajo .net, etc. Un lado no se tiene que preocupar de los detalles del otro.
- **Implementación:** DDS dispone de un protocolo de interoperabilidad, también estándar del OMG, denominado RTPS, de forma que incluso cada lado de la comunicación puede usar una implementación diferente del estándar.

Es importante también recalcar, que aunque el estándar no lo impone, las principales implementaciones no hacen uso de servidores intermedios que actúen como canalizadores de mensajes, de forma que el desacoplamiento es completo, y se evitan los puntos calientes (*single point of failure*): un fallo en un nodo no afecta a todo el sistema.

### Calidades de servicio (QoS)

Las publicaciones y suscripciones establecen contratos de calidad de servicio (QoS) para los datos, regulando el flujo de datos en la red. Existen multitud de calidades de servicio disponibles, siendo destacables:

- **Calidades de Servicio de Entrega de datos:** Definen el grado de fiabilidad de las comunicaciones y la frecuencia de envío de los datos. DDS dispone de dos modos de comunicaciones, uno denominado "*Best Effort*" que no garantiza la entrega, y el denominado "*Reliable*" que si la garantiza, incorporando un protocolo de control basado en ACKs/NACKs. Dependiendo de la naturaleza de nuestros datos usaremos uno u otro, por ejemplo, para los datos de un sensor de temperatura que se

actualizan con frecuencia, podríamos usar el modo *Best Effort*, que ahorra ancho de banda minimizando la latencia y maximizando la tasa de transferencia, y para ordenes o comandos podríamos usar el modo *Reliable*, que garantiza la entrega en el mismo orden que fueron enviados.

- **Calidades de servicio de Volatilidad de los datos:** Permiten configurar la persistencia de los datos en el espacio de datos global y su caducidad temporal, con opciones para que los datos persistan en memoria o en disco.
- **Calidades de servicio de Redundancia:** Permiten configurar de forma sencilla los escenarios comunes de redundancia en la publicación y en la suscripción, posibilitando una tolerancia a errores completa.

### Empaquetado y transmisión de los datos

Como se comento anteriormente, DDS usa un lenguaje de definición de datos estándar, denominado IDL, que define una correspondencia entre sus tipos y los de los lenguajes más extendidos (C, C++, Java, Ada...). Esto permite que el programador no tenga que preocuparse de en que lenguaje están escritos los diferentes participantes de su sistema distribuido: los tipos serán compatibles. Incluso existe un mapeo entre IDL y los tipos usados en SQL (*Structured Query Language*), lo que unido al hecho de que el modelo de datos de DDS incorpora claves (*keys*), permite pensar en el espacio de datos global de DDS como una gran base de datos distribuida. Existen herramientas que permiten integrar DDS con bases de datos relacionales de tiempo real de forma sencilla y transparente.

No obstante, en cada plataforma la representación interna de estos tipos puede ser distinta, y es necesario a la hora de transmitir los datos serializarlos en un formato independiente de la plataforma. Para resolver este problema, DDS usa CDR, también estándar del OMG. El CDR es un formato que es muy eficiente en términos de uso de ancho de banda y la serialización/deserialización de los datos a este formato consume muy poco tiempo de proceso. Por tanto, es el formato de elección en sistemas

distribuidos con baja disponibilidad de ancho de banda y conectividad pobre, y/o en aquellos con requerimientos de tiempo real críticos.

Para transmitir esos datos empaquetados en CDR, DDS usa como protocolo el RTPS, un protocolo diseñado para escenarios de conectividad pobre y escaso ancho de banda. RTPS puede ser implementado sobre distintos protocolos subyacentes, y las principales implementaciones de DDS, implementan RTPS sobre UDP (v4 y v6), en versiones *unicast* y *multicast*, y sobre otros menos difundidos.

### Implementaciones disponibles

Actualmente existen varios vendedores que ofrecen productos que desarrollan DDS. Los más importantes son:

- **Real Time Innovations (RTI):** esta empresa ha sido parte clave en la definición de los estándares DDS y RTPS. Su producto RTI DDS es una implementación de DDS disponible en C/C++, Java, Ada, C# y en más de 30 plataformas distintas. Además dispone de todo un conjunto de herramientas alrededor de DDS: herramientas de integración con bases de datos, herramientas de monitorización, interoperabilidad con CORBA, etc. RTI es la única implementación con presencia en España, mediante la empresa eProxima, su

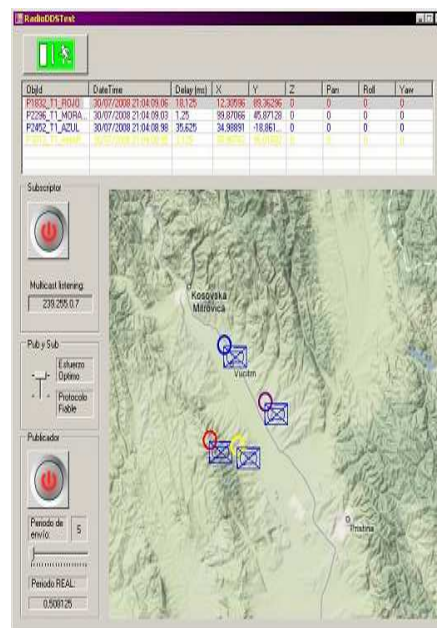


Fig. 4. Prototipo conceptual de uso del DDS en una aplicación de seguimiento de fuerzas amigas.

distribuidor oficial.

