Boletín DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA

SUBDIRECCIÓN GENERAL DE PLANIFICACIÓN, TECNOLOGÍA E INNOVACIÓN
Boletín de Observación Tecnológica en Defensa n.º 67 • 4.º trimestre de 2020

DIAR y DIFI, los nuevos sistemas de medida de firmas radar e infrarroja de la Armada

Seguridad en el Software Aeronáutico

Material de Sanidad para el Entorno Operativo de 2035

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO en línea: 083-15-183-4
NIPO impresión bajo demanda: 083-15-182-9
ISSN edición electrónica: 2444-4839

Autor: Sistema de Observación y Prospectiva Tecnológica (SOPT), Subdirección General de Planificación, Tecnología e Innovación (SDGPLATIN) de la Dirección General de Armamento y Material (DGAM). Paseo de la Castellana, 109, 28046 Madrid; teléfonos: 91 395 52 14 (Dirección), 91 395 52 80 (Redacción); observatecno@oc.mde.es.

Colaboraciones y suscripciones:
observatecno@oc.mde.es

http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/Paginas/SOPT.aspx

Catálogo General de Publicaciones Oficiales:
https://cpage.mpr.gob.es

Catálogo de Publicaciones de Defensa:
https://publicaciones.defensa.gob.es

SOPT

DGAM
Subdirección General de Planificación, Tecnología e Innovación

CONTENIDOS

ESTRATEGIA DE TECNOLOGÍA E INNOVACIÓN PARA LA DEFENSA (ETID 2020)

Como consecuencia de los trabajos llevados a cabo a lo largo de 2019 y 2020 por la DGAM, a finales de este año 2020 se ha publicado una nueva versión de la Estrategia de Tecnología e Innovación para la Defensa (ETID-2020), documento concebido para dirigir las actuaciones e inversiones en I+D+i del Departamento, la cooperación tecnológica en I+D+i, tanto a nivel nacional como internacional, así como para promover la mejora continua de los procesos del Departamento relacionados con el desarrollo de tecnología de aplicación a defensa.

Se trata de una estrategia que responde al conjunto de cambios que se han venido produciendo en los últimos años en el panorama internacional de la defensa, tales como la aparición o potenciación de nuevas amenazas para la seguridad y la defensa, la consolidación de las iniciativas de cooperación a nivel europeo o el vertiginoso avance tecnológico que está cambiando de forma radical la manera de vivir de la sociedad, ofreciendo nuevas posibilidades en beneficio del desarrollo de las capacidades militares.

La ETID 2020 desarrolla la Política de I+D+i del Departamento, la cual responde a dos grandes objetivos que dan sentido a todas sus actuaciones. Por un lado, el desarrollo de las capacidades militares a través de la tecnología para proporcionar una ventaja operacional a las FAS. Por otro, el apoyo a la capacitación tecnológica de la base tecnológica e industrial nacional, para que actúe como suministrador de los materiales y equipos que necesitan las FAS en sus misiones, aportando libertad de acción en el empleo de las capacidades militares.

La nueva estrategia se sustenta sobre tres pilares, que dan soporte a un conjunto de actuaciones tecnológicas y de gestión que se espera poner en práctica durante los próximos seis años.

El primer pilar, el de OBJETIVOS TECNOLÓGICOS, identifica las prioridades tecnológicas hacia las que dirigir los principales esfuerzos en I+D+i. Estos objetivos tecnológicos se organizan en tres niveles, en función de la dimensión y características de los sistemas y tecnologías involucradas y el tipo de actuaciones previstas para su consecución, los cuales se realimentan entre sí.

Así, el nivel superior promueve el desarrollo de tecnologías para ser incorporadas a las futuras grandes plataformas y sistemas de armas en los ámbitos terrestre, naval, aéreo y espacial. Por su parte, el nivel intermedio, se centra en abordar los principales retos tecnológicos presentes en los escenarios más complejos en los que tienen que operar las FAS. Y finalmente, el nivel inferior, apuesta por realizar vigilancia tecnológica en torno a los avances en un conjunto de tecnologías emergentes y de baja madurez tecnológica con potenciales efectos disruptivos.

El segundo pilar de la ETID pone el foco en la COOPERACIÓN TECNOLÓGICA tanto a nivel nacional como internacional, como elemento clave y fundamental para llevar a cabo las actividades de I+D+i necesarias para alcanzar estos objetivos tecnológicos.

En un contexto nacional, la ETID prevé avanzar en la coordinación con el resto de organismos públicos responsables de fomentar la investigación científica y técnica y la innovación, tanto estatales como regionales, para buscar las sinergias necesarias que favorezcan crecientes grados de financiación de tecnologías de uso dual. El hecho de que la ETID constituya la estrategia sectorial de defensa, dentro de la nueva Estrategia Española de Ciencia, Tecnología y de Innovación (EECTI 2021-2027), asumiendo sus principios y planteamientos, facilita ese acercamiento entre las inversiones púbicas en I+D+i duales y las necesidades del sector de la defensa. A su vez, en el ámbito internacional, la estrategia centra sus esfuerzos en aprovechar las nuevas oportunidades para el sector de la defensa a nivel europeo, en torno al Fondo Europeo de Defensa (EDF) y el Programa Europeo de Investigación en Defensa (EDRP), el cual va a constituir una de las principales vías de capacitación del tejido tecnológico nacional durante la próxima década, a través de actividades de I+D+i.

Finalmente, el papel central que juega el MINISDEF en el desarrollo de tecnologías de aplicación a defensa da sentido al tercer pilar, el de MEJORA CONTINUA, que promueve la excelencia en el Departamento a través de la mejora de sus procesos asociados a la I+D+i, para que actúen como catalizadores del desarrollo tecnológico del sector de la defensa.

Este enfoque integrar para abordar el desarrollo tecnológico en el sector de la defensa supone una apuesta decidida del Departamento para abordar los retos que depara esta nueva década, todo ello en beneficio del fortalecimiento de la defensa nacional y del desarrollo de la base tecnológica e industrial y de la sociedad en general.

Actualidad

¿Dónde hemos estado?

14 y 15 de octubre de 2020

Taller "10" de la Fuerza 2035: Jornada sobre Material de Sanidad.

La dirección de Adquisiciones (DIAD) del Mando de Apoyo Logístico del Ejército (MALE), junto con la SDG de Planificación Tecnología e Innovación (PLATIN), llevó a cabo mediante videoconferencia el Taller "10" de la Fuerza 2035 bajo la temática "Material de Sanidad", que estuvo centrado en el sistemas, equipos, materiales y soluciones para las necesidades específicas de la fuerza desplegada. El taller reunió expertos del ámbito militar e industria (empresas, universidades, centros de investigación…) para dar a conocer las necesidades de unos y las capacidades de otros respecto a soluciones de material sanitario en roles 1 y 2, principalmente. El objetivo último de las jornadas de la Fuerza 2035 es aunar los intereses de usuarios finales e industria para orientar eficazmente los esfuerzos nacionales en I+D+i.

19 y 20 de octubre de 2020

Webinar "*Military PNT" Enhancing Resilience and Capability for Warfighting PNT Systems - SMi U*)

El grupo SMi (UK) organizó a lo largo de dos días una serie de conferencias virtuales para proporcionar una visión en profundidad de la tecnología de navegación por satélite. Con proyecciones que estiman que una interrupción del GPS de 30 días podría costar a la industria estadounidense 45.000 millones de dólares, la necesidad de un PNT robusto, resistente y seguro es una misión imperativa para las Fuerzas Aéreas, el Ejército de Tierra y la Armada. Esto adquiere mayor importancia en un momento en que la constelación de Galileo está comenzando a alcanzar su capacidad operativa total y el Reino Unido está explorando alternativas a este sistema de radionavegación tras su salida de la Unión Europea. Existe una necesidad clara y apremiante de que los ejércitos nacionales, los socios industriales y las naciones aliadas se reúnan y discutan cómo se desarrollarán y utilizarán los sistemas globales de navegación por satélite. Se pueden destacar algunos de los participantes, tales como: UK MoD, UK *Space Agency*, UK *National Physical Laboratory*, DGA, *Fraunhofer Institute for integrated Circuits* iiS, US Army, US *Air Force, Finish Geospatial Research Institute* (FGI), CNES, *Italian Defence General Staff*, ESA, *Galileo Services*, o DARPA.

… entre otros eventos

¿Dónde hemos estado?

27, 28 y 29 de noviembre de 2020

Webinar III Congreso de ingeniería espacial. El espacio, la última frontera – EIE Madrid

Durante estos tres días España Ingeniería Espacial (EIE) organizó una serie de conferencias virtuales de gran interés sobre este sector. Alineados con los Objetivos de Desarrollo Sostenible (ODS), se analizó la capacidad del sector espacial y la evolución en la ingeniería de este área para lograr avances en la consecución de dichos objetivos, así como su aplicación para la mejora de la sociedad. Se hicieron visibles los desarrollos en I+D+I y se dió a conocer la participación y las capacidades españolas y la de nuestros profesionales en misiones y proyectos nacionales e internacionales, permitiendo una evaluación de la situación actual del sector (Observación de la Tierra, Comunicaciones, New Space, Lanzadores, Basura Espacial, Segmento Terreno, entre otros).

10, 11 y 12 de noviembre de 2020

Webinar "*Global MilSatCom 2020*" - SMi UK

La edición vigesimosegunda de la conferencia anual "*Global MilSatCom*" ha tenido lugar este año de manera virtual Organizada por SMi (UK), y durante tres días, ha tenido como objetivo discutir los desafíos clave y desarrollos en la industria SATCOM y proporcionando un foro que permite trabajar juntos para ofrecer el futuro de la conectividad por satélite a nuestras fuerzas armadas. El primer día se centró en el programa SKYNET de la nación anfitriona, dado que SKYNET 5 llega a su fin en 2022 y evoluciona a SKYNET 6, todo ello desde la perspectiva del Ministerio de Defensa y de la industria. Cabe destacar la participación de la DGAM entre los conferenciantes, que presentó sus programas espaciales, centrándose en la nueva generación de satélites de comunicaciones militares, SPAINSAT NG. El segundo día comenzó enfocado a las tecnologías disruptivas en el espacio, destacando la necesidad de una innovación tecnológica rápida, y demostró el poder comercial del espacio para acelerar el desarrollo en todos los ámbitos. Finalmente, el tercer día se centró en las actualizaciones clave de los socios internacionales, cubriendo temas clave que incluyen resiliencia y capacidad híbrida de SATCOM, así como el impacto de las megaconstelaciones LEO emergentes para la conectividad Global MILSATCOM.

del 30 de noviembre al 4 de diciembre de 2020

XIV Jornadas STIC CCN-CERT

Estas jornadas, organizadas por el Centro Criptológico Nacional, tuvieron lugar a través de una retransmisión online donde se reunió toda la comunidad que interviene en la salvaguarda del ciberespacio nacional, así como empresas y universidades. En ellas se abordaron diversos temas de interés en el sector de la ciberseguridad, tales como: ciberinteligencia, operaciones militares en el ciberespacio o el cumplimiento normativo del esquema nacional de seguridad.

