Boletín DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA

SUBDIRECCIÓN GENERAL DE PLANIFICACIÓN, TECNOLOGÍA E INNOVACIÓN
Boletín de Observación Tecnológica en Defensa n.º 49 • 1.er trimestre de 2016

Jornadas de pruebas de vuelo - Proyecto RAPAZ

El problema de la seguridad del software

Estrategia de Tecnología e Innovación para la Defensa 2015

El futuro del grafeno (IV): fotónica, optrónica y sensores químicos y biosensores

Edita:

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA · SECRETARÍA GENERAL TÉCNICA · SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL

NIPO en línea: 083-15-183-4
NIPO impresion 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 (SDG PLATIN) de la Dirección General de Armamento y Material (DGAM). C/ Arturo Soria 289, 28033 Madrid; teléfonos: 91 395 46 31 (Dirección), 91 395 46 85 (Redacción); observatecno@oc.mde.es.

Director: CF. Ing. José María Riola Rodríguez.

Redacción: Héctor Criado de Pastors, Jaime de la Parra Díaz.
Consejo Editorial: Óscar Jiménez Mateo, Tomás A. Martínez Piquer, José Agrelo Llaverol. **Equipo de Redacción**: Nodo Gestor: Guillermo González Muñoz de Morales, David García Dolla, Cristina Mateos Fernandez De Betoño, Álvaro Blasco Pérez; Observatorio de Armas, Municiones, Balística y Protección (OT AMBP): Óscar Rubio Gutiérrez; Observatorio de Electrónica (OT ELEC): Yolanda Benzi Rabazas, Fernando Iñigo Villacorta; Observatorio de Energía y Propulsión (OT ENEP): Héctor Criado de Pastors; Observatorio de Defensa NBQ (OT NBQ): Angélica Acuña Benito; Observatorio de Materiales (OT MAT): Luis Requejo Morcillo; Observatorio de Óptica, Optrónica y Nanotecnología (OT OPTR): Ing. D. Fernando Márquez de Prado Urquía, Pedro Carda Barrio; Observatorio de UAVs, Robótica y Sistemas Aéreos (OT UAVs): Ing. D. José Ramón Sala Trigueros, Guillermo Carrera López; Observatorio de Sistemas Navales (OT SNAV): CF Ing José María Riola Rodríguez, Juan Jesús Díaz Hernández, Jaime de la Parra Díaz; Observatorio de Sistemas Terrestres (OT STER): Cap. Carlos Calderón Carnero; Observatorio de Tecnologías de la Información, Comunicaciones y Simulación (OT TICS): Bernardo Martínez Reif, Isabel Iglesias Pallín.

Portada: Pista de lanzamiento e instalaciones de la campaña de vuelo RAPAZ, en la base militar Conde de Gazola, situada en el Ferral de Bernesga, León, España. (Fuente: DGAM), artículo «Jornadas de pruebas de vuelo - Proyecto RAPAZ».

El Boletín de Observación Tecnológica en Defensa es una publicación trimestral en formato electrónico del Sistema de Observación y Prospectiva Tecnológica orientado a divulgar y dar a conocer iniciativas, proyectos y tecnologías de interés en el ámbito de Defensa. El Boletín está abierto a cuantos deseen dar a conocer su trabajo técnico. Los artículos publicados representan el criterio personal de los autores, sin que el Boletín de Observación Tecnológica en Defensa comparta necesariamente las tesis y conceptos expuestos.

Colaboraciones y suscripciones:
observatecno@oc.mde.es

http://www.defensa.gob.es/areasTematicas/investigacionDesarrollo/sistemas/

SOPT
DGAM
Subdirección General de Planificación, Tecnología e Innovación

CONTENIDOS

ETID 2015

La Política de Armamento y Material, dentro del marco normativo por el que se regula el proceso de obtención de los recursos materiales, demanda la materialización de unas políticas específicas y unas líneas generales de actuación que afectan, entre otras, a la Investigación, Desarrollo e Innovación.

La visión a futuro es disponer de un sistema de I+D+i de defensa capaz de aprovechar tanto sus capacidades y recursos propios como las oportunidades externas a las que se pueda acceder. En este sentido se debe actuar en el conjunto de ámbitos tecnológicos que son relevantes para las misiones de las FAS en relación a diferentes niveles de madurez de las tecnologías que se precisan, de forma que la base tecnológica e industrial nacional pueda dar respuesta tanto a las necesidades tecnológicas actuales como adelantarse a los retos tecnológicos que depare el futuro.

Para ello, la I+D+i de defensa debe sustentarse prioritariamente sobre la capacidad tecnológica e industrial nacional, lo que obliga a orientar adecuadamente el esfuerzo de todos los actores implicados (administración, empresas, academia, organismos de investigación) en la misma dirección.

En los últimos años, el Ministerio de Defensa ha liderado diferentes iniciativas y actuaciones al objeto de que las empresas españolas aumenten su competitividad. Entre estas iniciativas y actuaciones, cabe destacar el desarrollo de la Estrategia de Tecnología Innovación para la Defensa (ETID).

Esta Estrategia, que ha sido actualizada durante el año 2015, constituye un documento de alto valor en el campo de la I+D+i en defensa por su capacidad de dar a conocer un modelo de organización más eficaz, siempre con el objetivo último de dotar a las Fuerzas Armadas de los mejores y más modernos sistemas de armas que satisfagan las capacidades militares.

La revisión de la ETID se ha producido en un contexto muy diferente al de la anterior versión, tras años de profundos cambios económicos, tecnológicos y de amenazas para la defensa y la seguridad, tanto en el contexto internacional como en el nacional. Consecuencia de ello es que la ETID 2015 tiene un carácter más integral, lo que permite que sirva a todos los actores vinculados a la I+D+i de defensa y seguridad como principal herramienta de orientación sobre la dirección a la que se va a dirigir ésta, promovida por el MINISDEF.

Para la DGAM, la ETID supone una responsabilidad, dada la importancia de los objetivos abordados, y un exigente desafío, teniendo en cuenta el contexto dinámico de cambio en el que vivimos. Pero supone sobre todo una fuente de motivación adicional, conscientes de la importancia de la I+D+i como elemento de impulso y evolución de las necesidades de las FAS.

Actualidad

¿Dónde hemos estado?

6 de octubre

Jornada «Retos y oportunidades de la I+D+i en los nuevos escenarios de la Defensa y la Seguridad»

En la Jornada se expusieron las necesidades de la Fuerzas Armadas en los nuevos escenarios en el ámbito de la I+D de Defensa y Seguridad, resaltando la importancia del fomento del desarrollo tecnológico y el fortalecimiento de las capacidades tecnológicas de uso dual.

29 de octubre

Unmanned Maritime Systems

La Jornada fue organizada de manera conjunta por la Agencia Europea de Defensa (EDA) y EuroDefense (Alemania) en la sede representativa del estado Schleswig-Holstein en Berlín. Durante la misma se enfatizó el importante papel que viene realizando la EDA mediante el impulso de capacidades conjuntas, la promoción de la cooperación en esta materia mediante el programa UMS, así como el esfuerzo que está realizando por consolidar la base tecnológica e industrial.

2 de noviembre

Jornada presentación resultados proyectos I+D AMMS y CITIUS

En la Jornada, organizada de manera conjunta por la Subdirección de Planificación Tecnología e Innovación (SDGPLATIN) y NAVANTIA en las instalaciones de la Jefatura del Apoyo Logístico de la Armada (JAL), se presentaron los proyectos «AMMS - Impact of Mission Modularity on a Naval Ship's Life Cycle Cost» y «CITIUS - Command and Control for InTeroperability of Unmanned Systems».

21 de enero

Jornada de participación del MINISDEF en el Programa H2020

La jornada tuvo el objeto de identificar las temáticas de potencial interés para las Unidades del Ministerio de Defensa de cara a participar en el Programa Marco H2020 de la UE para el período 2014-2020, que promueve el lanzamiento de proyectos de I+D+i encaminados a abordar los principales retos sociales existentes, así como el liderazgo industrial en Europa y reforzar la excelencia de su base científica.

... entre otros eventos

¿Dónde hemos estado?

26 y 27 de enero

Civil Dron 2016

El evento, organizado por la Fundación de la Energía de la Comunidad de Madrid, en colaboración con la Agencia Europea de la Energía, trató sobre la actualidad de los vehículos aéreos no tripulados, legislación, normativa, materiales, propulsión, sistemas de control y comunicaciones entre otros.

26 y 27 de enero

III Jornadas Ciberseg 2016

El objetivo de dichas Jornadas, organizadas por la Universidad de Alcalá de Henares, fue la promoción y difusión de temas relacionados con la seguridad y la ciberdefensa.

28 de enero

Instrumentos para financiar la I+D+i

El Instituto Tecnológico del Plástico de Valencia (AIMPLAS), organizó el pasado 28 de Enero esta Jornada, en la que diversas instituciones públicas como MINECO o CDTI, presentaron algunos de los instrumentos de financiación y futuras convocatorias de ámbito nacional para proyectos de I+D. La jornada tuvo la participación del SOPT con una ponencia sobre el Programa COINCIDENTE como un instrumento más de financiación de proyectos nacionales.

28 al 31 de enero

Global Robot Expo 2016

Entre los días 28 y 31 de enero tuvo lugar «Global Robot Expo», uno de los mayores eventos sobre tecnologías robóticas de Europa, espacio donde fabricantes, investigadores, inversores, integradores y potenciales clientes se pusieron en contacto, mostrándose las novedades del momento, todo ello acompañado de actividades de ocio relacionadas con dichas tecnologías.

10 y 24 de febrero

Jornadas CIS de apoyo sanitario en operaciones

El Servicio de Telemedicina del Hospital Central de la Defensa «Gómez Ulla» de Madrid organizó estas Jornadas de sensibilización por parte de todos los actores involucrados en los sistemas de información sanitarios, desde el punto de vista de sistemas y funcional enfocado en dos temas principalmente (COP (Common Operational Picture) sanitaria y Telemedicina).

... entre otros eventos

¿Dónde hemos estado?

10 y 11 de febrero

5º Foro Europeo para la Ciencia, Tecnología e Innovación (TRANSFIERE)

Celebrado en el Palacio de Ferias y Congresos de Málaga. El Ministerio de Defensa, a través de la SDG PLATIN, contando con representación en el Área de Administraciones Públicas, mantendría reuniones programadas con universidades, fundaciones, asociaciones y con empresas interesadas en cooperar en el sector Defensa.

11 de febrero

Forum Ciberseguridad 2016

En esta Jornada, organizada por IDC España e IDG Comunicaciones y celebrada en el Hotel Ritz de Madrid, se llevó a cabo el análisis de las tendencias de ataque y seguridad en el ámbito de la ciberdefensa, motivado principalmente por los nuevos métodos de ataque, el creciente uso de dispositivos móviles y al almacenamiento en la nube que ha eliminado el concepto de «perímetro de seguridad».

19 de febrero

NANOLAB - BISITE

El día 19 de febrero de 2016 se realizó una visita al laboratorio de física aplicada NANOLAB y al centro de investigación BISITE de la Universidad de Salamanca, donde se mostraron las capacidades y últimos proyectos en el ámbito de nanodispositivos de alta frecuencia, ciberdefensa, UAVs y wearables junto con la presentación del proyecto integral Biodiesel para equipos de campaña.

23 al 26 de febrero

SICUR 2016

Entre los días 23 y 26 de febrero de 2016 tuvo lugar «SICUR 2016 - Salón Internacional de la Seguridad», organizado por IFEMA, en el que se congregó a empresas, asociaciones, profesionales y usuarios de seguridad, protección y prevención, y donde los principales campos de actuación fueron la seguridad contra incendios y emergencias, seguridad laboral, defensa, así como la presentación de una selección de innovadores sistemas y soluciones relacionados.