- **PrismTech:** empresa que ofrece el producto OpenSplice DDS como un integrante más de su cartera.
- **Otros:** Milsoft y Twin Oaks Computing son dos empresas que también venden productos DDS, aunque con menos presencia en el mercado.
- **Software libre:** existe un grupo de desarrollo de software libre que ha desarrollado un producto denominado OpenDDS, escrito en C++.

## DDS en Defensa

Las aplicaciones de defensa tienen habitualmente requisitos muy exigentes: mínima latencia, tolerancia a fallos, enlaces de comunicaciones poco fiables, poco ancho de banda disponible, recursos de hardware limitados, múltiples plataformas... En este tipo de escenarios DDS encaja perfectamente:

- La pequeña "huella" (*footprint*) o eficiencia entre datos reales (*payload*) y uso de la red, junto con características como el uso del *multicast* le muestran como un candidato serio a explorar en aplicaciones donde la velocidad de transferencia sea limitada. Ejemplo de este tipo sería cualquier aplicación que deba enviar datos a través de radios tácticas.
- Las características de comunicaciones fiables, de tiempo real (que asegure tiempos) y distribución presenta al DDS como tecnología aplicable en sistemas C4ISR (*Command & Control, Communication, Computer, Intelligence, Surveillance, and Recognition*), donde la información puede venir de múltiples fuentes, pudiéndose crear modelos relacionales y/o jerárquicos de datos distribuidos.

Resumiendo los puntos anteriores se puede apuntar que el DDS puede ser una tecnología aplicable a todo el entorno NEC (*Network Enable Capability*), desde los sistemas de bajo y alto nivel hasta aquellos sistemas generales dentro de esta filosofía.

Desde el punto de vista de las aplicaciones actuales, se pueden aportar los siguientes ejemplos:

- **Sistemas de gestión de combate naval:** el TCEI (*Total Ship Computing Environment Infrastructure*) de Raytheon usa RTI DDS, o el TACTICOS de Thales, usa OpenSplice DDS. Un ejemplo interesante para España es el AEGIS de Lockheed Martin (RTI DDS) usado en multitud de barcos, incluyendo la nueva F105 de Navantia, actualmente en desarrollo.
- **Futuros Sistemas de Combate:** como el FCS (*Future Combat System*) de Estados Unidos que usa para las comunicaciones una arquitectura denominada SOSCOE (*System of Systems Common Operating Environment*), basando sus comunicaciones en RTI DDS. SOSCOE integra los distintos sistemas de FCS, conectados mediante enlaces de todo tipo (radio, satélite, líneas terrestres, etc.).
- **Sistemas de control en barcos y aviones:** como el famoso AWACS (*Airborne Warning and Control System*) de la fuerza aérea estadounidense.
- **Aviones, barcos y submarinos sin piloto:** controlados remotamente a través de enlaces de radio o sonar. Ejemplos de este tipo son el Predator y el BlueFin.

En España empresas como Navantia (fragata F105 - Aegis), INDRA (tráfico aéreo), EADS (aviones sin piloto), GMV (comunicaciones tácticas sobre

diferentes enlaces), Nextel (simulación) ya usan DDS, y existen numerosos proyectos donde se está evaluando su uso, siendo destacable el trabajo realizado por los Laboratorios Tecnológicos de la DGAM (Dirección General de Armamento y Material) para la evaluación de DDS en las radios tácticas del Ejército de Tierra, las PR4G.

## Conclusiones

Los *middlewares* son un punto esencial en la interoperabilidad entre sistemas y, en el entorno de Defensa, son la base tecnológica de obtención de capacidades de operación en red NEC. Los *middleware* están pensados para que el programador no pierda el tiempo programando actividades de comunicación repetitivas y de bajo nivel, por lo que aíslan los niveles 1 a 4 de ISO OSI. El DDS es un ejemplo de *middleware* orientado a datos que comunica aplicaciones mediante el paradigma de publicación/suscripción. Además, se ajusta a los requisitos de las aplicaciones de dispersión de la información con un amplio abanico de calidades de servicio configurables. Por tanto encaja perfectamente en el ámbito de Defensa, sobre todo en entornos estratégicos y operacionales, o incluso, en las redes de propósito general allí donde sea necesaria la compartición de datos. En particular debería tenerse en cuenta como una tecnología capaz de desarrollar en todo o en parte la infraestructura tecnológica NEC. Aunque esta tecnología este emergiendo, se puede decir que el mercado esta maduro, ya que existen diferentes vendedores del producto e integradores que la están utilizando, creando sistemas en aplicaciones para Defensa.

## agenda

### 3rd International Seville Conference on Future-Oriented Technology Analysis (FTA)

16 y 17 de octubre de 2008.  
Sevilla (España)

[http://forera.jrc.ec.europa.eu/fta\\_2008/intro.html](http://forera.jrc.ec.europa.eu/fta_2008/intro.html)

### RTO NATO MEETINGS:

#### RTO 10th Anniversary and NATO R&T Day

Del 21 al 23 de octubre de 2008.  
Bruselas (Bélgica)

#### HFM-167 Lecture Series on "Psychological Support Across the Deployment Cycle"

Octubre, 2008. (España)

### SET-166 Lecture Series on "Low Cost Navigation Sensors and Integration Technology"

Octubre, 2008. (España)

### SAS-072 Specialists Meeting on "Capability-Based Long Term Planning"

Octubre, 2008. (Noruega)

<http://www.rto.nato.int>

# Boletín de Observación Tecnológica en Defensa

Disponible en <http://www.mde.es/dgam/observatecnoF.htm>