Toda la información sobre estos y otros eventos puede consultarse en el Portal de Tecnología e Innovación del Ministerio de Defensa: www.tecnologiaeinnovacion.defensa.gob.es

… entre otros eventos

Material de Sanidad para el Entorno Operativo de 2035

Autor: Nuria Aboitiz Cantalapiedra, OT NBQ, SDG PLATIN.

Palabras clave: Fuerza 2035, Sanidad, materiales, biosensores, telemedicina, evacuación, biotecnología, robótica.

Metas Tecnológicas relacionadas: MT 9.2.1; MT 9.3.1.

Introducción

Ante el cambio que se viene observando durante los últimos años en el entorno operativo, el Ejército de Tierra (ET) ha visto necesario realizar un ejercicio de reflexión sobre las características de dicho entorno previsibles para el 2035, los posibles escenarios de actuación y los cambios que deberá afrontar para adaptarse y conseguir una ventaja operativa.

Este ejercicio de prospectiva forma parte del concepto Fuerza 2035, que el ET articula bajo la Directiva 03/18 "Estudios Fuerza 2035 y Brigada Experimental".

En este contexto, el Mando de Apoyo Logístico del Ejército (MALE) está llevando a cabo talleres que abordan un tema concreto y permiten el encuentro del ET con la Base Tecnológica e Industrial de Defensa (BTID), para intercambiar información sobre los intereses y necesidades de unos y los desarrollos y capacidades tecnológicas de otros.

Así, los pasados días 14 y 15 de octubre, tuvo lugar el Taller "10" sobre Material de Sanidad a través de videoconferencia, organizado con la colaboración de SDG PLATIN, dado el alto componente tecnológico del contenido, y de CDTI, por las posibilidades que ofrece para el desarrollo de proyectos de I+D+i de interés dual.

Primera Jornada

El primer día del Taller se inició con una presentación de los canales de colaboración de CDTI con Defensa (proyectos duales y proyectos finalistas) y de otras convocatorias de desarrollo relacionadas con la salud, como la reciente convocatoria centrada en proyectos para la lucha contra COVID-19.

Seguidamente, el GEMALE, el DIRAD y el GESUBSAR dieron unas palabras de bienvenida remarcando el interés transversal de este taller en Defensa, la dualidad (civil y militar) de los temas de sanidad, el sentido finalista de los talleres en cuanto que el objetivo final es la obtención de material, la importancia de la colaboración y alianza de empresas y universidades con el Ejército y la orientación expedicionaria en la búsqueda de soluciones a nuevos retos de la "Fuerza 2035".

Por su parte, el Col. Jefe de la DIVPLA/C2F35 del MALE enmarcó la iniciativa

Fig. 1. Taller 9 Defensa NBQ. (Fuente: MINISDEF).

del evento mediante una introducción sobre el concepto Fuerza 2035 y la Brigada Experimental (BRIEX), describiendo los escenarios a los que se enfrentará la Fuerza (múltiples, complicados y mixtos) y presentado la "Brigada 35" como referente para este nuevo tipo de combate.

A continuación, desde la Brigada de Sanidad, la Col. Hernández Frutos expuso la previsión de necesidades y requerimientos de la Fuerza desplegada respecto a medios y tecnologías para la atención sanitaria en zona de operaciones. La ponencia estuvo centrada en:

i) las claves del cambio de perfil de materiales (se buscan materiales ligeros, miniaturizados, duraderos, amarrables, trasladables, adaptables a nuevas tecnologías y procedimientos y resistentes a golpes, temperaturas extremas, humedad, polvo, contaminantes, descontaminantes, por entre otros)

ii) la unificación e interoperabilidad de los apliques de equipos (tamaños, terminales eléctricos, electrónicos y físicos, pasos de rosca y sistemas de perfusión), que deben estar previstos en los PPT y en las adquisiciones

iii) las capacidades en los puntos remotos a los que se debe llegar (simplificación, miniaturización, automatización, movilidad y protección del material sanitario y electromedicina, seguridad y banda suficiente en las comunicaciones para telemedicina, trazabilidad de bajas, realidad aumentada, entre otros.)

iv) la interacción e integración en el marco de las diversas unidades (compatibilidad con las plataformas de todos los ejércitos, adaptación de helicópteros para traslado de bajas, cobertura para todos los agentes lesivos convencionales y NRBQ, rapidez de despliegues, etc.).

También el Col. Juberías, Jefe del Centro Militar de Farmacia de la Defensa, hizo una presentación de las capacidades del Centro, encargado de la producción, abastecimiento y mantenimiento de los recursos farmacéuticos de las FAS y laboratorio de referencia de antídotos y medicamentos para la salud pública. El coronel esbozó antídotos y terapias contra agentes NRBQ y algunos proyectos que tienen en marcha o esperan poner en marcha próximamente, como desarrollos de formas farmacéuticas para administración de yoduro potásico y DTPA-Ca o síntesis de azul de Prusia para decorporación de isótopos radiactivos.

Análogamente, el Col. López Colón, Jefe del Instituto de Toxicología de la Defensa, presentó las capacidades y funciones del Instituto relacionadas con la defensa sanitaria para agentes de guerra química, el desarrollo de medicamentos en cooperación con los ensayos clínicos de los servicios médicos y epidemiología, toxicología y análisis de riesgo. Además, es laboratorio de referencia de drogas de abuso y sustancias psicotrópicas y de agresivos químicos de guerra en muestras biológicas.

Finalmente, Dña. Cecilia Hernández expuso las oportunidades e instrumentos de financiación de CDTI en el ámbito de la salud.

Segunda Jornada

La presentación de capacidades y proyectos de I+D de empresas, universidades y centros tecnológicos ocupó el segundo día del Taller, en el que se presentó una amplia variedad de tecnologías punteras para atención médica extra-hospitalaria por parte de entidades como TEDCAS, AWE Pharma Group, IDONIAL, SDLE, AGRENVEC, Hospital Gómez Ulla y las Universidades de Sevilla, Málaga y Complutense de Madrid. Entre dichas tecnologías destacan equipos para monitorización y estabilización de bajas, biosensores, equipos de apoyo al diagnóstico, robótica quirúrgica, realidad aumentada para telemedicina, UAS para evacuación de bajas, desarrollo de materiales para test rápidos de COVID-19 o impresión 3D de repuestos quirúrgicos y bioimpresión para medicina regenerativa.

Conclusiones

Se está llevando a cabo un notable esfuerzo de previsión y preparación para que el Ejército pueda hacer frente a los retos de los futuros escenarios operacionales en materia de sanidad. A pesar de no poder celebrarse de forma presencial, el Taller "10" sobre Material de Defensa alcanzó con éxito su objetivo de acercar las capacidades de la BTID a los usuarios finales de Defensa.

Fig. 2. Maniquí desfribilador. (Fuente: MINISDEF).

Participación del Departamento de Sistemas de Defensa NBQ del INTA-Campus de La Marañosa en proyectos de la Comisión Europea ISF-P: BULLSEYE y MALL-CBRN

Autores: María Victoria Ortega García, Juan Manuel Moreno Sobrino, Alfredo Gil Laso, Juan Carlos Cabria Ramos, INTA-SISTTER, Dpto. Defensa NBQ; Olga Bassy Álvarez, ISDEFE.

Palabras clave: alimentos, armonización, espacios públicos, primeros intervinientes, riesgos NRBQ y explosivos.

Metas Tecnológicas relacionadas: MT 10.2.1; MT 10.2.5.

Introducción

Las convocatorias del instrumento *Internal Security Fund-Police* (ISF-P) (2014-20) de la Comisión Europea (CE) tienen como objetivo apoyar acciones que abordan retos de seguridad interior, en consonancia con los objetivos estratégicos pertinentes establecidos por la UE en su Estrategia de Seguridad Interna adoptada en 2010 [1]. Para ello, los proyectos de las convocatorias ISF-P se centran en dos objetivos principales: por un lado, la lucha contra el crimen y la cooperación policial, y por otro, la protección de infraestructuras críticas y la gestión de crisis [2].

El Departamento de Sistemas de Defensa NBQ del INTA-Campus de La Marañosa, actualmente participa en dos consorcios europeos de las convocatorias ISF-P (BULLSEYE y MALL-CBRN). Estos proyectos están en consonancia con el *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks* (BULLSEYE y MALL-CBRN) y con el *Action Plan to support the protection of public spaces* (MALL-CBRN) de la UE. En ambos el personal del departamento participa en calidad de investigador/experto.

Los dos proyectos tienen una duración de 36 meses (2019-2022).

Proyecto BULLSEYE

El proyecto BULLSEYE, *Harmonised procedures and awareness of all agencies involved in the response of a chemical or a biological terrorist attack: education-training and train the trainer* (ISFP-2017-AG-PROTECT) (*Grant Agreement* No. 815220) está liderado por el *Service Public Federal Interieur* (Bélgica). El resto de participantes de este consorcio lo forman: *International Centre for Chemical Safety and Security* (Polonia), *Uniwersytet Lodzki* (Polonia), *ISEM-Institut* (Eslovaquia), *Ministerstvo Vnutra Slovenskej Republiky* (Eslovaquia), *Police Federale Belge* (Bélgica) y *Ministry of Defense* (Holanda) [3] [4]. El objetivo general del proyecto es mejorar la preparación y la respuesta de los servicios de emergencia europeos a los incidentes NRBQ y explosivos [3] [4].

Proyecto MALL-CBRN

Por su parte, el proyecto MALL-CBRN, *Creation of CBRNE protection system for large area shopping malls* (ISFP-2018-AG-CT-PROTECT) (*Grant Agreement* No. 861643), está liderado por la *Uniwersytet Lodzki* (Polonia). El resto de participantes del consorcio son los siguientes: *Forum Gdansk SP. z o.o.* (Polonia), *Wojskowy Instytut Chemii i Radiometrii* (Polonia), *ISEM-Institut* (Eslovaquia), *Hellenberg International OY* (Finlandia) y *Wojskowy Instytut Higieny i Epidemiologii* (Polonia) [5]. Además, tiene el apoyo de diversas instituciones, gobiernos y cuerpos especiales de policía, así como expertos civiles y militares, de diversos países (Hungría, República Checa, Eslovaquia, Bélgica, Portugal y Polonia). Entre los objetivos generales se encuentran: mejorar la protección de los espacios públicos y otros blancos fáciles, mejorar la protección contra los ataques NRBQ y explosivos y abordar esta amenaza, así como otras amenazas emergentes en relación a las infraestructuras críticas y los espacios públicos [5].

Materiales y métodos

Proyecto BULLSEYE

El proyecto BULLSEYE se basa en los análisis de brechas (*gap analysis*) anteriores que se han descubierto en otros proyectos de la UE, como el Proyecto EDEN, ya finalizado, y el proyecto ENCIRCLE todavía en curso [3].

Con el fin de armonizar los procedimientos de respuesta para todas las agencias relevantes, el consorcio BULLSEYE organizará 4 talleres interactivos. Se llevará a cabo un taller para cada una de las tres líneas de respuesta (primera, segunda y tercera) así como un taller multiagencia para asegurar la compatibilidad de todos los procedimientos respectivos [3] [4].

Durante estos talleres, expertos de dentro y fuera de la UE en diversos campos, así como expertos de la OTAN y EUROPOL, compartirán su experiencia con los primeros intervinientes para desarrollar procedimientos óptimos. Los expertos vendrán, no solo de los países socios, sino también del Reino Unido, Francia, Alemania y Estados Unidos [3].