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

ETID 2015

Autor: Héctor Criado de Pastors, OT ENEP, SDG PLATIN.

Palabras clave: ETID, Estrategia de Tecnología e Innovación para la Defensa, I+T, I+D+i.

Líneas de actuación funcional relacionadas: LAF 0.1.

La Estrategia de Tecnología e Innovación para la Defensa (ETID) es una iniciativa derivada de la política de I+D+i del MINISDEF que pretende proporcionar orientación tecnológica y promover la coordinación entre los diferentes actores, tanto internos como externos al Departamento, implicados en el desarrollo de la tecnología vinculada a las necesidades actuales y futuras de las FAS. Puede considerarse un documento de planeamiento, tanto desde el punto de vista interno de las FF.AA. como de los distintos agentes externos involucrados en el I+D+i.

Fig. 1. Vinculación entre la misión de la I+D+i del MINISDEF y los tipos de actividades. (Fuente: ETID 2015).

La nueva versión de la Estrategia de Tecnología e Innovación para la Defensa, ETID 2015, supone una actualización programada de la Estrategia publicada en el año 2010 que adecúa su contenido a la realidad actual y a los retos futuros, de forma que constituya una base sólida sobre la que articular la I+D+i de la Defensa en los próximos años. Durante el periodo de vigencia de la ETID 2010, la realidad nacional e internacional de crisis económica dificultó sensiblemente su desarrollo e implementación. Así mismo, se produjeron profundas transformaciones tanto en los panoramas estratégico, económico y tecnológico, a las que hay que sumar los cambios en la propia organización del Ministerio de Defensa.

La ETID 2015 es un documento más integral en el sentido de no ceñirse exclusivamente a los aspectos tecnológicos e incluir aspectos de política de I+D+i y elementos para desarrollar dicha política, cuya misión es contribuir a satisfacer las necesidades de las fuerzas armadas, tratando de alcanzar la ventaja operativa en base a la incorporación de nuevas tecnologías. Otras de las finalidades es la de contribuir a la capacitación de la base tecnología e industrial de la defensa, de forma que pueda aportar soluciones a esas necesidades. Todo ello en base al desarrollo de tecnología aplicada a través de demostradores y al desarrollo de prototipos, dado que el I+D+i en defensa tiene un carácter eminentemente finalista.

Fig. 2. Principales instrumentos de la I+D+i de Defensa. (Fuente: ETID 2015).

Una importante novedad de esta edición, es que en ella, y derivada de la misión de la I+D+i de Defensa, se establecen las directrices principales para su desarrollo: orientar las inversiones hacia temas prioritarios, aprovechar todas aquellas oportunidades externas para potenciar la acción de la I+D+i de Defensa, y mejorar la calidad y aprovechamiento de los resultados, involucrando en el proceso tanto a los usuarios finales como a los distintos agentes del I+D+i.

Otro de los cambios significativos se refiere al énfasis que se pone en diferenciar los objetivos tecnológicos de las herramientas disponibles para promover su desarrollo, a través de Instrumentos vinculados al desarrollo de soluciones tecnológicas, instrumentos de Coordinación y Cooperación y, por último, instrumentos vinculados al Conocimiento Tecnológico.

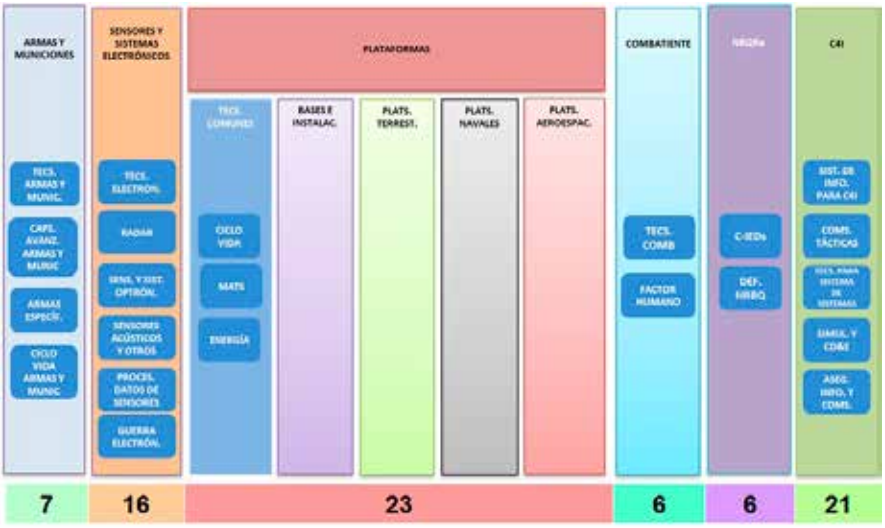

Fig. 3. Estructura de Áreas y Líneas de Actuación Funcional. (Fuente: ETID 2015).

Desde el punto de vista tecnológico, se ha puesto un especial énfasis en que la ETID tenga un enfoque más integral, de forma que cubra todas las actuaciones en I+D+i a diferentes niveles de madurez. A diferencia de la ETID 2010, que se focalizaba en las actividades menos maduras de I+T, en la versión actual se trata de recoger en una misma estrategia todas las actuaciones en I+D+i (tanto de I+T como de Desarrollo), intentando que exista una mayor continuidad y coherencia entre todas ellas, de cara a propiciar que los desarrollos de menor madurez se trasladen a soluciones reales.

Se incluye una versión actualizada de las Metas Tecnológicas que sirven de orientación tanto a las inversiones en I+D+i del Ministerio como de orientación a la base tecnológica e industrial nacional. Así mismo, se ha considerado conveniente revisar la organización de las metas en una estructura de Áreas y Líneas de Actuación Tecnológica diferente, a partir de la experiencia de realizar seguimiento en las metas de la ETID 2010, así como en un esfuerzo por adecuar la estrategia de I+D del MINISDEF a los nuevos retos operativos y avances tecnológicos.

Como resultado, el número de metas se ha reducido a setenta y nueve, combinando metas que abordan problemáticas ya presentes en los sistemas en servicio con otras que tratan aspectos más novedosos, hasta la fecha no tratados.

Las actuaciones que se han previsto llevar a cabo durante la fase de implantación de la Estrategia, al igual que la ETID 2010, se agrupan en cuatro ejes: el eje tecnológico, que establece las metas tecnológicas que guíen el planeamiento de I+D+i del MINISDEF; el eje de información, que ayuda a orientar a la base tecnológica e industrial nacional sobre los intereses tecnológicos del MINISDEF y a establecer mecanismos de intercambio de información; el eje de Coordinación y Cooperación, que facilita sinergias con el Sistema de I+D+i nacional y con los organismos de I+D+i internacionales vinculados a defensa y seguridad; y el eje de mejora continua, que optimiza la gestión de la I+D+i del MINISDEF y facilita el aprovechamiento de sus resultados. Para cada eje, se han establecido actuaciones particulares que serán abordadas durante el periodo de vigencia de la ETID.

Por último, es necesario destacar la relación existente entre la ETID y la Estrategia Industrial de Defensa (EID), documento de referencia para el desarrollo de las actuaciones contempladas en la ETID. La complementariedad y alineamiento de la ETID con las actuaciones contempladas en los diferentes Ejes de la EID, establece un nuevo marco de trabajo orientado a potencia las actuaciones del Ministerio en materia tecnológico e industrial.

La ETID 2015 está disponible públicamente a través del Portal de Tecnología e Innovación del MINISDEF.

Fig. 4. Portada ETID. (Fuente: ETID 2015).

III Congreso Nacional de I+D en Defensa y Seguridad

Autores: CF. Ing. José Mª Riola Rodríguez, Jefe de Unidad de Prospectiva y Estrategia Tecnológica, SDG PLATIN; Dª Cristina Mateos Fernández de Betoño, Nodo Gestor, SDG PLATIN.

Palabras clave: armas, municiones, sensores y sistemas electrónicos, plataformas, combatiente, C4I, defensa, seguridad.

Áreas de actuación funcional relacionadas: AT 1, AT 2, AT 3, AT 4, AT 5, AT 6.

Fig. 1. III Congreso Nacional de I+D en Defensa y Seguridad. (Fuente: Buxton, Daggitt y King - Cargo Access Equipment for a Merchant Ship).

Durante los pasados días 19 y 20 de noviembre se celebró en la Escuela naval Militar de Marín (Pontevedra), la tercera edición del Congreso Nacional de I+D en Defensa y Seguridad, cuyo objetivo sería la integración y puesta en común de la investigación entre los diferentes actores del ámbito de la I+D de Defensa y Seguridad, Universidades, OPIs, empresas y laboratorios que exponen sus trabajos y líneas de investigación de carácter innovador.

Durante la sesión inaugural, el Vicerrector del Campus de Pontevedra D. Juan Manuel Corbacho destacó el papel que viene realizando el CUD contribuyendo a formar parte de su campus a través del trabajo que desarrollan. Por otra parte, el Director de la Escuela Naval, CN José Manuel Nuñez Torrente, insistió en el compromiso con la ciencia y la formación de este centro militar de la Armada. El Director de la Agencia Gallega de Innovación D. Manuel Varela Rey, hizo especial hincapié en cómo este foro es una «oportunidad muy importante para el intercambio de conocimientos» y llamó a «aprovechar el carácter dual de muchas innovaciones». El Director de Educación Naval (DIENA), CA Aniceto Rosillo resaltó el importante papel del CUD como órgano responsable de elaborar y proponer planes y programas de estudios de las enseñanzas militares de formación y perfeccionamiento de esta escuela de la Armada. El Director del CUD de Marín, D. José María Pousada agradeció la participación y asistencia al mismo, y finalmente el VA Jesús Manrique Braojos (SDG PLATIN) incidió en las iniciativas que se vienen realizando en materia de I+D+i, tanto nacionales como a nivel internacional.

Al igual que en pasadas ediciones, se estructuró alrededor de unas ponencias plenarias, este año, organizadas en las siguientes temáticas: Contribución del IEEE a Defensa y Seguridad; Construcción Naval; Ingeniería de Defensa y Trabajos Fin de Grado en los CUDs.

Cabe destacar el éxito de participación de esta tercera edición, no sólo desde la parte universitaria adscrita al Ministerio de Defensa (CUDs), sino también del resto de Universidades y entramado empresarial relacionado con las actividades de Defensa. Se presentaron en torno a 140 artículos técnicos, cuyas ponencias se organizaron en seis sesiones en paralelo y las cuales cubrieron las siguientes áreas: Adquisición de Información y Procesado; Guiado, Energía y Materiales; Entorno, Sistemas y Modelado; Sociedad, Economía y Humanidades. Se ha logrado en el transcurso de estos tres años, un gran éxito en las nuevas convocatorias, con un incremento sustancial del número de artículos técnicos de gran interés respecto a las ediciones anteriores, por lo que se puede resaltar la consolidación de dicho congreso, habiendo despertado interés entre la industria y universidades.

Fig. 2. Logo DESEi+D. (Fuente: Portal CUD Marín).

Como novedad en esta edición, entre las ponencias se encontraron trabajos de fin de grado de los Centros Universitarios de Defensa de Marín, San Javier, Zaragoza y de la Guardia Civil, fruto de la gran labor que están realizando todos ellos. Este año ha sido la primera promoción en la que los nuevos Oficiales recibieron también las distintas titulaciones de graduados, sin olvidar al Centro Universitario de Madrid del que saldrá la primera promoción en dos años.