A lo largo de los talleres, los primeros intervinientes y los expertos cooperarán para crear borradores de procedimientos. Estos borradores se probarán en 7 entrenamientos de capacitación en los 5 países participantes y durante 1 ejercicio multiagencia en el Centro de Entrenamiento de Defensa en Vught (Holanda). Posteriormente, se adaptarán los procedimientos después del proceso de evaluación de

Fig. 1. Ejercicios dentro del proyecto BULLSEYE. (Fuente: https://www.bullseyeproject.eu/).

Fig. 2. Ejercicios dentro del proyecto MALL-CBRN. (Fuente: http://mall-cbrn.uni.lodz.pl/).

estos entrenamientos y ejercicios. Los procedimientos desarrollados serán validados después de todo este proceso. [3] [4].

Este proyecto contempla también la expansión de las instalaciones de entrenamiento de perros detectores de explosivos (K9), aspecto que se examinará y desarrollará más a fondo en cooperación con expertos relevantes en los próximos meses [3] [4].

Proyecto MALL-CBRN

Para el análisis de brechas, el consorcio del proyecto realizará una investigación documental acerca del sistema de protección en los centros comerciales y una investigación mediante encuestas a los responsables de la seguridad interna de los mismos por parte de expertos del consorcio y miembros del equipo asesor, a través de una serie de cuestionarios elaborados previamente. Además, el consorcio organizará visitas a centros comerciales seleccionados de los Estados miembros de la UE [5].

En relación a la identificación de los escenarios más probables de actos terroristas con agentes de NRBQ y explosivos, se llevará a cabo una serie de reuniones con los expertos.

En cuanto a la preparación de las recomendaciones para los procedimientos de prevención y respuesta a un incidente de este tipo, el consorcio realizará una serie de reuniones con los equipos responsables de los paquetes de trabajo y se elaborarán materiales didácticos y guías de colaboración [5].

En la prevención de incidentes NRBQ relacionados con el consumo de alimentos, se realizarán también visitas a centros comerciales y entrevistas al personal encargado de la seguridad interna de estos centros. Además, se llevarán a cabo dos entrenamientos de sensibilización sobre esta amenaza para gestores y agentes de seguridad, así como reuniones con los expertos [5].

Finalmente, la verificación y evaluación de las recomendaciones de prevención y respuesta elaboradas se llevará a cabo mediante tres entrenamientos para el personal de los centros comerciales, así como dos grandes ejercicios en estos centros [5].

Resultados y discusión

En relación al proyecto BULLSEYE, los resultados previstos son:

- Proporcionar personal de servicios de emergencia altamente capacitado que luego podrá servir como capacitadores para sus respectivos equipos con el fin de ampliar aún más el alcance de los procedimientos dentro de la UE.
- Garantizar la provisión de un kit de herramientas para capacitadores.
- Compartir los procedimientos con otros países a través del Grupo Asesor NRBQ y explosivos del *Directorate-General for Migration and Home Affairs* (DG Home) para garantizar el máximo rendimiento del esfuerzo de la CE.
- Ampliación del centro de certificación y entrenamiento de perros de detección de explosivos de la UE.

En cuanto al proyecto MALL-CBRN, se esperan los siguientes resultados:

- La elaboración de un libro que recoja los resultados del análisis de brechas realizado en los sistemas de seguridad interna de los centros comerciales.
- La elaboración de un plan de estudios de formación.
- La elaboración de un manual didáctico.
- Una guía con las mejores prácticas para la prevención de incidentes NRBQ y explosivos relacionados con los alimentos.
- Un procedimiento de contramedidas en el caso de incidentes NRBQ y explosivos relacionados con los alimentos.

Conclusiones

Si bien en ambos proyectos queda aún mucho trabajo por realizar, estos disponen de consorcios fuertes y cuentan con una nutrida red de expertos y asesores, así como de personal motivado. Los dos proyectos surgen de necesidades reales como la mejora de los sistemas de prevención, actuación y desarrollo de capacidades frente a las amenazas NRBQ y explosivos, por lo que se espera aporten una solución más eficaz y eficiente a futuros desafíos. Por otro lado, se quiere destacar el gran interés que conlleva el participar en este tipo de proyectos coordinados, así como la utilidad de trabajar de forma conjunta entre diferentes instituciones, organismos y países para llevar a cabo actividades tan complejas, no solo por la temática objeto de estudio, sino también por razones de coordinación.

Referencias

[1] *Internal Security Fund-Police-European Commission* (2020). [Internet]. Disponible en https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/union-actions_en

[2] A. Heeres, "*Internal Security Fund*", en SEREN4 Training on ISF, 2020.

[3] I. van Mechelen, *EU Project 'BULLSEYE': Harmonized procedures for first responders after biological or chemical terrorist attack, NCT Magazine*, 2(8) (2019) 14.

[4] *Bullseye Project* (2020). [Internet]. Disponible en https://www.bullseye-project.eu/

[5] *About the project-MALL-CBRN* (2020). [Internet]. Disponible en http://mall-cbrn.uni.lodz.pl/

La rueda se reinventa (verde en todos los sentidos)

Autor: Ignacio Requena Rodríguez, Advantaria.

Palabras clave: seguridad vial, tecnología antipinchazos, rueda, rueda mixta, rueda mixta protegida, huella medioambiental de vehículos terrestres.

Metas Tecnológicas relacionadas: MT 5.1.2.

Introducción

La utilización de la rueda viene acompañando a la humanidad desde hace más de 6.000 años. Su lugar y fecha de aparición no se conocen con exactitud, aunque se estima como posible su invención en Mesopotamia alrededor del 4.500 a.C.

Su aportación al desarrollo económico, tecnológico, científico y social resulta completamente indudable, habiendo sido un factor fundamental de progreso al facilitar la circulación habitual de personas y mercancías.

Hasta mediados del siglo XIX las principales innovaciones se centraron en la incorporación de elementos metálicos en la zona de contacto con el terreno y en el buje, y en la utilización de radios en su zona central, con el fin de aumentar la vida útil y reducir la fricción del eje, el peso y el momento de inercia.

En el siglo XIX el descubrimiento de la vulcanización del caucho por Charles Goodyear, unido a la capacidad, ya conocida entonces, de redistribución uniforme de la presión en un fluido estanco según el principio de Pascal (1647), permitieron la aparición de los primeros neumáticos (Robert W. Thomson 1845, John B. Dunlop 1888). En la segunda mitad del siglo XX, aparecieron las primeras cubiertas sin cámara y las carcasas de caucho de los neumáticos comenzaron a incorporar cables metálicos y materiales textiles (como el poliéster), distribuidos en planos comunes al eje de giro, dando lugar a la generalización de los neumáticos radiales. Las últimas décadas se han visto caracterizadas por la utilización de

Fig. 1. Rueda mixta de bicicleta antes de acoplar la banda de rodadura (Fuente: Advantaria / Mixtire).

Fig. 2. Rueda mixta de automóvil: diagrama, corte parcial y vista externa. (Fuente: Advantaria / MixTire).

nuevas aleaciones en las llantas, nuevos materiales sintéticos en las cubiertas y por la incorporación de sistemas auxiliares, tales como sistemas antibloqueo ABS, sistemas de control de presión, entre otros.

Desafíos actuales

La reciente aparición de vehículos autónomos, vehículos eléctricos y la necesidad de aumentar la movilidad y capacidad de los vehículos blindados han llevado a replantearse el concepto de rueda tradicional.

En este sentido, los automóviles sin conductor cuentan con sistemas de monitorización y mantenimiento predictivo que disminuyen de forma relevante la posibilidad de un fallo mecánico, desapareciendo, asimismo, la posibilidad de fallo humano. De este modo, los principales factores de accidente se relacionan con la reacción imprevista de otros vehículos no autónomos, cruce de peatones, y con la pérdida brusca de presión debida a la aparición de objetos punzantes en la calzada, cuya detección a una distancia suficiente para poder modificar la trayectoria de forma segura, no está aún resuelta con la tecnología actual.

Del mismo modo, el cambio de paradigma asociado a la ausencia de conductor en el ámbito del transporte de pasajeros o mercancías, presenta nuevos desafíos.

Por un lado, los nuevos modelos de negocio basados en el uso bajo demanda, frente a los actuales modelos basados en su propiedad, hace que el número total de automóviles se reduzca previsiblemente, aumentando la tasa de utilización y disponibilidad de cada vehículo autónomo. En este nuevo escenario de optimización de los trayectos y del tiempo de utilización de cada automóvil, la posibilidad de fallos en los neumáticos supone un factor que puede alterar la previsibilidad del sistema.

Por otro lado, un fallo de un neumático cuando no se encuentre ningún adulto entre los pasajeros, como puede ser un trayecto de menores de edad al colegio, puede suponer un problema de seguridad en caso de accidente, especialmente en lo relativo a la toma de decisiones acerca de si se debe o no abandonar el vehículo, y acerca de la determinación del lugar más seguro para esperar la ayuda que se solicitaría de manera automática.

De esta forma, la exigencia de mayor disponibilidad y fiabilidad en los vehículos autónomos, obliga a buscar neumáticos más seguros.

Asimismo, la progresiva generalización de los vehículos eléctricos e híbridos, implica también un impacto en el desarrollo de la rueda.

En la actualidad, los automóviles eléctricos cuentan con un mayor peso que los que operan con motores de combustión, debido a la incorporación de pesadas baterías, aumentando la carga sobre las ruedas. Por otro lado, los motores eléctricos cuentan con un par instantáneo superior, incrementando el esfuerzo sufrido por el neumático. Estos dos factores hacen aconsejable el aumento del agarre de las ruedas y la disminución de su resistencia a la rodadura.

Del mismo modo, en el ámbito de la seguridad, la creciente implicación de las fuerzas armadas en conflictos asimétricos ha potenciado el uso de vehículos blindados sobre ruedas, los cuales incorporan cada vez mayores capacidades, contando con amplias ventajas desde el punto de vista de movilidad sostenida, autonomía y huella logística frente a los vehículos de cadenas.

Actualmente, su principal vulnerabilidad está relacionada con la posible pérdida de presión en los neumáticos como consecuencia de un impacto. Las distintas soluciones disponibles como dispositivos *Run on Flat* no proporcionan una respuesta plenamente satisfactoria, debido a las limitadas características de autonomía y velocidad, una vez producida esta pérdida de presión.

Un intento recurrente para tratar de solucionar estos inconvenientes ha sido el desarrollo de ruedas sin aire. Esta tecnología, conocida habitualmente como *airless*, consiste en la incorporación de una banda de rodadura similar a la de un neumático tradicional, sustituyendo el volumen neumático por una estructura elástica, constituida por materiales elastómeros o por materiales inextensibles con elasticidad lateral por pandeo.

Algunos de los principales fabricantes de neumáticos han intentado desde hace décadas, el desarrollo y comercialización de este tipo de ruedas, sin que hasta el momento se hayan podido superar las dificultades inherentes a su estructura. La principal desventaja de una rue-

da carente de aire a presión en su interior (o de otro tipo de gas) viene dada por el hecho de que la absorción de las vibraciones e impactos producidos durante la rodadura se produce únicamente en la estructura de la parte inferior de la rueda, que se encuentra sometida al peso del vehículo, produciéndose la compresión del material fundamentalmente según una dirección radial, a diferencia de la absorción en un compartimento estanco a presión, que se realiza de forma uniforme e isótropa en todo su volumen. Esto hace que la capacidad de absorción, y de recuperación, sea muy superior en una rueda neumática que en una *airless*.

Separación de la banda de rodadura del volumen neumático

Esta necesidad de mantener un volumen a presión en cualquier nuevo diseño de rueda, unida a la necesidad de incrementar la resistencia frente a pinchazos o impactos de proyectiles lleva a la aparición de las ruedas mixtas. Estas ruedas mixtas incorporan, en la parte interior a la banda de rodadura, una estructura anular de naturaleza rígida o flexible, constituida por elementos radiales, que rodea a un volumen neumático interior que se encuentra en contacto con la llanta. De este modo, se produce una separación efectiva entre el volumen neumático y la banda de rodadura, permitiendo que una perforación de esta última no implique una pérdida de presión.

La utilización de elementos radiales con menor capacidad de deformación puede disminuir los microdeslizamientos en la zona de contacto mejorando el agarre, reduciendo, a su vez, el efecto del esfuerzo producido por el par de giro. Asimismo, la separación de los dos elementos principales que hasta el momento han constituido los neumáticos tradicionales: la banda de rodadura y la carcasa que rodea al volumen neumático tiene otras dos importantes implicaciones:

- Posibilidad de blindar el volumen neumático: Se pueden incorporar placas blindadas en los laterales del compartimento de gas a presión, así como elementos radiales con cabezales blindados en la estructura anular, proporcionando a la rueda una resistencia frente a impactos.

- Posibilidad de sustituir la banda de rodadura de manera sencilla: Actualmente la sustitución de la banda de rodadura requiere, para su unión con la carcasa, de un proceso de vulcanización mediante el uso de una prensa o de un autoclave a presión. La separación del volumen neumático de la banda de rodadura permite el anclaje de esta última mediante procedimientos mecánicos, facilitando su rápida sustitución por necesidades operativas (caso de requerirse una banda más ancha para mejorar la conducción en terrenos blandos), o por motivo de su desgaste.

Conclusiones

Las dos características anteriores motivan el título del presente artículo. Algunas empresas están investigando en el desarrollo de bandas de rodadura biodegradables a partir de materiales de origen vegetal. Su menor duración puede quedar compensada por una sustitución sencilla y frecuente de la banda de rodadura. Al mismo tiempo, las investigaciones en el ámbito de la defensa (concepto éste que se ha ido redefiniendo hasta abarcar también aspectos medioambientales y sanitarios, tal y como muestran las diferentes actuaciones de los ejércitos durante la actual situación de pandemia) pueden producir, asimismo, un importante desarrollo de mejoras en el ámbito civil, proporcionando una inmejorable oportunidad de cooperación internacional entre empresas, administraciones, universidades y organismos de investigación, tanto en aspectos relativos a la seguridad vial y la disminución de la huella medioambiental, como relacionados con la defensa.

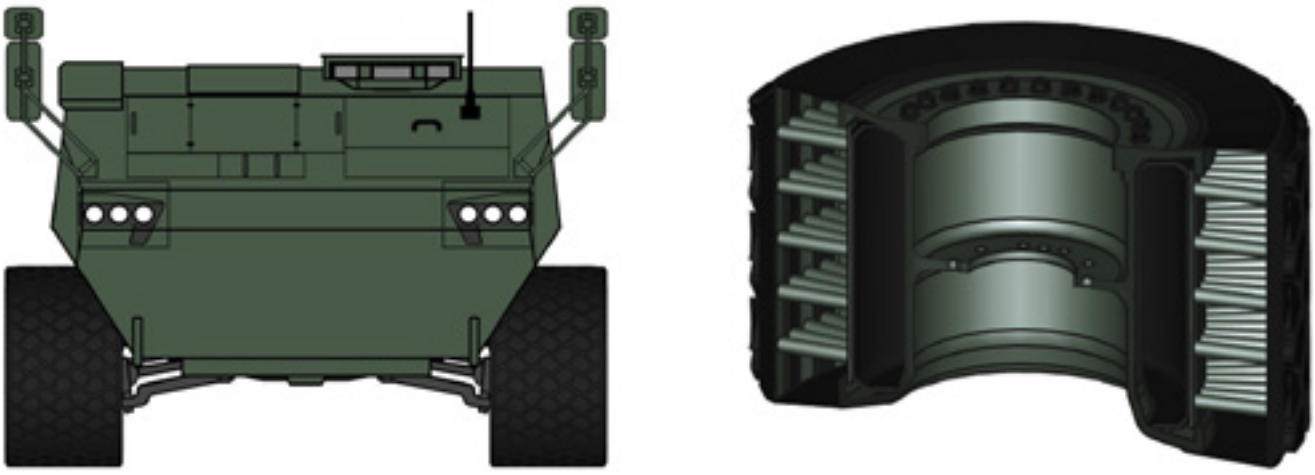

Fig. 3. Frontal de VCR 8x8 con ruedas mixtas protegidas y corte de la rueda. (Fuente: Advantaria / MixTire).

DIAR y DIFI, los nuevos sistemas de medida de firmas radar e infrarroja de la Armada

Autores: TN (CIA EOF) Francisco José Calviño Dopazo, CF (CIA EOF) Rafael Ángel Valencia Cruz, Ministerio de Defensa. Armada Española. Subdirección de Ingeniería. Centro de Medidas Electromagnéticas (CEMEDEM).

Palabras clave: firma radar, firma infrarroja, SER, RCS, SAR, ISAR, perfiles, blanco, misil, chaff, bengala, contramedidas.

Metas Tecnológicas relacionadas: MT 2.2.1; MT 2.3.1; MT 2.7.1..

Introducción

De forma resumida se podría decir que los sistemas radar tratan de detectar o caracterizar objetivos predefinidos[1] mediante la reflexión que produce en ellos una señal electromagnética, normalmente generada en ese mismo sistema radar.

Las aplicaciones actuales de los sistemas radar son innumerables, abarcando campos como la teledetección, seguimiento, guiado de misiles, control de tráfico aéreo, navegación, control de velocidad, meteorología, detección de restos arqueológicos, comprobación del nivel en los océanos, etc.

Por otro lado, está el campo de la radiación infrarroja, que es la propiedad de cualquier objeto de emitir en el espectro infrarrojo simplemente por el hecho de tener una temperatura superior al cero absoluto (-273.15ºC). A mayor temperatura mayor será la radiación infrarroja emitida, si bien las propiedades de esas emisiones variarán y la tecnología necesaria para caracterizarlas deberá asimismo adaptarse a esas variaciones.

Nuevamente, la implacable mejora de la tecnología en este campo ha permitido el desarrollo de equipos con aplicaciones en multitud de ámbitos y usos: sistemas de guiado de misiles, sistemas de visión nocturna, sistemas de vigilancia, mandos a distancia, aplicaciones médicas, climáticas, comunicaciones ópticas, etc.

Tanto en un caso como el otro, el ámbito militar ha sido decisivo, no solo para el avance de estas tecnologías, sino para su misma generación. La necesidad de lograr una ventaja táctica sobre los posibles adversarios ha llevado a idear sistemas que permiten detectar, e incluso identificar, unidades enemigas y con la antelación suficiente para dotarnos de un mayor tiempo de respuesta y aumentar las probabilidades de supervivencia.

Pero en este escenario no sólo basta con poder identificar y caracterizar al adversario, sino que también es preciso evitar que dicho adversario haga lo propio con nosotros. Por ello es necesario el poder definir nuestras unidades, observar sus deficiencias, corregirlas en la medida de lo posible o tenerlas presentes para futuras versiones. Los campos radar e infrarrojo (así como el acústico, magnético u óptico) son hoy de vital importancia en el ámbito militar, fundamentalmente porque las principales amenazas a nuestras unidades atienden a sus características en estas áreas y, adicionalmente, debido a las posibilidades de innovación y mejora que aún pueden ofrecer.

La Armada y la Dirección General de Armamento y Material (DGAM) han impulsado el desarrollo de sendos sistemas de medida de firma radar e infrarrojo, que habilitan en el ámbito de la defensa este indispensable

[1] La característica de predefinido hace referencia a la obvia necesidad de establecer unos límites a las características de los objetivos y blancos que cualquier sistema requiere para su diseño y desarrollo.

Fig. 1. Sistema DIAR. (Fuente: MINISDEF).

En profundidad

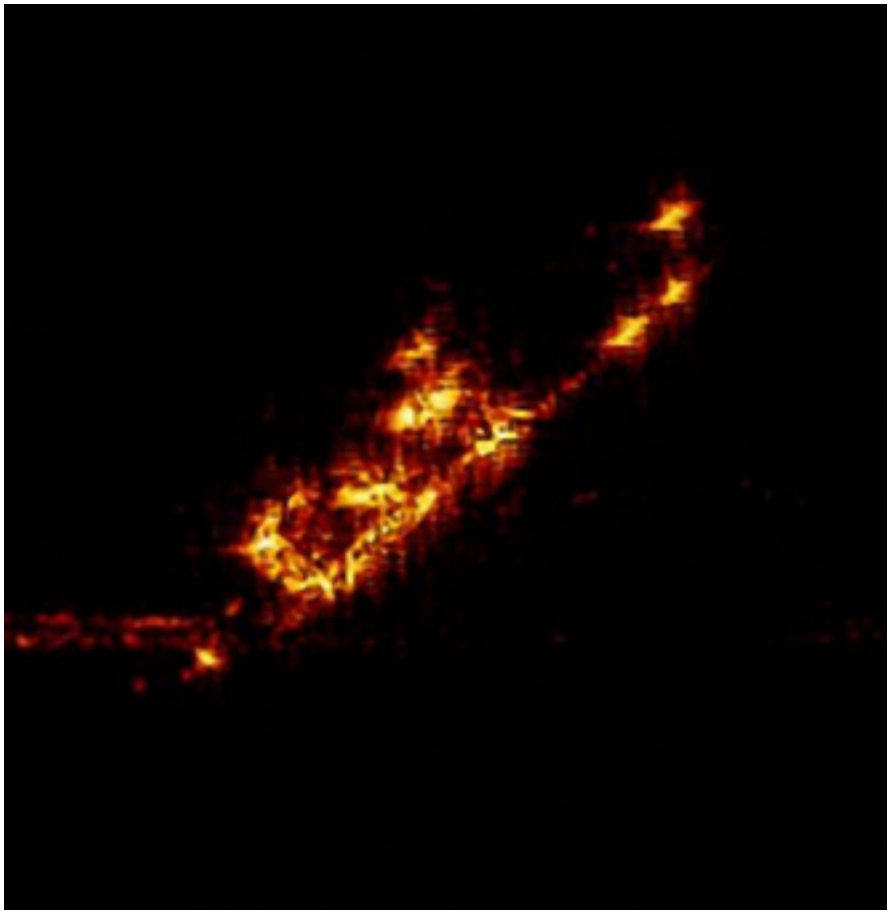

Fig. 2. Imágenes ISAR y HRRPs obtenidos con DIAR. (Fuente: MINISDEF).

requisito de caracterizar nuestras unidades navales, definir sus posibilidades de detección y poder así establecer las acciones tácticas más oportunas para evitarla. Estos equipos son el sistema DIAR (Demostrador Instrumental de Alta Resolución) y el sistema DIFI (Demostrador Instrumental de Firma Infrarroja), dos sistemas que la I+D+I española (en concreto el Grupo de Antenas y Radar de la Universidad de Vigo) ha situado en la vanguardia de la tecnología internacional en su campo de aplicación.