En el ámbito de este congreso, la DGAM, expuso las necesidades y prioridades presentes en las Fuerzas Armadas, tuvo conocimiento de las actividades en el campo civil que pueda ser de su interés y dio a conocer la nueva edición de la Estrategia de Tecnología e Innovación para la Defensa y su conjunto de metas tecnológicas que representan los principales intereses tecnológicos del Ministerio de Defensa en los próximos años y sirven de guía de orientación a futuras ediciones del Congreso y a nuevas propuestas al programa COINCIDENTE.

Seminarios IST - 134 «*Advanced Algorithms for Effectively Fusing Hard and Soft Information*»

Autor: Fernando Iñigo Villacorta, Área de Cooperación Internacional de I+D, SDG PLATIN.

Palabras clave: fusión de información, soft information, hard information, procesamiento de la información.

Metas tecnológicas relacionadas: MT 2.5.2; MT 6.1.4.

La Dirección General de Armamento y Material (DGAM) y la Universidad de Salamanca, a través del grupo de investigación BISITE, han colaborado para la organización en España de una sesión de los seminarios internacionales **IST-134 «*Advanced Algorithms for Effectively Fusing Hard and Soft Information*»**, promovidos por la Organización de Ciencia y Tecnología de la OTAN (STO - *Science and Technology Organization*). La sesión mencionada se celebró los días 15 y 16 de octubre de 2015 en el Colegio Arzobispo Fonseca de la Universidad de Salamanca.

Los seminarios o clases magistrales de la STO («*Lecture Series*», por su denominación en inglés) son eventos de carácter formativo que se organizan anualmente en distintos países de la OTAN, con el objetivo de difundir el estado del arte en temas científicos y tecnológicos de gran interés para la Alianza y sus Estados Miembros. Estos seminarios están dirigidos a especialistas del ámbito operativo, académico e industrial y constituyen una excelente oportunidad para las naciones que los acogen, ya que son impartidos por expertos de reconocido prestigio internacional en la temática considerada.

Los seminarios IST-134 estuvieron enfocados a la problemática de la fusión de información de tipo «*hard*» y «*soft*». En general, se considera información de tipo «*hard*» toda aquella información que es cuantificable de manera numérica, fácil de registrar y transmitir e independiente del proceso de recolección. En esta categoría entrarían, por lo tanto, la información obtenida a través de los distintos tipos de sensores (radar, cámaras ópticas

Fig. 1. Cartel de las Jornadas. (Fuente: BISITE (USAL)).

e infrarrojas, sensores acústicos, etc.). La información «*soft*», por el contrario, es difícil de medir y de cuantificar, aunque puede ser muy exacta en cuanto a la información a transmitir. Dentro de esta categoría entraría principalmente la información textual o conversacional (p. ej.: informes transmitidos de un soldado) y el conocimiento del contexto en el que se obtiene esa información.

Tanto la información «*hard*» como la «*soft*» están presentes en grandes volúmenes en los entornos operativos actuales, procedentes de múltiples fuentes con un elevado grado de heterogeneidad. Por lo tanto, resulta esencial

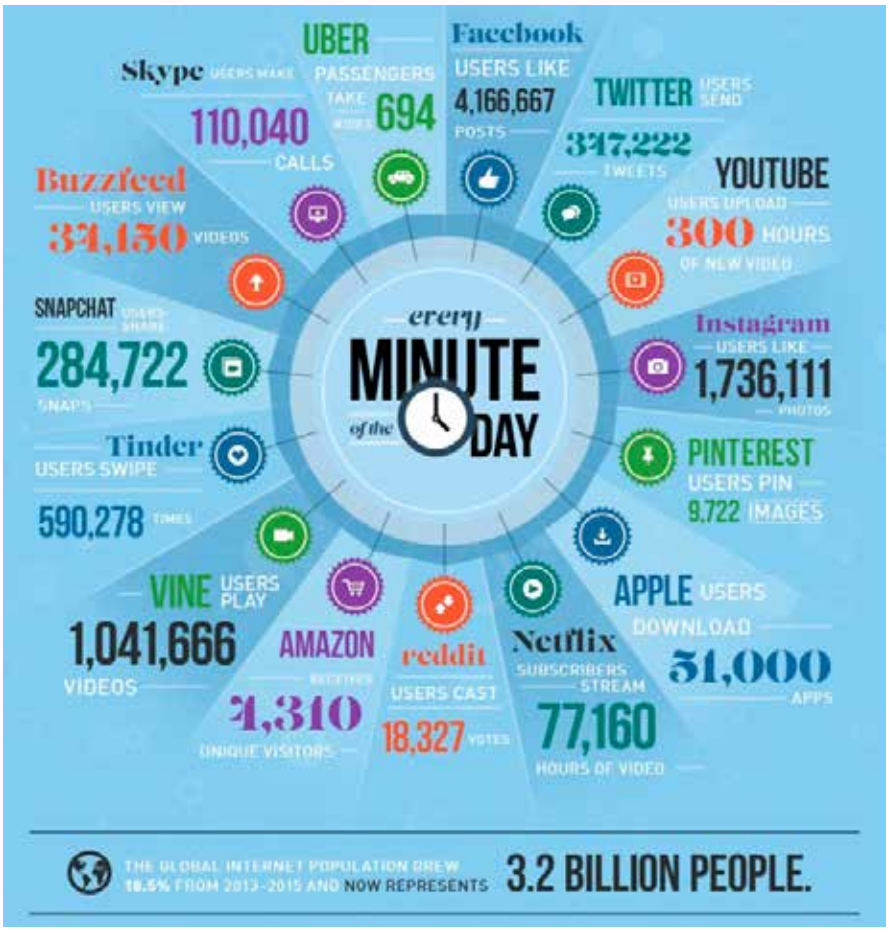

Fig. 2. Cada minuto del día se generan ingentes volúmenes de datos procedentes de todo tipo de dispositivos electrónicos. Las técnicas para fusión de información de tipo "soft" resultan esenciales para poder extraer información de inteligencia, relevante para seguridad y defensa, de todos estos datos. (Fuente: www.domo.com).

desarrollar los algoritmos y herramientas adecuadas que permitan la fusión de todos estos elementos para conseguir la información de inteligencia necesaria para el éxito de las operaciones.

Hasta la fecha, las comunidades «*hard*» y «*soft*» han tendido a trabajar muy aisladas entre sí, enfocadas en sus propias problemáticas. Sin embargo, se considera esencial impulsar el trabajo conjunto de ambas comunidades, ya que cada una de ellas se puede enriquecer de los algoritmos, métodos y experiencia desarrollados por la otra. En este sentido, los ponentes de los seminarios IST-134 consideran que estas charlas constituyen un importante paso adelante para promover el acercamiento entre ambas comunidades.

Las ponencias de los seminarios tuvieron, por lo tanto, componente tanto «*hard*» como «*soft*». En el primero de los casos, se habló extensamente de los algoritmos y métodos empleados en la actualidad para el seguimiento de objetivos y la fusión sensorial, así como las ventajas y desventajas de cada uno de ellos. Aunque muchas de estas técnicas se pueden considerar maduras, en ciertos casos su verdadero potencial está aún por explotar. Un buen ejemplo se puede encontrar en el ámbito de los sensores CBRN, cuya plena capacidad sólo puede alcanzarse utilizando técnicas avanzadas de fusión sensorial.

En el apartado «*soft*», las ponencias se dedicaron a dos temas: por un lado, se analizó el problema de la utilización de la información contextual, clave para interpretar correctamente la información de tipo «*hard*». Para la explotación de esta información contextual, resulta esencial el desarrollo de ontologías adecuadas para la representación de dicha información. Por otro lado, se analizaron los grandes desafíos que aún persisten para el tratamiento automatizado de la información textual. Estos desafíos, relacionados con el amplio espectro de significados que se pueden atribuir a las palabras en función de los interlocutores, del contexto en el que se produce la comunicación, de las variedades idiomáticas, etc. dificultan enormemente los avances en esta disciplina.

Se espera que esta iniciativa de acercamiento entre ambas comunidades de investigadores tenga continuidad en futuros seminarios, en los que se podrá abordar de manera más detallada los aspectos de fusión conjunta «*hard*» y «*soft*», que en estas primeras charlas se han tratado de manera más sucinta.

Las ponencias de los seminarios fueron impartidas por el Dr. Wolfgang Koch, jefe del departamento «*Sensor Data and Information Fusion SDF*» del Instituto Fraunhofer FKIE (Alemania) y director de los seminarios; la Dra. Kellyn Rein, perteneciente al mismo Instituto Fraunhofer FKIE; el Dr. Roy Streit, de la consultora científica Metron (EEUU); el Dr. Stefano Coraluppi, de la empresa Systems & Technology Research (EEUU); y el Dr. Jesús García Herreros, de la Universidad Carlos III de Madrid.

Los seminarios IST-134 se celebraron en tres localizaciones más: el Instituto Fraunhofer FKIE de Wachtberg (Alemania), el Adelphi Laboratory Centre (US Army Research Laboratory) en Adelphi (EEUU) y el DRDC de Ottawa (Canadá). La sesión celebrada en Salamanca resultó un éxito, ya que contó con la asistencia de un espectro muy amplio de participantes: miembros del Ministerio de Defensa, del Ministerio del Interior, de la industria y del ámbito académico y de investigación nacional, así como representantes de organismos de la OTAN y de ministerios de defensa, universidades y centros de investigación de otros países.

Fig. 3. Sólo mediante el uso de algoritmos avanzados de fusión sensorial puede aprovecharse plenamente la capacidad de ciertos sensores para la identificación de amenazas. En la imagen, sistema experimental HAMLeT (Hazardous Material Localization and Person Tracking) para la detección de terroristas con armas químicas. (Fuente: Instituto Fraunhofer FKIE).

Jornadas de pruebas de vuelo - Proyecto RAPAZ

Autores: Tcol. José Manuel Mateo Alonso, Área de Planificación y Control, SDG PLATIN; Guillermo Carrera, OT UAVS, SDG PLATIN.

Palabras clave: RPAS, sistemas de aeronaves remotamente pilotadas, UAVs, sistemas de aeronaves no tripuladas, sistemas aéreos no tripulados, vehículos aéreos no tripulados, micro vehículos aéreos, micro vehículos aéreos no tripulados, vigilancia aérea, reconocimiento aéreo, ISR, drones, minidrones, microdrones,

Metas tecnológicas relacionadas: MT 3.1.1; MT 3.1.3; MT 3.1.4; MT 3.5.1; MT 3.5.2; MT 3.5.3; MT 3.5.4; MT 3.5.5.

Introducción

Entre los días 9 y 12 de noviembre de 2015, tuvo lugar en la Base Militar «Conde de Gazola», situada en el Ferral de Bernesga (León), la primera de las dos campañas de vuelo del proyecto RAPAZ dentro de su primera fase de evaluación. La elección de esta localización para efectuar la campaña de vuelo se debió a la experiencia de la unidad coordinadora de las pruebas, Grupo de Artillería de Información y Localización (GAIL), en el uso de estos sistemas, al estar operando el Sistema Táctico de Vigilancia (SIVA), así como de las instalaciones que esta base posee para el uso y operación de este tipo de aeronaves, contando con una pista de 550 m de longitud para operar el SIVA.

Esta primera campaña consistió en un conjunto de pruebas de vuelo en las que se reunieron a diecisiete empresas participantes que presentarían un total de dieciocho sistemas, todos ellos de CLASE I. Para garantizar la seguridad de las jornadas, se tomó la decisión de realizar la primera campaña de vuelo de forma centralizada, de manera que todos los sistemas fueran evaluados en unas instalaciones que reuniesen los requisitos necesarios para semejante propósito debido al desconocimiento, que a priori se tenía, sobre las capacidades de vuelo reales de los sistemas presentados.