Ambos sistemas se han desarrollado para su explotación en el Centro de Medidas Electromagnéticas (CEMEDEM) perteneciente a la Subdirección de Ingeniería de la Jefatura del Apoyo Logístico de la Armada, organismo con el que el citado grupo de la Universidad de Vigo colabora desde hace más de treinta años.

Junto a la renovación del Laboratorio Móvil del CEMEDEM, los equipos fueron entregados a la Armada en octubre de 2019 y, tras cumplirse un año de garantía, la experiencia obtenida con ellos en el CEMEDEM es plenamente satisfactoria.

Sistema DIAR

DIAR es un sistema de medida de firma radar, capaz de obtener en tiempo real y de forma simultánea resultados tan complejos como la sección equivalente radar (SER), perfiles de alta resolución longitudinal (HHRP) e imágenes SAR/ISAR (*Synthetic Aperture Radar*/*Inverse Synthetic Aperture Radar*) de un objetivo, sea o no colaborador, y ya sea este un blanco marítimo, terrestre o aéreo.

Estas características hacen del DIAR un sistema puntero a nivel internacional. Es un equipo con una arquitectura basada en equipos comerciales, lo que lo dota de un grado alto de escalabilidad. Su capacidad de despliegue es también muy versátil al ir montado sobre un vehículo todoterreno y disponer de protección frente a cualquier clima. Adicionalmente, ofrece la posibilidad de desmontarlo de forma sencilla del vehículo y ajustarlo a cualquier tipo de terreno o estructura sobre la que necesite ser ubicado.

Las aplicaciones directas del sistema DIAR pasan por la caracterización completa de las unidades medidas a nivel radar. Esto supone conocer su grado de detección ante radares enemigos, la variabilidad de esta propiedad ante los diferentes factores influyentes (frecuencia, polarización, demora, distancia o geometría, entre otros), la identificación de los puntos que más contribuyen a su detección y la correspondiente propuesta de medidas para su corrección (cuando es viable), la evaluación de tratamientos RAM[2] y el estudio de la efectividad de *chaff* y contramedidas.

El potencial del *hardware* implementado en DIAR lo dotan de muchas más posibilidades con poca inversión adicional, como podrían ser el análisis y excitación de los sistemas de guerra electrónica de nuestras unidades o la caracterización de las condiciones de propagación, entre otras.

El sistema cubre las bandas C, X y Ku, polarizaciones horizontal y vertical, con capacidad para transmitir tanto de forma continua como pulsada. Esto permite a DIAR medir y caracterizar desde el periscopio de un submarino hasta el mayor de los portaviones y con un grado de resolución de hasta decímetros, según el tipo de unidad a medir.

Dispone de capacidad de seguimiento óptico, radar o por GPS.

Además, el sistema es perfectamente manejable tanto de forma local como remota a través de enlaces vía WIFI o 4G totalmente seguros y configurables. Dispone de una unidad remota embarcable que además de permitir el seguimiento por GPS envía información de parámetros dinámicos de la unidad (balance, cabezada, guiñada, velocidad). Esta unidad remota es una ayuda a la hora de procesar los datos de una medida, pero no es imprescindible para obtener resultados.

[2] *RAM: Radar Absorbing Material*

Fig. 3. Sistema DIFI. (Fuente: MINISDEF).

Sistema DIFI

DIFI es un sistema cuya principal función es la de obtener la firma infrarroja de un blanco en condiciones ambientales conocidas. Esto permitirá caracterizar el objetivo en el espectro infrarrojo y definir su grado de detección en este ámbito, analizando los puntos calientes que más contribuyen a su respuesta y posibilitando la toma de medidas correctivas cuando sea viable.

Al igual que DIAR, DIFI posee una arquitectura también basada en su mayoría en equipos comerciales, si bien alguno de sus componentes ha sido sometido a ciertas mejoras *ad hoc* para garantizar unos resultados superiores a los ofrecidos por dicho componente en su versión habitual. Por este motivo su escalabilidad futura está garantizada.

El transporte y despliegue de la unidad es similar a la del sistema DIAR, montado en un vehículo todoterreno y con la posibilidad de hacer independientes sistema de medida y vehículo, lo que permite su puesta en funcionamiento en menos de 30 minutos una vez alcanzado el lugar de medida.

El demostrador permite realizar medidas en las dos bandas de interés militar a nivel IR, la banda MWIR (*Medium Wavelength Infra-Red*), que abarca las bandas espectrales de 3 a 5μm y la banda LWIR (*Long Wavelength Infra-Red*), que incluye la banda de 8 a 12μm[3], y con tiempos de integración totalmente configurables para poder caracterizar con precisión diferentes rangos de temperatura. Se puede nuevamente controlar localmente, vía WIFI o 4G [3]. Sus capacidades de despliegue y seguimiento son conceptualmente las mismas que las del sistema DIAR. El alcance en distancia para proporcionar datos se extiende hasta los 8 km. También posee una unidad remota embarcable que, además de enviar a la unidad de medida datos de telemetría, añade información de las condiciones ambientales a bordo del blanco, lo que permite definir con mucha más precisión el comportamiento del blanco. Las medidas sin esta unidad embarcable también son posibles, si bien la calidad de los datos generados disminuye.

Así, el sistema DIFI permite evaluar a las unidades bajo medida en las bandas del infrarrojo indicadas, resaltar qué elementos contribuyen más a la

[3] Estas ventanas son aquellas en las que a día de hoy funcionan las principales amenazas tipo misil contra nuestras unidades y gran parte de las aplicaciones en los ámbitos civil y militar.

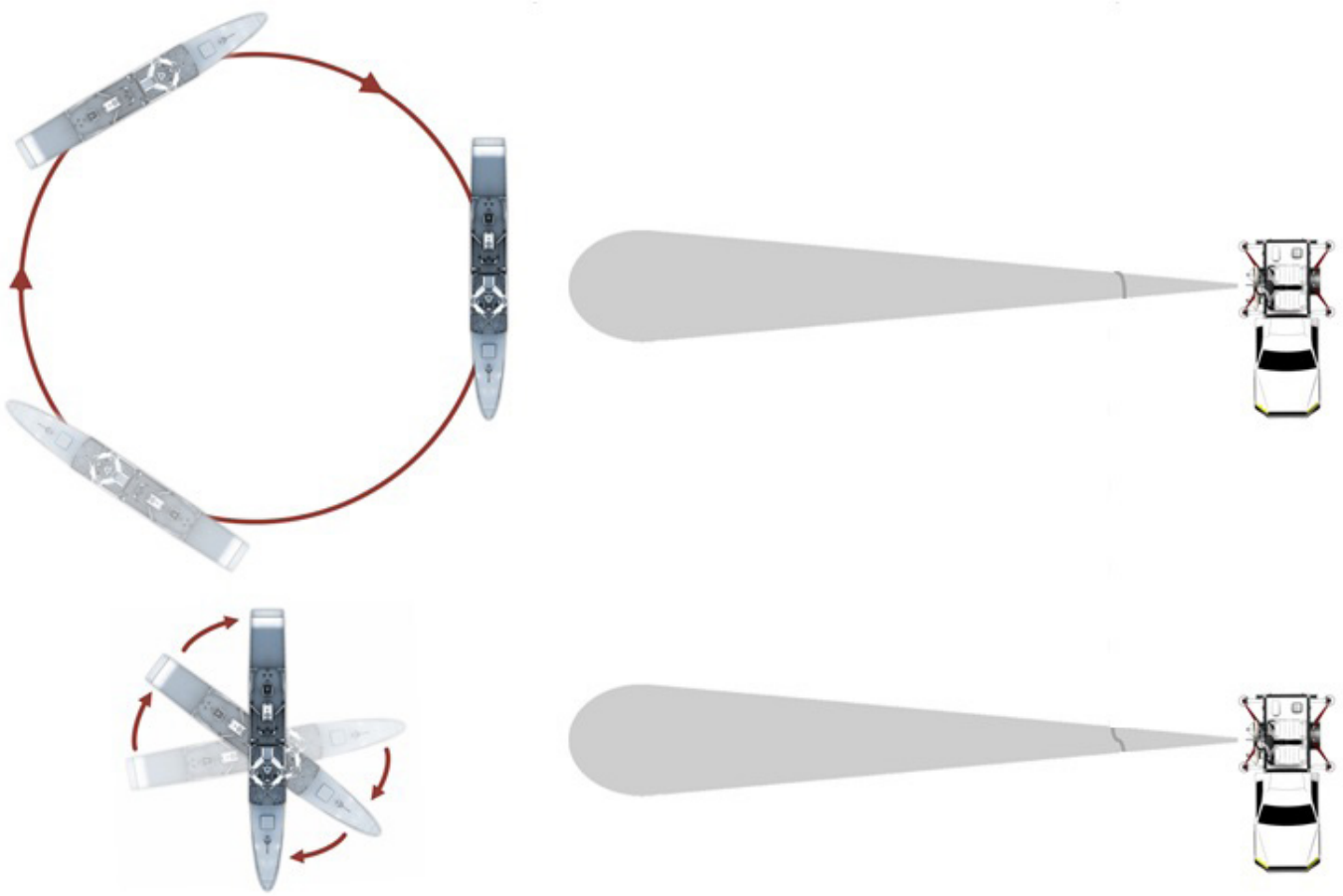

Fig. 4: Evoluciones necesarias para medida de firmas. (Fuente: MINISDEF).

detección de las mismas y caracterizar el comportamiento de las contramedidas IR desplegadas frente a la unidad.

Mecanismo de medida de firmas SER e IR

Aunque tanto DIAR como DIFI parten de un concepto orientado más a la medida de plataformas navales, en la realidad se ha demostrado que es posible también llevar a cabo medidas a unidades terrestres y aéreas.

El protocolo de medida parte de la base de que es necesario medir a la unidad en los 360º que conforman su contorno para poder caracterizarla adecuadamente. Por ello, el blanco objeto de medida describe evoluciones circulares (idealmente en un punto) a una distancia especificada con el radio táctico mínimo posible. La configuración exterior de la plataforma a medir ha de ser la de interés (si hay varias, deberán medirse cada una por separado) y no debe cambiarse mientras dure la medida. Tampoco es apropiado cualquier tipo de emisión en la banda del espectro en la que se esté midiendo, debido a que muy probablemente incrementará la respuesta esperada de la unidad.

Para el caso de un blanco colaborador, la figura 4 muestra cómo sería el proceso de medida.

Empleando el DIAR, con una sola evolución se puede obtener la SER en todo el ancho de banda de trabajo y para una polarización. Sin embargo, la obtención de imágenes ISAR o perfiles de alta resolución requieren de una evolución por frecuencia de interés (también se obtendría la SER a esa frecuencia y polarización).

En la parte infrarroja DIFI se obtiene, por cada evolución dada, las imágenes IR en ambas bandas de trabajo, pero para un solo tiempo de integración, es decir, para un solo rango de temperaturas a caracterizar. Lo habitual es utilizar diferentes rangos de temperatura en diferentes evoluciones para caracterizar puntos a temperaturas dispares. Si sólo midiéramos para obtener los puntos más calientes, el resto de elementos a temperaturas más bajas quedarían enmascarados y pasarían desapercibidos. Y al contrario, al medir para detectar elementos menos calientes, los elementos que más contribuyen quedarían al mismo nivel que aquellos, quedando oculta su verdadera importancia.

En el caso de blancos no colaborativos los sistemas serían capaces de realizar el seguimiento de los mismos llevando a cabo la medida en las demoras visibles.

Un punto negativo de ambos sistemas es que no ofrecen la posibilidad de ser embarcados en una aeronave para llevar a cabo medidas en eleva-

ción, lo cual también es importante para definir adecuadamente la unidad y en base al comportamiento que están presentando misiles de nueva generación.

Unidades "*STEALTH*"

El avance que las tecnologías de detección en general han sufrido en los últimos años es realmente importante, motivado por un lado por la mejora en todo el *hardware* involucrado en la generación y transmisión de las señales requeridas para la "detección" y, por otro, por la capacidad de procesamiento de los equipos actuales, que permiten obtener resultados en tiempo real que no hace mucho eran inviables.

Esta carrera por detectar de forma cada vez más precisa y más detallada lleva inevitablemente asociada la opuesta, es decir el desarrollo de tecnologías que eviten la detección y contribuyan al ocultamiento de las unidades. Son las denominadas tecnologías de invisibilidad o "*STEALTH*"[4]. Las propiedades *stealth* abarcan los diferentes aspectos aprovechables para reducir la detección de un blanco: aspectos radar, infrarrojos, magnéticos, ópticos, sónicos o de uso de sistemas LPI[5].

Hoy en día el diseño de unidades con características *stealth* es ya una necesidad y requiere necesariamente de simulaciones por *software* que permitan abordar la construcción de dichas unidades con ciertas garantías[6] de baja detección.

Una vez finalizada la construcción, los sistemas DIAR y DIFI, en los ámbitos de la firma radar e infrarroja, ayudarán a comprobar que tales requisitos se cumplen y a generar una retroalimentación de información que, a su vez, redundará en la optimización de futuras unidades.

Conclusiones

Tal y como se ha expuesto anteriormente, los sistemas de medida de firma DIAR y DIFI constituyen dos herramientas fundamentales en el ámbito de la defensa, al permitir definir y concretar aspectos decisivos de nuestras unidades navales en el campo de la detección radar e infrarroja, así como el estudio y valoración de las diversas contramedidas de tipo seducción o distracción derivadas de la defensa antimisil. Por otro lado, contribuirán a comprobar las especificaciones de nuevas construcciones en sus respectivas áreas de aplicación y permitirán establecer una base de conocimiento importante a la hora de acometer nuevos diseños.

Estos proyectos han permitido a la Armada sistemas tecnológicamente punteros a nivel internacional, de gran escalabilidad y fundamentados en desarrollos completamente nacionales, lo que pone nuevamente en valía el potencial de la industria nacional.

[4] Como ejemplo más notorio de estas tecnologías está la clase de destructores "ZUMWALT" de la armada estadounidense.

[5] Los sistemas LPI (*Low Probability of Intercept*) son aquellos que usando muy poca potencia tienen las mismas o mejores prestaciones que los sistemas habituales, dificultando la detección de la unidad que los usa por emisiones propias.

[6] Un ejemplo de estos simuladores a nivel radar podría ser el *software* M3 desarrollado por la Universidad de Vigo y la Universidad de Extremadura, actualmente uno de los mejores del mundo.

Referencias

[1] *The generalized forward-backward method for analysing the scattering from targets on ocean-like rough surfaces.* M.Rodríguez Pino, L. Landesa, J.L. Rodríguez, F. Obelleiro, R.J. Burkholder. *IEEE Trasactions on Antennas and Propagation*, *volume* 47, *pags* 25-33. 1999.

[2] *Radar Cross Section, Second Edition*. Eugene F. Knott, John F. Schaeffer, Michael T. Tulley. *SciTech Publishing*, 2004.

[3] *Understanding Synthetic Aperture Images*. Christopher Oliver, Shaun Quegan. *Scitech Pub*, 2004.

[4] *Experimental verification of the relation between the radar cross section and the list angle of surface vessels*. J.F. Pérez Ojeda, J.L Rodríguez, I. García-Tuñón, F. Obelleiro. *Microwave and Optical Technology Letters*, 48-11, *pags* 2237-2241. 2006

[5] *Infrared Thermal Imaging: Fundamentals, Research and Applications*. M. Vollmer, K. P. Möllmann. *2nd Edition*. Wiley-VCH Verlag GmbH. 2010.

[6] Experiencia en el control de la firma radar y reducción de la sección recta radar (RCS) de una plataforma naval. Inés García-Tuñón blanca, José Luis Rodríguez Rodríguez, Fernando Obelleiro Basteiro. II Congreso Nacional de I+D en Defensa y Seguridad. Noviembre 2014.

[7] Manuales del Demostrador Instrumental de Alta Resolución. Dirección General de Armamento y Material, 2018.

[8] Manuales del Demostrador Instrumental de Firma Infrarroja. Dirección General de Armamento y Material, 2018.

[9] La simulación electromagnética en buques de la Armada Española. José Antonio López Moreno, Fernando Obelleiro Basteiro, Revista General de Marina, marzo 2019.

Seguridad en el *Software* Aeronáutico

Autor: Coronel Fernando Aguirre Estévez, Dirección de Ingeniería del Mando del Apoyo Logístico del Ejército del Aire.

Palabras clave: certificación, crítico, fallo, fiabilidad, peligro, riesgo, *safety*, seguridad, *software*.

Metas Tecnológicas relacionadas: MT 3.1.1; MT 7.1.1; MT 7.1.2; MT 7.3.1.

Introducción

Recientemente, el Departamento de Defensa Norteamericano reconoció 873 deficiencias de *software* sin resolver en el caza F-35, de las cuales 13 son de clase 1 (consecuencias operacionales en la plataforma). Los resultados son desalentadores, teniendo en cuenta que en el anterior informe el número de deficiencias identificadas fueron 917 [1]; si bien no debe olvidarse que el F-35 es un avión construido alrededor de un grupo de ordenadores extraordinariamente complejos, donde el número de líneas de código ya se cifran en veinticuatro millones en las versiones más avanzadas del caza.

El IEEE (*Institute of Electrical and Electronics Engineers*) define *software* como "un conjunto de programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación" [2]. Así, el vocablo *software* abarca no solo al ejecutado por los ordenadores donde esté instalado, sino que también alcanza a los datos que necesitan estos programas, al sistema operativo y a los interfaces que interaccionan con el resto de los equipos. La importancia del *software* en las aeronaves es capital, habida cuenta de que un fallo de un programa puede ir desde insignificante, que no afecta a las prestaciones de la plataforma y sus sistemas, hasta el fallo de componentes críticos. Es por ello que se requiere aplicar unos procedimientos de verificación y validación del *software* que garantice que no existe riesgo de que se produzcan condiciones de fallo inseguras.

Aprobación del *software*

Atendiendo a lo indicado en el Reglamento de Aeronavegabilidad de la Defensa (RAD), el Certificado de Tipo hace constar que una aeronave y sus sistemas embarcados han sido diseñados y ensayados siguiendo las normas y procedimientos aprobados y que, por tanto, se considera segura para el vuelo [3]. La aprobación del *software* embarcado forma parte del proceso de certificación de la aeronave y sus sistemas, que busca demostrar que se cumple con los requisitos mínimos que garantice la seguridad en vuelo.

La criticidad de los cometidos encomendados a un paquete *software* será función de la severidad que el fallo pudiera ocasionar. Para establecer una clasificación relativa a dicha criticidad, la FAA (*Federal Aviation Administration*) ha adoptado el estándar DO-178 "*Software Considerations in Airborne Systems and Equipment Certification*" [4] para sistemas embarcados, desarrollado en colaboración con la EUROCAE (*European Organisation for Civil Aviation Equipment*), que en Europa se ha designado ED-12. Este estándar define cinco niveles de seguridad DAL (*Design Assurance Level*), en función de las posibles consecuencias del malfuncionamiento del *software*, graduado desde sin efectos (*No Safety Effect*) hasta catastrófico. Dependiendo del DAL, el programador/desarrollador debe cumplir un conjunto de requerimientos, que el estándar denomina objetivos, y lograr cada objetivo requiere, a su vez, implementar un conjunto de actividades o subobjetivos.

El DO/178/ED/12 permite realizar la verificación y validación del *software* aeronáutico, agilizando los trámites de certificación ante la Autoridad Aeronáutica [5]. Para ello, este documento proporciona una guía a seguir en el ciclo de vida de un paquete *software* con el objeto de verificar su integridad y calidad, alcanzando una mayor portabilidad y reusabilidad a menores costes, donde el fin último es garantizar que cada línea de código esté libre de errores y que los procesos de codificación y ensamblado de este código no adicionen *software* corrupto.

Asimismo, la modificación de un producto software después de su entrega es un procedimiento común de mantenimiento, debido a la necesidad de corregir defectos, mejorar el rendimiento u otras propiedades deseables, adaptarlo a un entorno distinto, y/o incorporar nuevas capacidades. Según lo indicado por el RAD [3], mientras que las modificaciones menores en aeronaves y sus sistemas deben ser aprobadas por el Órgano Técnico Competente, las modificaciones mayores, diseñadas y ensayadas por una organización distinta del titular del Certificado de Tipo, requieren de un Certificado de Tipo Suplementario que demuestre el cumplimiento de los requisitos y procedimientos aplicables aprobados. Por su parte, el Ejército del Aire instituyó la Instrucción General 70-12 como documento normalizador del Ciclo de Modificaciones de un Sistema de Armas, especificando las fases de diseño y desarrollo, así como las competencias de cada entidad involucrada.

El DO-178/ED-12 no solo puede aplicarse al *software* desarrollado y certificado previamente con este mismo estándar, sino que también puede usarse para modificaciones de *software* desarrollado con anterioridad bajo otro estándar y que deba ser certificado de nuevo, ya sea bajo el mismo entorno de desarrollo u otro diferente. Además, este estándar también se ha empleado en modificaciones

DAL	CONDICIÓN DE FALLO	PROBABILIDAD DE FALLO
A	Catastrophic	menor de 10^{-9} por hora de vuelo
B	Hazardous/Severe-Major	entre 10^{-7} y 10^{-9} por hora de vuelo
C	Major	entre 10^{-5} y 10^{-7} por hora de vuelo
D	Minor	mayor que 10^{-5} por hora de vuelo
E	No Effect	ninguna

Fig. 1. Categorización de la condición de fallo en función del DAL del *software*. (Fuente: DO-178/ED-12).

PROCESOS DEL DESARROLLO	DAL				
	A	B	C	D	E
Software Planning Process	7	7	7	2	0
Software Development Process	7	7	7	7	0
Verification of Outputs of Software Requirements Process	7	7	6	3	0
Verification of Outputs of Software Design Process	13	13	9	1	0
Verification of Outputs of Software Coding & Integration Processes	7	7	6	0	0
Testing of Outputs of Integration Processes	5	5	5	3	0
Verification of Verification Process Results	8	7	6	1	0
Software Configuration Management Process	6	6	6	6	0
Software Quality Assurance Process	3	3	2	2	0
Certification Liaison Process	3	3	3	3	0
TOTAL	66	65	57	28	0

Fig. 2. Número de objetivos a cumplir en cada proceso en función del DAL. (Fuente: DO-178/ED-12).

de *software* embebido en productos COTS (*Commercial-Off-The-Shelf*).