Hay que destacar la diversidad en los sistemas presentados abarcando tanto la categoría MICRO (5 sistemas) como MINI (11 sistemas) y SMALL (2 sistemas) siendo éstos tanto de ala fija, como rotatoria. Todos los sistemas presentados pasaron previamente por un proceso de certificación de aeronavegabilidad llevado a cabo por el INTA, con el fin de obtener el permiso necesario para operar en espacio aéreo segregado.

Para la evaluación de los sistemas se trató de buscar la máxima heterogeneidad en los equipos encargados de esta tarea, contando para ello con personal de diferentes unidades tanto del Ejército de Tierra, Ejército del Aire y Armada, así como observadores de EMAD, UME, INTA y otros organismos. La tarea de estos equipos consistió en la evaluación de todos los sistemas presentados en base a unos criterios de calificación establecidos, evaluándose entre otros aspectos la plataforma aérea, GCS, el montaje del sistema completo tanto plataforma aérea como GCS, briefing explicativo de las medidas de seguridad, checklist de prevuelo, así como la correcta ejecución de un conjunto de misiones pre-definidas con el fin de comprobar las capacidades reales de cada sistema. La calificación otorgada por cada evaluador estaría acompañada de una ficha descriptiva de cada sistema en la que se señalarían tanto fortalezas como debilidades destacadas, dando por tanto, una visión global de la situación de cada sistema frente a los requisitos deseados. Gracias a la variedad de evaluadores, esta información sería de gran utilidad, puesto que, además de los requisitos comunes en todas las unidades presentes, cada una de ellas presenta una serie de requisitos propios, permitiendo de esta forma, la distribución de los sistemas según los requisitos de las unidades de cara a la fase II del proyecto.

	SISTEMA (EMPRESA)
DÍA 1	BLACKHORNET (PAUKNER)
	HUGINN X1 (E&Q)
	IRIS 4 (TRIEDRO)
	ONS (SOTICOL)
DÍA 2	SHEPHERD MIL (EXPAL)
	ALCOTAN (USOL)
	SX8 (SERTEC)
	DRONEQUASAR (DRONETOOLS)
	GEODRONE (CONYCA)
	ARACNOCOPTER (ARBOREA)
	ALTEA EKO (FLIGHTECH)
DÍA 3	SNIPER (ALPHA UNMANNED)
	MANTIS (INDRA)
	RW5 VULTUR (INDA)
	ORBITER 2 (AERONAUTICS)
	MICRO B (TRIEDRO)
	SPYLITE (TRIEDRO)
DÍA 4	FULMAR (THALES ESPAÑA)

Fig. 1. Empresas participantes y sistemas proyecto RAPAZ. (Fuente: DGAM).

Jornadas de vuelo

Las jornadas de vuelo se distribuyeron a lo largo de cuatro días durante los cuales se evaluaron todos los sistemas presentados.

La primera jornada comenzó con la bienvenida por parte de la organización y de los mandos de la base Conde de Gazola, tras la que se daría un *briefing* sobre las jornadas de vuelo, respondiendo a las dudas presentadas por las empresas participantes. A lo largo de la mañana del primer día se evaluaron los sistemas de menor tamaño tanto NANO como MICRO, dado que las misiones que tenían que realizar, así como el circuito para realizarlas, difería de los sistemas de mayor tamaño. La tarde de la primera jornada fue empleada por diferentes empresas para caracterizar la pista en sus sistemas, así como para que la organización modificase ligeros aspectos organizativos de cara a las siguientes jornadas.

A lo largo de la segunda y tercera jornada se evaluaron el grueso de los sistemas presentados, un total de trece entre ambas jornadas, realizándose todas las pruebas en las instalaciones que el GAIL había preparado para la ocasión junto a la pista que emplea para operar el SIVA, teniendo que destacar la ausencia de cualquier tipo de incidencias, tanto a nivel organizativo como operacional.

A lo largo de la cuarta y última jornada, se llevaría a cabo la evaluación del último sistema, disponiéndose del *Distinguished Visitor Day* (DvD) en el que las Autoridades Militares, entre las que se encontraba el DIGAM, visitaron la exposición estática dispuesta para la ocasión en la que las empresas participantes mostraron los sistemas presentados en el proyecto RAPAZ, así como diferentes sistemas y tecnologías que desarrollan. A lo largo del DvD tuvieron lugar diferentes demostraciones aéreas de diversos sistemas.

Conclusión

Las primeras pruebas de vuelo del proyecto RAPAZ han resultado ser

un gran éxito a todos los niveles, logrando acercar los requisitos demandados por las FAS, a las empresas participantes, en su gran mayoría de ámbito civil. De la misma manera, las Jornadas han servido para conocer de primera mano, así como corroborar, la existencia de capacidad nacional para desarrollar RPAS de CLASE I, tanto de categoría micro como mini y small. Se ha podido observar que a partir de 25 kg de MTOW (*máximum take-off weight*), la inversión que es necesaria realizar, así como la complejidad para lograr desarrollar un sistema, aumenta de forma significativa. Prueba de ello es que de la categoría small con un MTOW superior a 25 kg sólo pudo ser evaluado un sistema.

Durante el 2016 tendrá lugar una segunda campaña de vuelo descentralizada, en la que se asignará el sistema más adecuado a la unidad operativa de las FAS, acorde al ámbito de los ejercicios de instrucción y adiestramiento programados.

Esta segunda fase conceptual o de evaluación operativa termina con la remisión de un informe que refleja los resultados de las pruebas realizadas, identificando las carestías o mejoras a realizar por la empresa para cumplir los requisitos exigidos por las distintas unidades usuarias de estos sistemas en las FAS.

Fig. 2. Vehículos aéreos no tripulados participantes en el Proyecto RAPAZ. (Fuente: DGAM).

Proyecto EDA - LAVOSAR II

Autor: Héctor Criado de Pastors, OT ENEP, SDG PLATIN.

Palabras clave: Arquitecturas abiertas, vetrónica, plataformas terrestres, estandarización, NGVA.

Metas Tecnológicas relacionadas: MT 3.3.3.

Los avances en las tecnologías de información están haciendo cada vez más sencillo el desarrollo de arquitecturas abiertas, con numerosas aplicaciones en el ámbito de defensa, desde sistemas de combatiente a infraestructuras, pasando por distintos tipos de plataforma. Estas arquitecturas permiten mejorar la efectividad de la misión y, al mismo tiempo, ahorrar costes de adquisición, mantenimiento o modernización de los sistemas. En el caso de plataformas terrestres, permiten mejorar la conciencia situacional y mejorar la eficiencia, velocidad y precisión de los efectos militares. Para lograr estos beneficios, así como mejorar las capacidades de la base tecnológica e industrial europea en este ámbito, es necesario desarrollar estándares comunes que sean relevantes en el entorno de defensa. De este modo, partiendo de una base común que incremente el número de elementos compatibles, se podrán desarrollar nuevos sistemas de misión o soluciones específicas para cada vehículo.

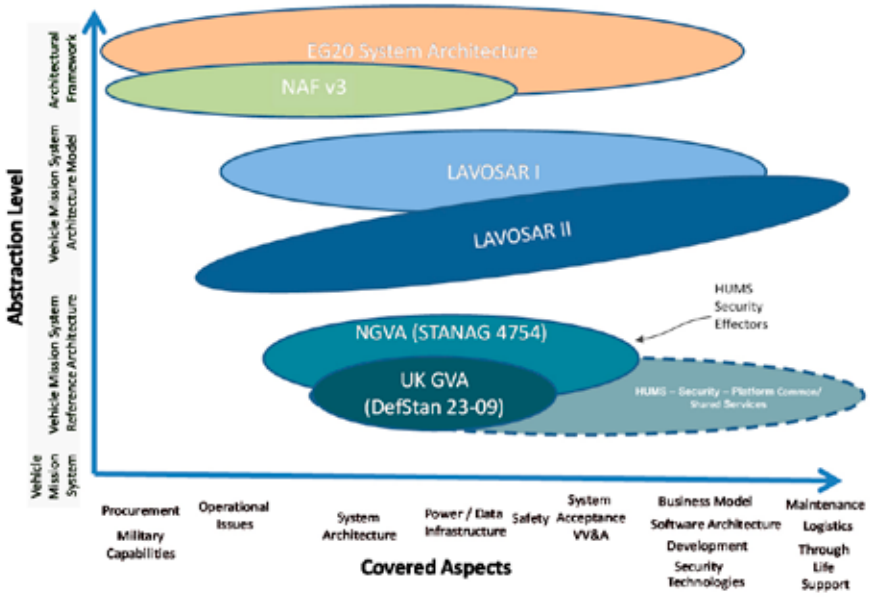

Fig. 1. Contexto de LAVOSAR Domain Context. (incl. planned UK GVA future extensions). (Fuente: EDA Lavosar II Public Executive Summary).

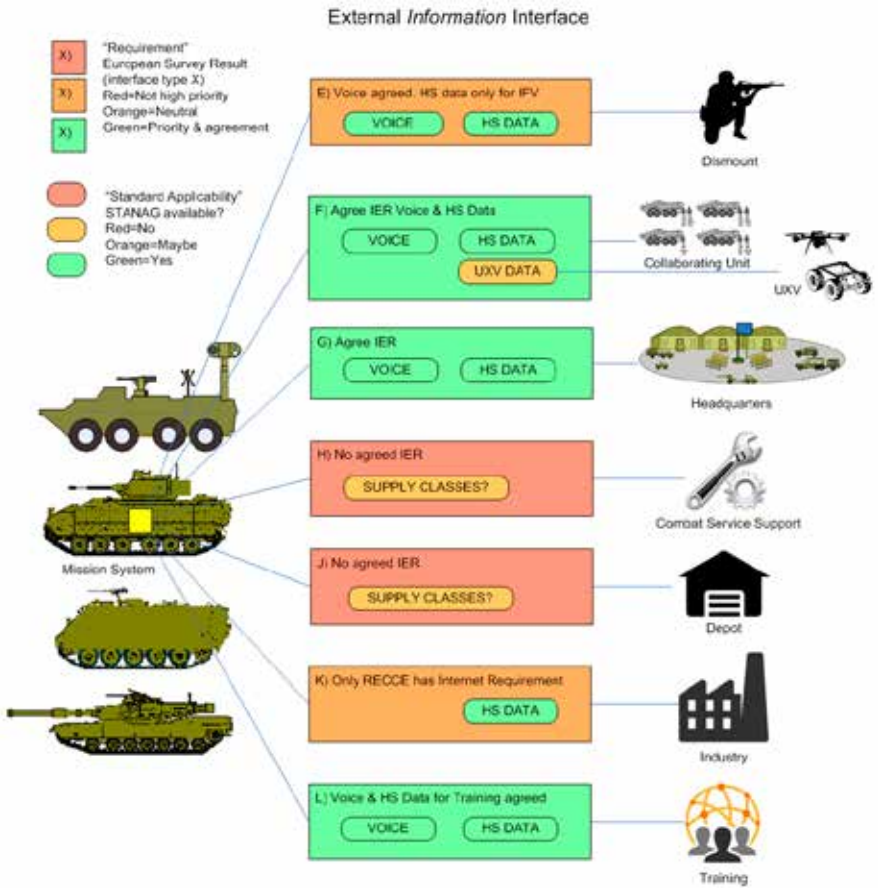

Fig. 2. Estatus de requisitos de intercambio de información y aplicabilidad de estándares en distintos tipos de plataformas terrestres. (Fuente: EDA Lavosar II Public Executive Summary).