Software crítico

La utilización del *software*, particularmente en sistemas críticos, se ha multiplicado en los últimos años [5], volviéndose estos dispositivos cada vez más complejos, de tal modo que la incorporación de nuevas capacidades en los Sistemas de Armas pasa indefectiblemente, en mayor o menor medida, por cambios *software* que demandan análisis de riesgos específicos que eviten condiciones de fallo. Si a lo anterior se añade que estas modificaciones no solo afectan a la plataforma aérea sino también al elemento logístico, al *Health Monitoring System*, a la *Combat Cloud*, a la compatibilidad con el simulador de vuelo, etc., se configura un caldo de cultivo donde es preciso hacer uso de protocolos de seguridad *software*.

Un *software* que tiene encomendadas funciones críticas tiene que protegerse de peligros y/o fallos críticos, de tal modo que no causen daños importantes al sistema. Para ello es necesario disponer de dispositivos y/o mecanismos que mitiguen o controlen estos peligros o fallos, siendo preferible que estos mecanismos sean vía *software*. Para que este *software* crítico funcione correctamente se deben dar una serie de principios:

- El *software* no debe fallar al implementar las funciones críticas que tenga asignadas, de modo que conduzca al sistema a un estado peligroso e inesperado.
- El *software* no debe fallar en la detección o corrección del estado peligroso del sistema.
- El *software* no debe ser la causa de que tengan que actuar los mecanismos de mitigación.
- El *software* no debe fallar a la hora de implementar mecanismos de mitigación o reducción de efectos, en caso de que ocurra un estado peligroso.

La prevención de fallos intenta evitar que se introduzcan fallos en el sistema antes de que entre en funcionamiento, mientras que si el sistema continúa funcionando aunque se produzcan fallos es lo que se denomina tolerancia al fallo, siendo la redundancia una solución a este problema como factor mitigador. Qué duda cabe que al emplear componentes o *softwares* añadidos que detectan el fallo y recuperan el comportamiento correcto, se induce una mayor complejidad en el sistema y también se pueden producir fallos adicionales, dándose dos situaciones: en la redundancia estática, los elementos redundantes están siempre activos mientras que en la redundancia dinámica los elementos redundantes entran en funcionamiento al actuar los mecanismos de mitigación cuando se detecta un fallo.

De cara a abordar los análisis de riesgos, el Anexo 19 de la OACI (Organización de Aviación Civil Internacional) define el riesgo como "la probabilidad y la severidad previstas de las consecuencias o resultados de un peligro", mientras que para entender el concepto de peligro se puede acudir al *Safety Management International Collaboration Group,* que concibe el peligro como "la condición que puede causar o contribuir a un incidente o accidente de la aeronave". Asimismo, el IEEE define la fiabilidad como "la probabilidad de que un sistema desempeñe sus cometidos, bajo condiciones específicas, en periodos de tiempo determinados", la cual aumenta con la tolerancia al fallo. La probabilidad de fallo de un *software* depende esencialmente de dos factores: los errores en el código, propiamente dicho, y/o la entrada de valores erróneos para los cuales el sistema no tiene respuesta. Ciertamente, un *software* fiable y robusto sigue cumpliendo su misión a pesar de recibir variables erróneas. Finalmente, la seguridad (*safety*) es la probabilidad de que no ocurra ningún evento que provoque un fallo (ISO/IEC 15026), que aumenta con una adecuada prevención de fallos.

Una vez identificados los riesgos, el análisis de los mismos se encarga de su categorización, dependiendo de su severidad y probabilidad, para a continuación intentar evitarlos o, si no se puede, incluir medidas mitigadoras incorporando mayores redundancias entre otras opciones. Además, es necesario planificar y programar criterios de cancelación de la misión FTS (*Flight Terminate System*) en caso de que se materializase un fallo crucial. Para la gestión de riesgos son de aplicación diferentes procedimientos como el estándar MIL-STD-882E "*System Safety*", el STANAG 7160 "*Aviation Safety*" o el Doc 9859 AN/474 OACI "Manual de gestión de la seguridad operacional" [6], por citar los más relevantes.

Singular preeminencia cobran en estas circunstancias todos aquellos procesos de comprobación y análisis, simulaciones, tanto en bancos de pruebas como en vuelo, explorando los distintos modos de fallo así como las limitaciones inducidas y los criterios FTS. Estos procesos permitirán asegurar que el *software* se desarrolla de acuerdo a sus especificaciones y satisface los requisitos (verificación), desde un punto de vista teórico, mientras que en la validación se deben cumplir los requisitos del usuario en un análisis práctico.

Desarrollo *software*

El fin último de los procesos de desarrollo *software* es minimizar la probabilidad de fallos durante la creación del sistema. Así, es de destacar que tras la introducción del DO-178B en la década de los 90, no ha ocurrido un solo incidente letal que pueda ser atribuido a un fallo en el desarrollo del *software* certificado bajo este estándar.

La última versión DO-178C mantiene los principios establecidos por sus versiones anteriores, DO-178A y DO-178B. Así, aunque el DO-178C tiene muchos cambios menores respecto al DO-178B, estos son en su mayoría aclaratorios. De hecho, el *software* existente que ha sido aprobado previamente bajo el DO-178B también puede aprobarse bajo el DO-178C [7].

Dado que es bastante difícil probar la completa ausencia de errores de *software*, el principal objetivo del DO-178/ED-12 es demostrar la calidad del proceso de desarrollo desde los comienzos hasta el final, teniendo siempre presente la necesidad de minimizar la creación de errores. Así, la filosofía de los estándares DO-178/ED-12 requieren que se realicen una gran cantidad de pruebas de *software* basadas en requisitos, análisis de seguridad del sistema, análisis de *software*, revisiones de *software* y pruebas formales, las cuales se emplean en soportar y dar confianza en todo el proceso de desarrollo.

Software Development Plan

El *Software Development Plan* (SDP) concreta los lenguajes de programación utilizados, el estándar de codificación, los métodos de pruebas, las herramientas de *debugging,* los procedimientos de desarrollo y diseño del *software*, así como el *hardware* usado en el desarrollo y ejecución del *software*. El SDP tiene como principal objetivo el limitar los errores introducidos y, en segundo lugar, detectar aquellos errores que pudieran adicionarse mediante métodos de verificación. Para ello, es necesario disponer de compiladores, linkadores, además de herramientas para verificación y validación. El *Software Development Plan* contiene cronogramas de eventos y entregables, debiendo someterse a revisiones periódicas que tengan

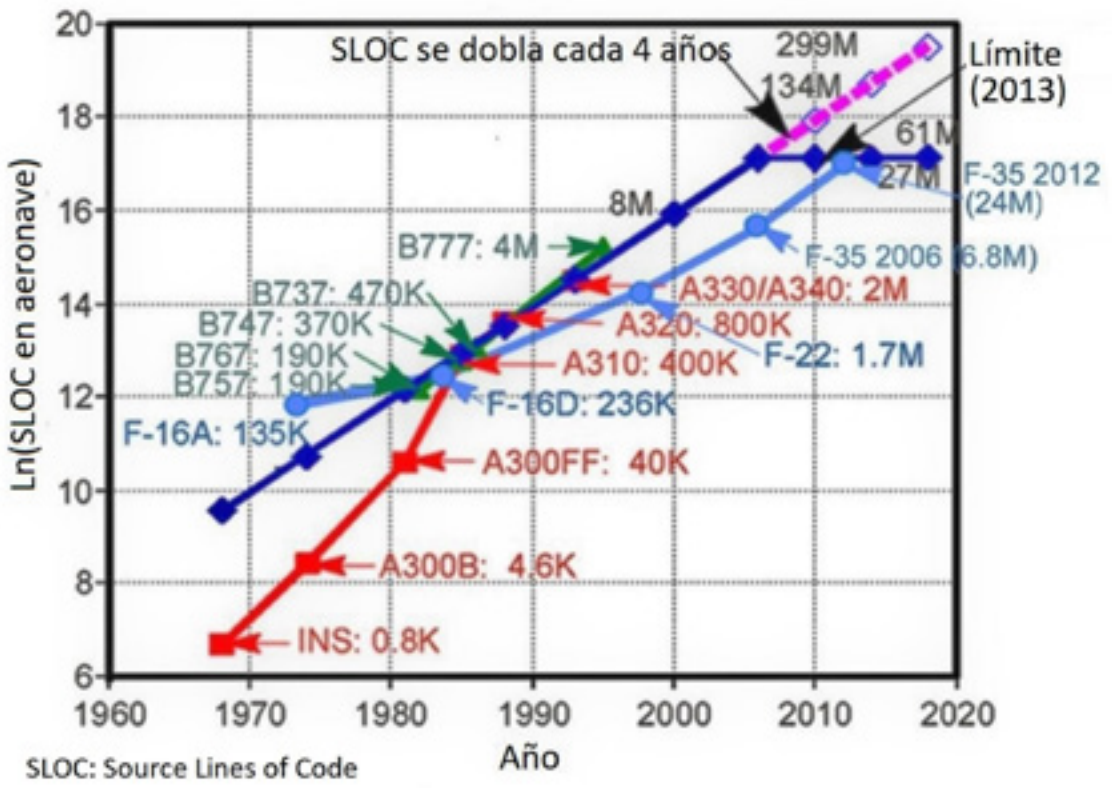

Fig. 3. Crecimiento del número de líneas de código *software* en aeronave (Fuente: Boeing Airbus).

Fig. 4. Gestión de riesgos de seguridad (Fuente: Doc 9859 AN/474 OACI).

en cuenta modificaciones y desviaciones, contemplando el ciclo de vida en el desarrollo del *software*.

Software Development Process

A partir de las especificaciones iniciales se generan los requisitos de alto nivel, que deben ser desarrollados para generar los requisitos de usuario, los cuales tienen que ser traducidos a requisitos *software*. El proceso de desarrollo *software* convierte estos requisitos en arquitectura *software* que, mediante un proceso secuencial, son transformados en código. El conjunto de los requisitos *software* es lo que el DO-178C denomina requisitos del sistema, los cuales no solo incluyen aquello que debe hacer el *software* sino también otro tipo de requisitos, como la evaluación de seguridad del sistema o el rendimiento. La validación es el proceso final donde se determina que los requisitos de *software* son correctos, están libres de errores y están completos. El DO-178C no da una guía como tal para las pruebas de validación, ya que se parte de la base de que si la verificación del *software* es correcta, no deberían aparecer problemas de validación en las pruebas de integración y sistema. El *Software Development Process* considera el desarrollo *software* como un ciclo de vida que comienza con la planificación y desarrollo, de acuerdo a los requisitos *software*, continúa con la verificación y validación, finalizando con la implantación mediante la carga en flota y su posterior mantenimiento.

Software Verification Process

La verificación del *software* busca obtener una evidencia de que es correcto contra los requisitos. Así, este proceso consiste en revisiones de requisitos, revisiones de diseño, de estado, de arquitectura, de código, análisis y pruebas, que van desde la implementación del *software* hasta la entrada de datos, pasando por la inyección de fallos controlados que identifican fuentes de errores y/o estadística de probabilidades de eventos, examinando la trazabilidad de las salidas de los procesos.

Especial relevancia cobran en este proceso las pruebas de no regresión que garantizan que, al modificar un *software*, no se introducen errores adicionales y continua cumpliendo sus funcionalidades iniciales.

Certificación del software

Mediante la certificación del *software*, los programadores/desarrolladores dan evidencia a la Autoridad Aeronáutica de que es seguro. Técnicamente, la certificación se refiere a la evaluación de la conformidad que asegura que un producto, proceso o sistema de gestión cumple unos requisitos específicos.

De acuerdo al estándar DO-178/ED-12, el proceso de certificación se alcanza cuando se demuestra ante la Autoridad Aeronáutica el cumplimiento del *Plan for Software Aspect of Certification* (PSAC), plan que ha sido previamente aprobado por dicha Autoridad. Asimismo, el *Software Accomplishment Summary* (SAS) da evidencias que demuestran el cumplimiento del PSAC, describiendo el sistema de forma general en cuanto a arquitectura, funciones y características de seguridad, entre otras.

El PSAC enlaza con los cuatro planes restantes que exige el DO-178/ED-12: el SDP, ya visto anteriormente, el *Quality Assurance Plan* (QAP), el *Configuration Management Plan* (CMP) y el *Software Verification Plan* (SVP). El QAP especifica cómo se llevaran a cabo las auditorías del *software* y de los procesos que se ven involucrados. El CMP define el control de configuración del *software*, el control de revisiones, la trazabilidad y los informes requeridos. El SVP es similar al SDP pero concretando el proceso de revisión (interno, externo, por pares,…), actividades de verificación del *software*, de requisitos, de diseño,

tipos de herramientas para verificación, revisión de procedimientos de prueba, etc.

Consorcio FACE

La carga de trabajo que suponen los protocolos de seguridad *software* junto al imparable aumento en el empleo del mismo ha provocado tal incremento de costes que, si se continúa con la actual tendencia, la futura generación de Sistemas de Armas no podrá abordarse con los presupuestos actuales. Por ello, los Estados Unidos han tomado cartas en el asunto en un esfuerzo de estandarización y normalización en diversas áreas, lanzando en 2010 el *Consorcio Open Group* FACE (*Future Airborne Capability Environment*) [8] al objeto de definir un entorno de programación de *software* abierto para todo tipo de plataformas militares aerotransportadas. Este entorno de aplicación funcional y compartible, busca disminuir costos y tiempos, a la par que intensificar la seguridad, promoviendo la reutilización, portabilidad, modularidad e interoperabilidad del *software* mediante la utilización de principios de diseño y la definición de una arquitectura común de referencia. Esponsorizado por el US *Army*, la US *Navy* y la USAF (*United States Air Forces*), así como las compañías Boeing, Lockheed Martin y Collins, actualmente el FACE es un grupo de proveedores de la industria, clientes, centros y usuarios, con una amplia trayectoria en el desarrollo *software*, cuyo número sigue creciendo, acercándose al centenar [9].

El enfoque adoptado por el FACE es una estrategia nacional, industrial y comercial estadounidense, para dotarse de sistemas *software* a costes asequibles, que promueven la innovación e integración rápida de capacidades entre distintos programas. El Consorcio FACE proporciona un foro de intercambio, donde industria y gobierno trabajan conjuntamente para el desarrollo y consolidación de estándares *software* abiertos, guías de trabajo, estrategias de innovación, entornos de desarrollo, herramientas de verificación y validación, etc., con el objetivo de patrocinar y fomentar:

- la portabilidad de aplicaciones a través de múltiples proveedores adheridos al consorcio FACE
- los estándares que proporcionen una arquitectura robusta de *software* de calidad
- el empleo de interfaces que permitan la reutilización de capacidades
- un amplio catálogo de aplicaciones para su uso en todo el espectro de sistemas a través de un entorno operativo común
- el dotarse de mayores capacidades que lleguen al cliente más rápidamente
- las aproximaciones a estándares abiertos dentro de los diferentes sistemas de aviónica
- la adquisición de productos del estándar FACE
- la disminución de costes de los sistemas FACE
- la innovación y competencia dentro de la industria de *software* de aviónica.

Para cumplir con los objetivos, el FACE parte de un estándar técnico que emplea una arquitectura patrón de referencia, la cual evoluciona un desglose conceptual de funcionalidades, promoviendo la reutilización de paquetes *software*, compartiendo capacidades entre sistemas diversos. Esta arquitectura define interfaces estandarizados para permitir que los paquetes *software* desarrollados por compañías diferentes puedan instalarse en distintos sistemas. Los interfaces estandarizados siguen una arquitectura de datos homogénea que garantice la comunicación entre paquetes instalados en componentes diferenciados.

El origen del FACE parte de los programas de arquitectura abierta desarrollados por la NAVAIR (*US Naval Air Systems Command*) que surgieron en un intento de mejorar la interoperabilidad y la portabilidad del *software* de aviónica en las plataformas de aviación naval, al cual se unieron posteriormente el US *Army* y la USAF. El objetivo en sí no deja de ser ambicioso, reducir el ciclo típico de desarrollo de nuevas capacidades

Probabilidad del riesgo	Severidad del riesgo				
	Catastrófico A	Peligroso B	Mayor C	Menor D	Insignificante E
Frecuente 5	5A	5B	5C	5D	5E
Ocasional 4	4A	4B	4C	4D	4E
Remoto 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremadamente improbable 1	1A	1B	1C	1D	1E

Fig. 5. Matriz de riesgos (Fuente: Doc 9859 AN/474 OACI).

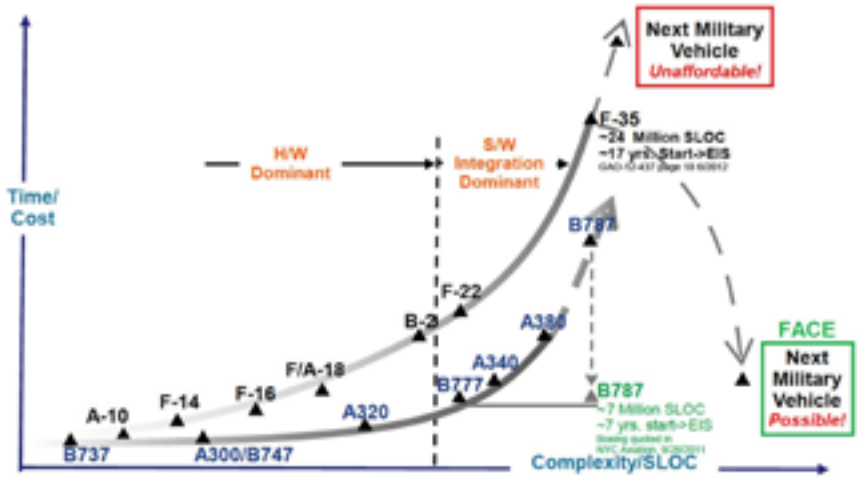

Fig. 6. Con la actual tendencia, la futura generación de Sistemas de Armas sería inabordable (Fuente: FACE consorcio).

software en plataformas aerotransportadas militares, que actualmente se estima en hasta seis años, a tan solo seis meses.

El objetivo último del FACE es consolidarse como estándar de *software* abierto, en tiempo real, para hacer que aquellas aplicaciones informáticas de carácter crítico para la seguridad adquieran una mayor solidez, sean más interoperables, portables, a la par que seguras. Aunque el consorcio se orientó inicialmente a la aviónica, en estos momentos el ámbito de aplicación se ha vuelto mucho más amplio en un intento por involucrar otro tipo de tecnologías.

Conclusiones

La utilización de *software* embarcado se ha incrementado sustancialmente en los últimos años, adquiriendo mayores funcionalidades, lo cual abarca también a los sistemas críticos de las aeronaves. Para ello es preciso aplicar los procedimientos más innovadores, como el estándar DO-178/ED-12 para el desarrollo, que permite efectuar la verificación y validación del *software* aeronáutico, acelerando los trámites de certificación ante la Autoridad Aeronáutica.

Actualmente, los Sistemas de Armas resultan cada vez más costosos de adquirir, lo cual supone sucesivas extensiones del tiempo de vida, retrasando así su retirada en servicio. En estas circunstancias, mantener la capacidad operativa de estos sistemas pasa por la adopción de actualizaciones que le permitan hacer frente a las nuevas amenazas, bien sea mediante nuevos dispositivos físicos o renovación de los ya existentes, o bien a través de cambios *software*, verificando y validando que la alteración introducida cumple las especificaciones y es segura para el vuelo. Para ello se aplican las técnicas más modernas con la finalidad de eliminar el riesgo o, si no se pudiera, mitigarlo hasta niveles tolerables de seguridad, lo cual permitirá agilizar los trámites de certificación de estas modificaciones ante la Autoridad Aeronáutica.

Este aumento incontrolado del *software* embarcado también conlleva electos colaterales, como son unos costes prohibitivos, difíciles de asumir en el futuro por las naciones. Conscientes de este problema, los Estados Unidos han lanzado el consorcio FACE bajo las premisas de compartición, reusabilidad, portabilidad, modularidad e interoperabilidad del *software*, en el mayor número posible de Sistemas de Armas.

Referencias

[1] *Air Force Times*. https://www.airforcetimes.com/opinion/commentary/2020/03/02/congress-is-ultimately-to-blame-for-f-35-fiasco/.

[2] 610.12-1990 - IEEE *Standard Glossary of Software Engineering Terminology*, 31 de diciembre de 1990. https://ieeexplore.ieee.org/document/159342. DOI: 10.1109/IEEESTD.1990.101064.

[3] Reglamento de Aeronavegabilidad de la Defensa, Boletín Oficial del Estado número 255, Real Decreto 866/2015, de 2 de octubre.

[4] *Software Considerations in Airborne Systems and Equipment Certification*, 1 de diciembre de 1992. https://www.academia.edu/24446830/SOFTWARE_CONSIDERATIONS_IN_AIRBORNE_SYSTEMS_AND_EQUIPMENT_CERTIFICATION.

[5] DO-178C: *Improved certification for cost-effective avionics systems*. http://vita.mil-embedded.com/articles/do-178c-certification-cost-effective-avionics-systems/.

[6] Manual de gestión de la seguridad operacional, Doc 9859 AN/474 OACI, 2009.

[7] Richard Hawkins, Ibrahim Habli, Tim Kelly, John McDermid; *Assurance cases and prescriptive software safety certification: A comparative study, Journal Safety science*, vol 59, 2013. http://www.sciencedirect.com/science/article/pii/S0925753513001021 DOI: 10.1016/j.ssci.2013.04.007.

[8] https://www.electronicproducts.com/host-opens-military-coffers-to-embedded-systems-developers/.

[9] FACE *Future Airborne Capability Environment*. https://www.opengroup.org/face.

Boletín de Observación Tecnológica en Defensa

Disponible en

http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/Publicaciones.aspx?cat=BOLETINES TECNOLÓGICOS

https://publicaciones.defensa.gob.es/catalogsearch/result/?cat=0&q=boletin+de+observaci