Dentro de este ámbito de desarrollo, la EDA ha llevado a cabo el proyecto LAVOSAR II: Estándar europeo de referencia sobre arquitecturas abiertas para modernos sistemas de misión electrónicos integrados en vehículos militares terrestres. Este proyecto es continuación del LAVOSAR (*Land Vehicles with Open System Architecture* – Vehículos Terrestres con Arquitecturas Abiertas de Sistema), que fue tratado en el número 42 de este Boletín.

LAVOSAR II ha extendido la arquitectura propuesta en el primer proyecto, cubriendo algunos gaps existentes entre ésta y otras arquitecturas abiertas nacionales (UK DefStan 23-09, Victory, Scorpion) o de la OTAN (NGVA - NATO Generic Vehi-

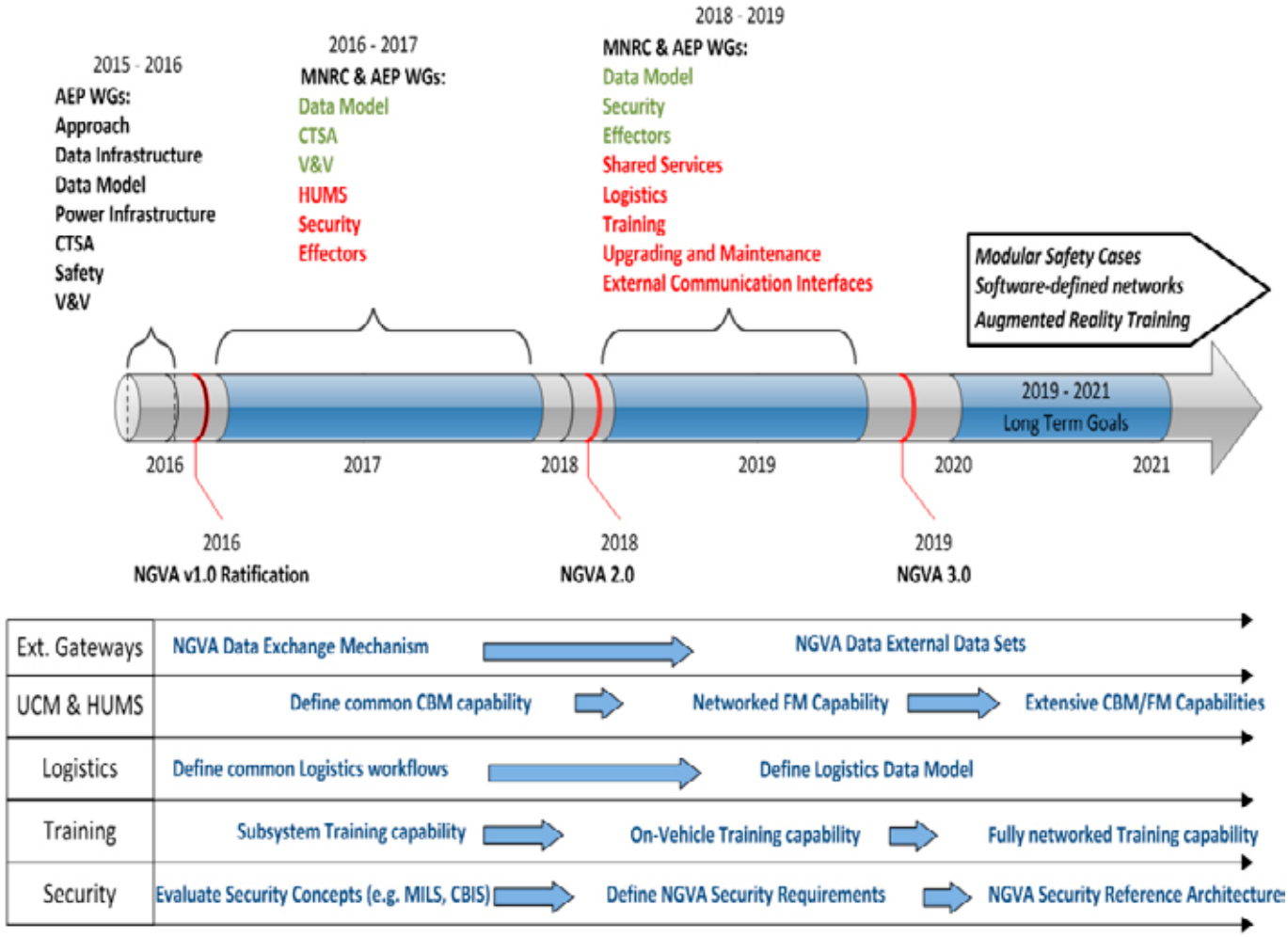

Fig. 3. Roadmap LAVOSAR vs NGAV. (Fuente: EDA Lavosar II Public Executive Summary).

cle Architecture), como se puede ver en la figura 1. Además, se ha realizado una actualización de los flujos de trabajo, componentes logísticos y estándares definidos en LAVOSAR I. La arquitectura LAVOSAR ha sido incluida en el repositorio de arquitecturas de la EDA.

Dentro de las tareas del proyecto, se realizaron sendos workshops gubernamentales y abiertos a la industria y se recopilaron requisitos de los países miembros para estudiar los ámbitos donde es más factible avanzar en el desarrollo de arquitecturas abiertas. Los resultados pueden verse en la figura 2.

Cabe destacar que el proyecto LAVOSAR II está contribuyendo al desarrollo y revisión de la NGVA (ver figura 3), avanzando la coordinación en áreas que aún no han sido integradas, como HUMS, integración de sensores y seguridad, así como otras que aún no han entrado en el proceso de estandarización OTAN, como la integración con plataformas no tripuladas, mantenimiento, logística o entrenamiento, entre otros. Se ha recomendado que, a corto plazo, se trabaje en la estandarización de:

- Radio data links
- Seguridad y comunicaciones inalámbricas seguras
- Logística
- Mantenimiento
- Entrenamiento, entrenamiento embebido y simulación
- Conformidad de verificación y validación
- Seguridad de sistemas
- Servicios comunes compartidos
- Interfaces en lenguaje natural para terminales de tripulación
- NATO Architectural Framework

A más largo plazo, otras áreas que actualmente se encuentran en desarrollo, serán susceptibles de ser integradas mediante arquitecturas abiertas, como redes definidas por software o realidad aumentada.

Foro Consultivo para la Energía Sostenible en el Sector de Defensa y Seguridad

Autor: Héctor Criado de Pastors, OT ENEP, SDG PLATIN.

Palabras clave: Comisión Europea, EDA, energía, eficiencia energética, energías renovables, infraestructuras.

Metas tecnológicas relacionadas: MT 3.1.5; MT 3.1.6; MT 3.2.3; MT 3.3.2; MT 3.4.2; MT 3.5.4; MT 4.1.2.

El Foro Consultivo para la Energía Sostenible en el Sector de Defensa y Seguridad es una iniciativa de la Comisión Europea gestionada por la EDA. Reúne a expertos de los sectores de defensa y de energía para compartir información sobre prácticas adecuadas para mejorar la gestión energética, la eficiencia y el uso de la energía renovable en usos considerados civiles. Participan todos los países miembros de la UE y Noruega. Está centrado en compartir buenas prácticas y conocimientos sobre la legislación europea sobre energía, en particular la Directiva de Eficiencia Energética, la Directiva de Eficiencia Energética en Edificios y la Directica de Energía Renovable para analizar la implementación de medidas en el sector de defensa que contribuyan a los esfuerzos actuales de descarbonización. El Foro será además un lugar donde se fomenten proyectos en áreas clave así como donde se identifiquen posibles líneas de financiación. En función de sus resultados, el Foro podría desarrollar recomendaciones para desarrollar directivas o modificar políticas sobre los mecanismos europeos de financiación para defensa.

El Foro Consultivo tendrá lugar en una serie de cinco reuniones plenarias durante dos años. El trabajo se llevará a cabo a través de tres grupos de trabajo paralelos, cada uno de ellos con centrados en un área:

- Grupo de trabajo 1: Gestión energética. Examinará los aspectos de gestión y de comportamiento relacionados con la eficiencia energética para determinar la aplicabilidad de análisis de datos, sistemas de gestión, concienciación y acceso a fuentes de financiación del sector de defensa en su enfoque sobre eficiencia energética. Una de sus tareas será examinar la protección de infraestructuras críticas energéticas para determinar si existe interés entre los participantes en desarrollar este tema desde una perspectiva militar.
- Grupo de trabajo 2: Eficiencia energética. Examinará la eficiencia energética desde el punto de vista de las infraestructuras, dado que la energía en edificios e infraestructuras fijas constituye una considerable parte de la energía consumida por las fuerzas armadas de los países de la UE en su conjunto. El grupo de trabajo también examinará la energía en campamentos en territorio de la UE y en despliegues internacionales liderados por la UE. El grupo también abordará la eficiencia energética en plataformas y sistemas militares para lograr reducir el consumo de energía y determinar dónde se pueden encaminar los esfuerzos para mejorar la eficiencia energética.
- Grupo de trabajo 3: Energía renovable. El grupo estudiará las fuentes de energía renovable, la producción de energía (eólica, solar, undimotriz, mareomotriz, biomasa, geotermia), el uso de terrenos militares para la generación de energía renovable, la conversión y almacenamiento de energía, el uso de energía en transporte y la aplicabilidad de energías renovables en transporte militar.

Fig. 1. Logotipo de la EDA. (Fuente: EDA).

Cabe destacar que el Foro promueve la participación de la base tecnológica e industrial, en especial de las pymes.

La primera reunión tuvo lugar los días 14 y 15 de enero en la sede de la EDA en Bruselas y participaron más de 80 expertos. Las próximas reuniones están previstas para junio y noviembre de este año. Toda la información sobre el Foro Consultivo puede encontrarse en el correspondiente portal específico de la EDA: European Defence Energy Network (http://eda.europa.eu/european-defence-energy-network).

Fig. 2. Inauguración del Foro Consultivo por parte del Comisario Europeo de Acción por el Clima Miguel Arias Cañete, el Director Ejecutivo de la EDA Jorge Domecq and el Director General de Energía de la Comisión Europea Dominique Ristori. (Fuente: EDA).

Evolución de los puertos militares ante la automatización de los sistemas de amarre

Autor: TN. Ing. Raúl Villa Caro, Inspector de buques del Arsenal de Ferrol (ICOFER).

Palabras clave: puerto, amarre, buque, automatización, accidente.

Líneas de actuación funcional relacionadas: LAF 3.4.

Introducción

Durante la estancia de un buque mercante atracado, una parte más que importante de sus gastos corresponden a los denominados «Costes de Carga y Descarga». Ese tiempo mínimo deseado para la estancia en puerto, está influenciado por los movimientos que experimenten los buques atracados. En el caso de los buques de guerra, este condicionante habitualmente no es tan importante, ya que los buques atracan en sus bases para otros motivos, pero no deja de tener importancia la posibilidad de poder realizar las operaciones de atraque y amarre, de una manera mucho más rápida, eficaz y segura.

Los tiempos en puerto de los buques mercantes, es decir, sus estadías, han sido poco estudiados en los tiempos actuales. Prácticamente no existe ninguna publicación moderna que haya analizado los tiempos que permanecen los buques en puerto. Una de las fuentes más fiables, pero ya antigua, es la representada en la tabla de la figura 1, en la que se pueden apreciar los valores típicos de viajes de distintos tipos de buques.

Tipo de buque	*Tamaño*	*Duración viaje (millas)*	*Escalas por viaje*	*% estancia en puerto*
Bulkcarrier grande	110.000 GT	10000	2	23
Bulkcarrier pequeño	25.000 GT	11000	4	31
Ro-Ro	90 remolques	800	2	33
Portacontenedores	2300 TEU	12000	6	29
Costero	3000 GT	1400	2	45

Fig. 1. Tiempos de estancia en puerto.
(Fuente: Buxton, Daggitt y King - Cargo Access Equipment for a Merchant Ship).

Evidentemente, en el caso de los buques de guerra, estos tiempos de estancia en puerto son totalmente diferentes y variables, ya que existen otro tipo de exigencias.

Sistema de amarre por vacío

Existen compañías especializadas en el diseño de amarre automatizado que están revolucionando los sistemas de amarre para buques civiles y militares. Estos sistemas de amarre, aún no implementados en nuestro país, han sido adoptados por importantes compañías portuarias, debido a su elevado tráfico, entre las que se encuentran algunas que operan en el Puerto de Dover. En 1999 se instaló por primera vez un sistema llamado «*IronSailor*» en un buque de pasaje. Después de su puesta en marcha este sistema se ha utilizado de forma segura en más de 10.000 operaciones de amarre automático sin amarras.

El sistema de amarre por vacío representa un hito importante, a pesar de que su implantación no exige instalaciones específicas en el barco y permitiría adhesión directa de las planchas del casco, de la mayoría de los buques civiles y militares, con los muelles. Este sistema, de cara al muelle, tiene la gran ventaja de su alojamiento retráctil, cuando no se encuentra en uso. Esto permite al sistema el poder permanecer detrás de la línea de defensas para resguardarse del impacto, durante el momento del acercamiento inicial del buque al muelle, durante el atraque. Cuando se activa el sistema, la estructura de soporte de la ventosa se extiende hacia el exterior y la conexión de amarre por vacío se establece en unos segundos. Este sistema está diseñado para apoyar a la mayoría de los buques y cuenta con varias características importantes entre las que se incluyen la actuación en tres grados de libertad, el posicionamiento de los buques, y el control mediante monitorización en tiempo real a través de redes informáticas y registro de los datos obtenidos.

Se podría decir que nos enfrentamos al desafío de un cambio radical ante el antiguo, tradicional y aceptado sistema de amarre con estachas. Automatizar el proceso de amarre representa un nuevo campo en la tecnología marítima. Se trata de un sector muy complejo y multidisciplinario, relacionado con el diseño de nuevos productos, por lo que se debe realizar un análisis en profundidad de las condiciones ambientales, las cargas, las formas de los cascos, los requisitos estructurales, las sociedades de clasificación, y las necesidades de los potenciales clientes.

Sistema de amarre hidráulico

La empresa «KRVE» ha desarrollado y probado un sistema sencillo de amarre en colaboración con la Autoridad Portuaria de Rotterdam. Ofrece una tensión permanente sin necesidad de energía externa constante. El sistema se denomina «*Shore-Tension*». Este sistema reduce el movimiento del buque provocado por el viento, la corriente o buques que pasen cercanos al buque atracado, y ha sido probado en España en el puerto de Ferrol, y probablemente a corto plazo se realice un encargo.

Shore-Tension funciona como un sistema de amarre hidráulico au-

tecnologías emergentes

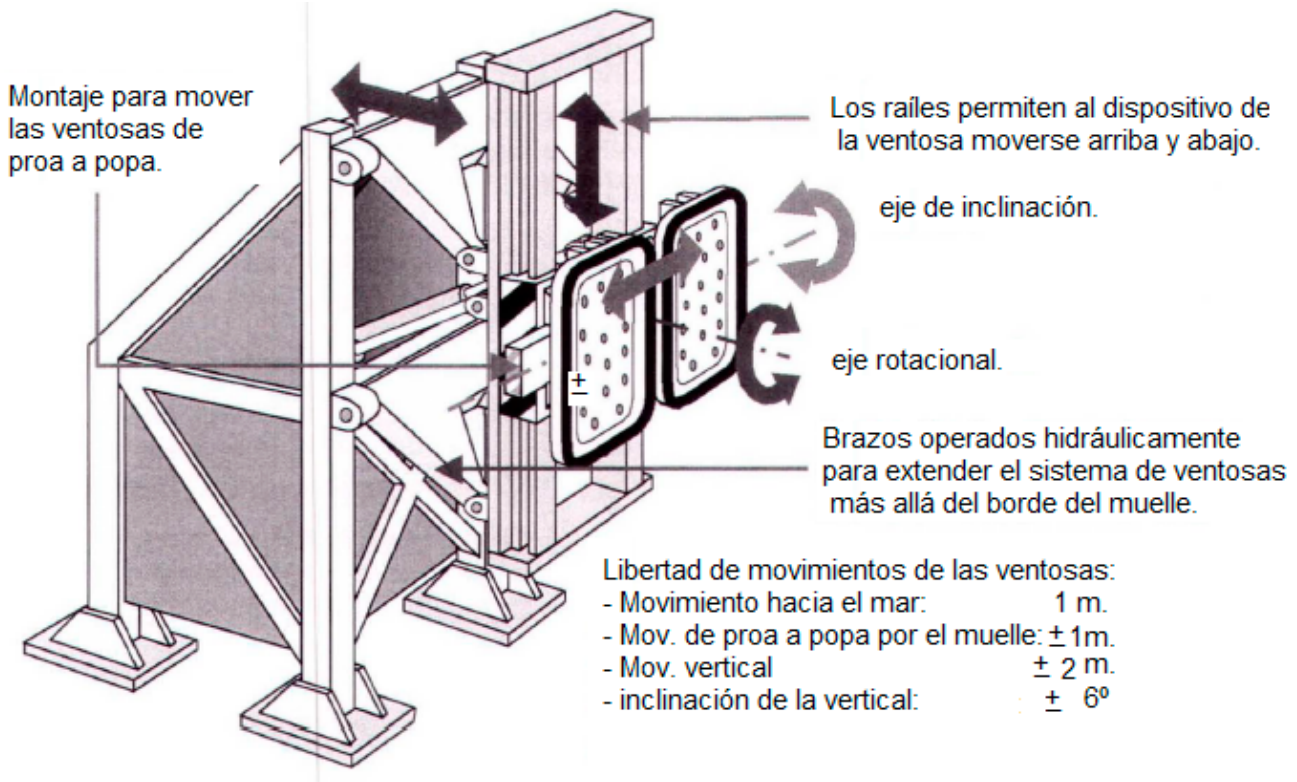

Fig. 2. Esquema dispositivo amarre por vacío. (Fuente: Mooring Equipment Guidelines (October 2008); Autor: OCIMF).

tomático. Unas válvulas de control aseguran que la tensión de la línea de amarre no supere la carga de seguridad de los cabos de amarre y norays del muelle. Gracias a esto, todas las líneas de amarre tendrán la misma tensión, lo cual mejorará el amarre.

Gracias al uso del nuevo sistema, evitaremos líneas de amarre adicionales. El sistema no elimina las estachas de amarre tradicional, pero las complementa y reduce el número de las mismas necesario. Recientemente se utilizó este dispositivo para auxiliar en el adrizamiento del buque Ro-Ro «Modern Express», barco que se encontraba a la deriva y que finalmente atracó en el puerto de Bilbao, con ayuda de remolcadores y con más de 50 grados de escora.

Ventajas del sistema de *ShoreTension*:

- Impide que las líneas de amarre rompan.
- Garantiza la seguridad del buque.
- Supone menos amarras, por lo que los accidentes deberían disminuir.
- Reduce el problema del mar de fondo en las dársenas.
- Compensa el problema de succión creado por los buques que pasan cerca.
- Aumenta la velocidad de carga y descarga.
- Es versátil y puede ser instalado sobre cualquier muelle.
- Puede suministrar una tensión constante.
- Tiene sensores que registran las tensiones en las estachas.
- Presenta datos que serán accesibles para la dotación del buque, y que además quedarán registrados

Fig. 3. Dispositivo de amarre por vacío. (Fuente: www.cavotec.es).

para su evaluación y posterior análisis.

- Está reconocido por la Sociedad de Clasificación LRS.

Evolución futura

Es probable que en un futuro no muy próximo, los puertos empiecen a dotarse de los equipos necesarios para el amarre sin estachas, mediante vacío. Hasta ese momento puede que se asienten los sistemas híbridos tipo «*shoretension*», que son una solución intermedia, y utilizan los sistemas hidráulicos y las estachas.

Aunque en muelles previstos para tráfico de buques portacontenedores, por ejemplo, tarden más en asentarse estos sistemas, de cara a aquellos puertos que alberguen tráfico de buques de pasaje de línea regular, los dispositivos de «amarre por vacío» seguro que se asientan con mayor celeridad. La apuesta por estos sistemas en los puertos militares, podría estar cerca. La US *Navy* ya lleva tiempo detrás de estos sistemas, y ya ha hecho pruebas para implementarlos en sus buques y muelles.

Junto con los mencionados en este artículo, existen otros sistemas novedosos de amarre, pero de todos ellos, los sistemas de amarre por vacío son los que dotan de mayor flexibilidad a las líneas convencionales, manteniendo una tracción horizontal uniforme en el casco del buque.

En los sistemas de vacío los sensores continuamente miden la carga en las ventosas mientras estas se encuentran sujetas al buque, por lo que el sistema puede ser monitorizado y operado en remoto. El modo en el que las ventosas están montadas en la unidad permite normalmente trincar y afirmar los buques en puertos y dársenas expuestos a gran oleaje.

Los remolcadores pueden ser usados para empujar el buque hacia el muelle, donde deben estar dispuestas al menos dos unidades separadas a lo largo del muelle. Los sellos de goma de las ventosas son entonces comprimidos contra el costado del buque por medio de cilindros hidráulicos mientras las válvulas entre el acumulador de baja presión y las ventosas se abren para producir la succión que asegure el buque a las ventosas. La aplicación del vacío a las ventosas invierte solo quince segundos. Los fabricantes pueden producir unidades que tengan una capacidad de 20 a 80 toneladas.

Las ventosas de vacío deben sujetar partes del buque que:

- Consistan en planchas casi planas cercanas a la parte paralela al muelle.
- Estén libres de hielo y no tengan protuberancias significativas.
- Sean suficientemente fuertes para soportar la fuerza de succión de las ventosas. Una diferencia de presión de unas 9 t/m2 doblaría las planchas a las que estén sujetas las ventosas, con lo que cualquier distorsión debe estar dentro de los límites elásticos de la plancha del casco.

Conclusiones

Los tiempos de estancia en puerto de los buques suponen un tanto por ciento muy importante de la vida operativa de los mismos, por lo que se debe estudiar la mejora de los sistemas de amarre que se utilizan en puerto, apostando por los sistemas de amarre por vacío.

Aunque los costes de instalación y mantenimiento de estos sistemas serán mucho mayores que los de los norays y bolardos a los que el sistema reemplaza, los puertos deberían ser capaces de recuperar esta inversión con la obtención de mayor efectividad en el uso de los muelles por medio de una mayor rotación de buques y por la menor necesidad de espacio entre buques a lo largo del muelle que este sistema permite. También se producirán menos paradas en el trabajo de carga y descarga debido a movimientos excesivos en puertos expuestos a oleaje. Sin embargo, como cualquier otro sistema de aseguramiento del buque, la capacidad del sistema tiene sus límites y los usuarios deben seguir las recomendaciones e instrucciones de los fabricantes.

Fig. 4. Sistema de amarre Shore Tension. (Fuente: www.shoretension.com)

El futuro del grafeno (IV): fotónica, optrónica y sensores químicos y biosensores

Autor: Pedro Carda Barrio, OT OPTR, SDG PLATIN.

Palabras clave: grafeno, fotónica, optrónica, sensores químicos, biosensores, láser, terahercios, defensa y seguridad.

Metas Tecnológicas relacionadas: MT 2.3.1; MT 5.2.1.

Introducción

El grafeno tiene la capacidad de absorber energía de manera independiente a la longitud de onda de la radiación incidente en un material. Gracias a ello, podría sustituir en un futuro a múltiples materiales que se utilizan actualmente en dispositivos optrónicos y nanofotónicos. Mediante un dopaje electrostático (proceso de agregar impurezas en un material puro con el objetivo de modificar sus propiedades), se podrían conseguir propiedades ópticas sintonizables en función de la longitud de onda, así como el almacenamiento de altas cantidades de energía electromagnética en pequeños volúmenes, por lo que, ciertas prestaciones de los dispositivos optrónicos y nanofotónicos actuales podrían mejorar enormemente.

Como consecuencia de lo descrito anteriormente, es perfectamente posible imaginar cambios relevantes en la integración de los dispositivos optoelectrónicos que impliquen mejoras muy importantes en la sensibilidad y en la velocidad de detección de los sensores de visión en los rangos visible e infrarrojo, en nuevos dispositivos que trabajen en el rango de los terahercios, láseres y metamateriales sintonizables, circuitos y dispositivos nano-optoelectrónicos, fibras ópticas, sensores químicos, biosensores, etc.

Todo ello podría suponer un cambio disruptivo en el sector de las telecomunicaciones y en el mercado de los sensores en los rangos visible, infrarrojos y terahercios.

Fotodetección: detección en los rangos visible, infrarrojos y visión nocturna

El grafeno tiene unas propiedades fotosensibles muy particulares al ser capaz de detectar la radiación incidente en todo el espectro visible, infrarrojo y ultravioleta de manera simultánea, por lo que se investiga la posibilidad de incorporarlo en múltiples fotodetectores que trabajen en dicho espectro.

Actualmente, la mayoría de los detectores que trabajan en el rango visible no necesitan ser refrigerados. Respecto de los detectores que trabajan en los diferentes rangos del infrarrojo, pueden necesitar o no refrigeración, dependiendo principalmente del rango del infrarrojo. Por ejemplo, entre 3 y 5 µm sí suelen necesitar refrigeración mientras que entre 8 y 12 µm no suele ser necesario. La refrigeración hace posible el uso de detectores de una alta sensibilidad térmica, pero supone un problema en cuanto al aumento de peso, volumen y consumo eléctrico de los sistemas, además de producir vibraciones.

En el caso de futuros detectores fabricados con grafeno, la detección sería simultánea en todo el espectro (visible + todas las bandas de infrarrojos), y no sería necesaria la refrigeración, lo que implicaría una mejora en la capacidad de detección, y disminuiría el peso, volumen y consumo energético de los equipos actuales para aplicaciones tan diversas como vigilancia, visión nocturna, sanitarias, detección de averías eléctricas y fugas de gases, etc.

Otro ámbito en el que el grafeno podría resultar de gran interés sería en el de las fibras ópticas, cuya principal limitación en cuanto a su capacidad actual viene dada por los receptores que convierten las señales ópticas en eléctricas y viceversa. Mediante fotodetectores de alta velocidad basados en grafeno, se podrían crear nuevas conexiones de fibra óptica con mayor capacidad de transmisión de datos y mucho más rápidas.

No obstante, hay que tener en cuenta que todavía existen importantes retos tecnológicos a resolver. El grafeno absorbe un porcentaje muy bajo de la radiación incidente (inferior al 3%), con lo que resulta difícil generar las corrientes eléctricas que son necesarias para la fabricación de los fotodetectores.

Láser

El grafeno podría ser utilizado para la creación de nuevos láseres de pulsos ultracortos de femtosegundos (1fs = 10^{-15} s), de diferentes longitudes de

Fig. 1: Imagen de visión nocturna de un AV-8B Harrier norteamericano. (Fuente: Wikipedia).

onda, gracias a su capacidad de absorción de la luz.

Por otro lado, los láseres actuales se fabrican con materiales que sólo son capaces de absorber la luz en longitudes de onda específicas, mientras que los futuros láseres basados en grafeno serían sintonizables en múltiples longitudes de onda. Esto implica que con este tipo de láser se podrían cubrir un número mayor de aplicaciones como la detección y seguimiento de partículas tóxicas o contaminantes.

Dispositivos de detección en el rango de terahercios

Otra de las múltiples propiedades del grafeno es su capacidad de amplificación de la radiación electromagnética en el rango de los terahercios (longitud de onda entre 0,1 y 1 mm), por lo que se está investigando la posibilidad de crear nuevos dispositivos de detección en dicho rango.

Los sistemas basados en ondas de terahercios tienen sus principales aplicaciones en la detección de explosivos (basados en la identificación de los componentes químicos del explosivo) y en los escáneres de personas para la detección de armas y explosivos ocultos, con lo que son de un alto interés en seguridad y defensa.

Sensores químicos y biosensores

El grafeno es conocido por su ligereza, dureza, flexibilidad y capacidad de detección, además de por su elevada conductividad eléctrica y térmica. Estas propiedades son de gran importancia en los materiales que se utilizan en los detectores de sustancias químicas y biológicas, por lo que se está considerando la posibilidad de incorporar el grafeno en las futuras generaciones de detectores.

Los sensores químicos y los biosensores transforman la información de las sustancias detectadas en energía eléctrica mediante un transductor, y posteriormente, en una señal medible con un sistema electrónico. Actualmente se fabrican sensores químicos y biosensores con una superficie de óxido de grafeno de alta sensibilidad para la detección de células cancerígenas, bacterias o virus, ya que este material tiene una alta capacidad de absorción de dichas sustancias. Además, los sensores químicos y biosensores basados en grafeno tendrían un bajo ruido eléctrico, lo que haría mejorar la relación señal/ruido.

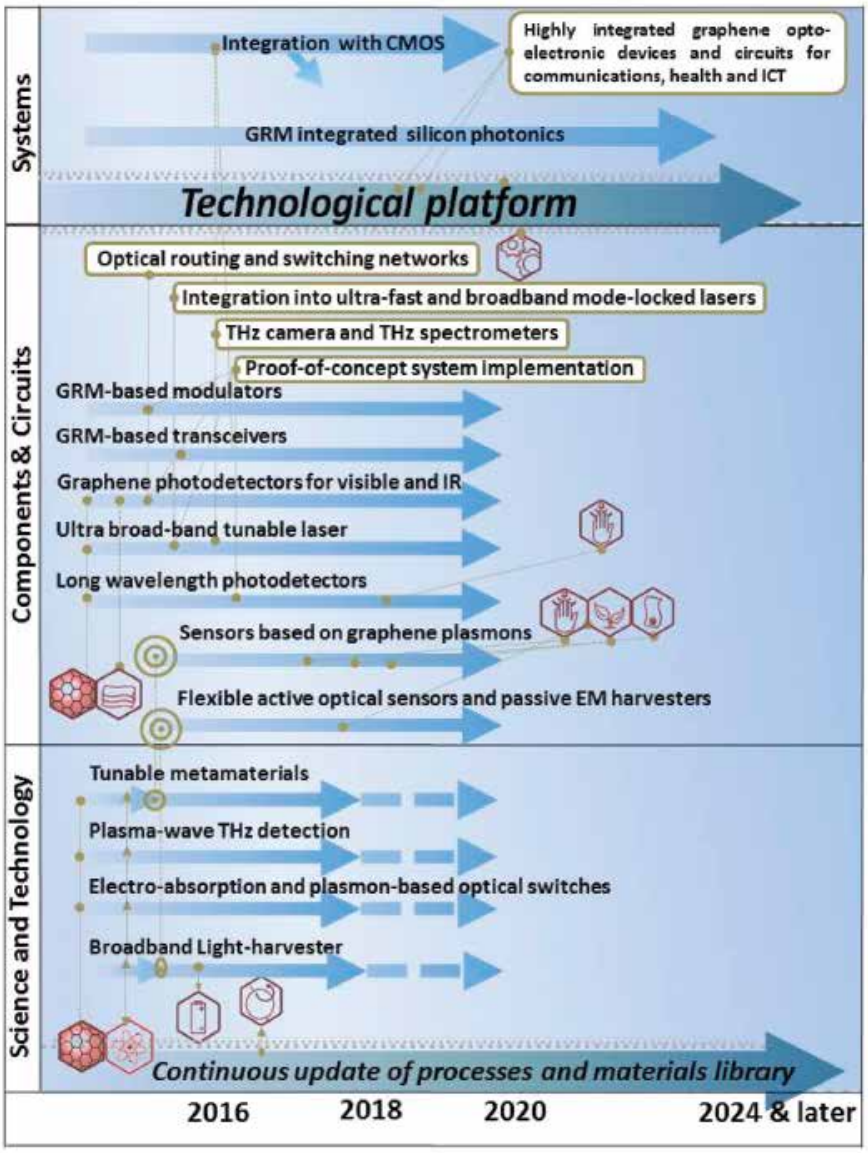

Fig. 2: Hoja de ruta fotónica y optrónica 2016-2024. (Fuente: Nanoscale 2015).

Conclusiones

Dentro de las investigaciones que se están llevando a cabo para el uso del grafeno en los campos de la fotónica, optrónica y sensores químicos y biosensores, existen múltiples posibles aplicaciones en defensa y seguridad, como la mejora de los equipos actuales de visión nocturna, nuevos designadores láser para objetivos militares, sistemas de detección de explosivos y armas ocultas en el rango de los terahercios o detección de sustancias químicas y biológicas mediante nuevos sensores.

La comunidad científica estima que al ritmo del desarrollo actual podríamos encontrar en el mercado alguno de estos nuevos dispositivos en un periodo no superior a cinco años.

Referencias

[1]. Ministerio de Defensa. Monografías del SOPT (Sistema de Observación y Prospectiva Tecnológica) (2013).

[2]. Royal Society of Chemistry. Nanoscale (2015). Recuperado el 21 de marzo de 2015 de http://www.rsc.org/nanoscale.

El problema de la seguridad del software

Autor: Cte. Javier Bermejo Higuera, Responsable de la Unidad de Ingeniería y Seguridad del CESTIC, MINISDEF; Cap. Juan Ramón Bermejo Higuera, Investigador seguridad TIC, INTA.

Palabras clave: *software, security, abuse case, static analysis, dynamic analysis, risk analysis, security requirement, attack pattern, review, SDLC, risk based tests*.

Metas tecnológicas relacionadas: MT 6.5.1; MT 6.5.2.

Introducción

Hoy en día, los ataques cibernéticos son cada vez más frecuentes, están más organizados y resultan más costosos por el daño que infligen a las administraciones públicas, empresas privadas, redes de transporte, redes de suministro y otras infraestructuras críticas desde la energía a las finanzas, hasta el punto de poder llegar a ser una amenaza a la prosperidad, la seguridad y la estabilidad de un país.

En la figura 1 se puede observar un gráfico cualitativo en el que se muestran diversos incidentes ocurridos a lo largo de los últimos quince años en relación con su nivel de complejidad. Como se aprecia, la amenaza es creciente con los años y cada vez su nivel de complejidad es más elevado.

La sociedad actual está cada vez más vinculada al ciberespacio. Un elemento importante del mismo lo constituyen el software o las aplicaciones que proporcionan los servicios, utilidades y funcionalidades. Sin embargo estas aplicaciones presentan defectos, vulnerabilidades o configuraciones inseguras que pueden ser explotadas por atacantes de diversa índole, desde aficionados hasta organizaciones de cibercrimen o incluso estados en acciones de ciberguerra, utilizándolas como plataformas de ataque comprometiendo los sistemas y redes de la organización.

La cada vez más consolidada introducción de dispositivos móviles no ha hecho más que multiplicar el número de elementos, incrementando enormemente la superficie de vulnerabilidad con multitud de aplicaciones que la gente se baja sin demasiadas precauciones y sin una conciencia de la seguridad muy sólida, elevando exponencialmente los riesgos debido a la conectividad global.

El problema de la peguridad del poftware

Nadie quiere software defectuoso e inseguro, especialmente los desarrolladores cuyo código desarrollado contiene vulnerabilidades derivadas de errores cometidos y desconocimiento de prácticas de seguridad, pero la realidad desborda con creces los mejores deseos. Las vulnerabilidades vienen derivadas de una serie de causas posibles que hacen que el software resulte inseguro como se pone de manifiesto en el informe de *Klocwork* [3]:

- Tamaño excesivo y complejidad de las aplicaciones.
- Mezcla de código proveniente de varios orígenes como compras a otra compañía y reutilización de otros existentes, lo que puede producir comportamientos e interacciones no esperados de los componentes del software.
- Defectuosa integración de los componentes del software, estableciendo relaciones de confianza inadecuadas entre ellos, etc.
- Debilidades y fallos en la especificación de requisitos y diseño no basados en valoraciones de riesgo y amenazas.
- Uso de entornos de ejecución con componentes que contienen vulnerabilidades o código malicioso embebido, como pueden ser capas de middleware, sistema operativo u otros componentes COTS.
- No ejecución de pruebas de seguridad basadas en riesgo.
- Falta de las herramientas y un entorno de pruebas apropiado que simule adecuadamente el entorno real de ejecución.
- Cambios de requisitos del proyecto durante la etapa de codificación.
- Mezcla de equipos de desarrolladores, entre los que pueden haber equipos propios de desarrollos, asistencias técnicas, entidades subcontratadas, etc.
- Falta de conocimiento de prácticas de programación segura de los desarrolladores en el uso de lenguajes de programación propensos a cometer errores como C y C++ y utilización de herramientas de desarrollo inadecuadas.
- No controlar la cadena de suministro del software, lo cual puede dar lugar a la introducción de código malicioso en origen.
- No seguir, por parte de los desarrolladores, las guías normalizadas

Fig. 1. Incidentes de seguridad. (Fuente propia).

de estilo en la codificación.

- Establecimiento de fechas límite de entrega de proyectos inamovibles.
- Cambios en la codificación en base a petición de nuevas funcionalidades.
- Tolerancia a los defectos.
- No tener actualizadas las aplicaciones en producción con los parches correspondientes, configuraciones erróneas, etc.
- Por otro lado, el problema alcanza mayores dimensiones cuando las aplicaciones son amenazadas y atacadas, no solo en su fase de operación, sino también en el resto de fases de su ciclo de vida [2]:
- Desarrollo. Un desarrollador puede alterar, de forma intencionada o no, el software bajo desarrollo comprometiendo su fiabilidad futura durante la fase de operación.
- Distribución e instalación. Ocurre cuando no se protege el software evitando que se manipule antes de ser enviado o publicado. Del mismo modo, si el instalador del software no bastiona la plataforma en la que lo instala o la configura de forma insegura, queda vulnerable a merced de los atacantes.
- Operación. Cualquier software que se ejecuta en una plataforma conectada a la red tiene sus vulnerabilidades expuestas durante su funcionamiento. El nivel de exposición variará dependiendo de si la red es privada o pública, conectada o no a Internet, y si el entorno de ejecución del software ha sido configurado para minimizar sus vulnerabilidades.
- Mantenimiento o sostenimiento. Puede producirse debido a no publicar los parches de las vulnerabilidades detectadas en el momento oportuno o incluso por introducir código malicioso por parte del personal de mantenimiento en las versiones actualizadas del código.

Según el informe «*2011 Top Cyber Security Risks Report*» [1], las vulnerabilidades detectadas en aplicaciones alcanzaron su punto máximo en el año 2006 iniciando a partir de ese año un lento declive (ver figura 2).

Esta disminución de vulnerabilidades

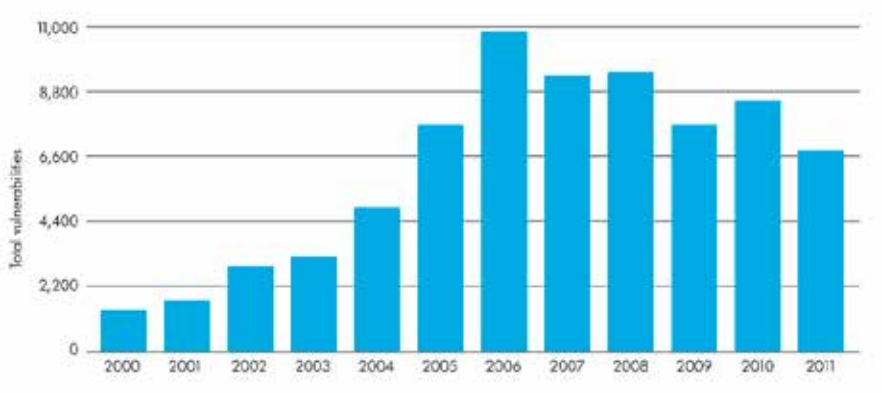

Fig. 2. Vulnerabilidades descubiertas por OSVDB, 2000 - 2011. (Fuente: Referencia [3]).

detectadas no significa que el software sea cada vez más seguro. Es una sensación de seguridad falsa, pues el número de vulnerabilidades de alta severidad está creciendo a un ritmo más rápido que los otros niveles de vulnerabilidad (CVSS[1] 8 a 10, clasificación definida en la OSVDB[2]). En la figura 3 se refleja cómo el porcentaje de vulnerabilidades de alta severidad se ha incrementado en los últimos diez años.

Las vulnerabilidades de alta severidad dan lugar a que un atacante pueda explotarlas rápidamente y hacerse con el control total del sistema. Su explotación requiere un conocimiento poco especializado de la aplicación al alcance, no solo de organizaciones cibercriminales, sino de cualquiera con conocimientos de informática.

En el informe «*HP Security Research*» del año 2015 [6], se publicó un gráfico que mostraba las vulnerabilidades descubiertas durante el año 2014 (figura 4). En él se indicaba que la aplicación más explotada fue Internet Explorer debido a la vulnerabilidad CVE-2014-0322 del tipo *use after free*, que básicamente consiste en el uso de un espacio de memoria después de liberarla, haciendo uso de Adobe Flash para saltarse las defensas contra este tipo de amenazas, que implementan los sistemas operativos del tipo Windows para entregar su carga útil ejecutable final. El *exploit* fue visto por primera vez en la Operación *SnowMan*, dirigida a entidades del gobierno de Estados Unidos y sus compañías de defensa.

Tal y como se ha mencionado, ciertos aspectos son especialmente críticos a la hora de identificar las vulnerabilidades más frecuentes: su complejidad, su extensión en líneas de código y el nivel de exposición a los ataques. Estos factores son los que a fin de cuentas determinan que sean las aplicaciones web las que tienen más probabilidades de ser atacadas y, por tanto, presenten el mayor número de vulnerabilidades conocidas.

Además erróneamente, a pesar de que los datos podrían convencer de lo contrario, se sigue confiando en que la implantación de tecnologías y dispositivos de seguridad de red como cortafuegos, sistemas de gestión y correlación de eventos (SIEM), sistemas de detección de intrusos, sistemas de gestión de acceso y cifrado del tráfico, etc., son medidas suficientes para proteger los sistemas de la organización. Sin embargo, los atacantes continúan intentando descubrir nuevos fallos en el software relacionados con la seguridad del sistema que den lugar a una vulnerabilidad con un gran impacto y riesgo asociado para la entidad propietaria.

El aumento de los ataques al software vulnerable ha dejado patente la insuficiencia de las protecciones a nivel de infraestructura. En este contexto es conveniente minimizar los ataques en la capa de aplicación y, por tanto, el número de vulnerabilidades explotables. Por todo ello se considera necesario que las diferentes organizacio-

[1] Common Vulnerability Scoring System (CVSS). Es un sistema que categoriza la severidad de una vulnerabilidad, de manera estricta a través de fórmulas, proporcionando un estándar para comunicar las características y el impacto de una vulnerabilidad en el software

[2] Vulnerability information from the Open Source Vulnerability Database (OSVDB). http://osvdb.org/search/advsearch

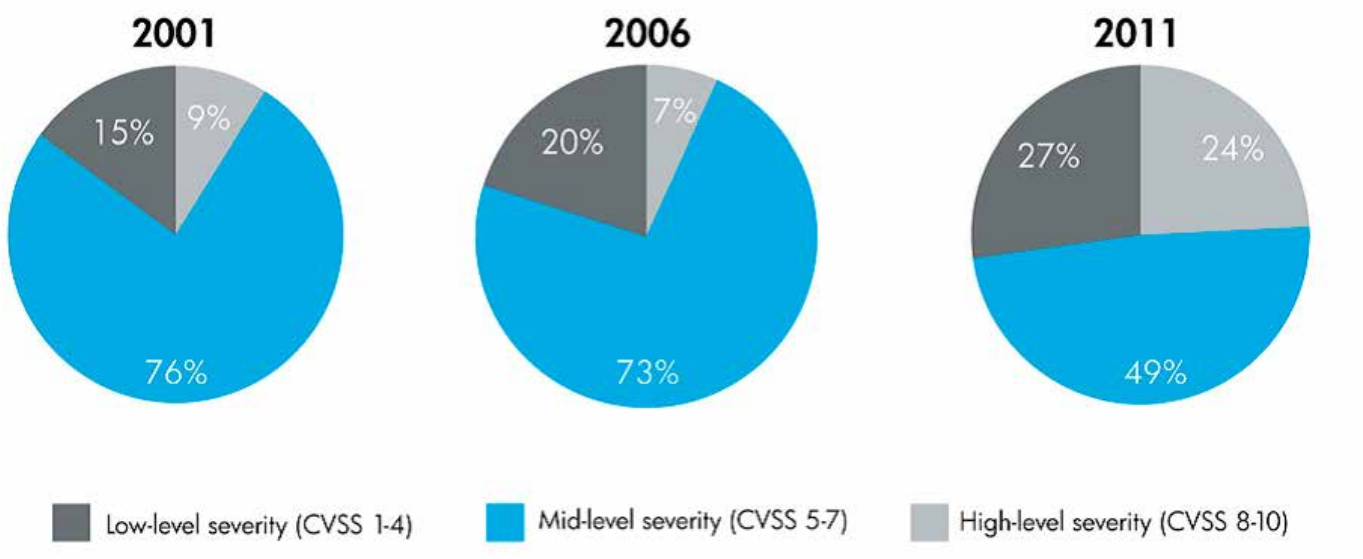

Fig. 3. Gravedad de las vulnerabilidades OSVDB en 10 años. (Fuente: Referencia [3]).

nes públicas o privadas dispongan de software fiable y resistente a los ataques, es decir de confianza, con un mínimo número de vulnerabilidades explotables.

Concepto de seguridad del software

Como respuesta a la problemática expuesta anteriormente surge el concepto de Seguridad del Software, que en el documento de referencia [4] de *SAFECode* se define como: «La confianza de que el software, hardware y servicios estén libres de vulnerabilidades intencionadas o no intencionadas y que, por lo tanto, funcionen conforme a lo especificado y deseado».

El Departamento de Defensa de los Estados Unidos (DoD) [7] lo define como «El nivel de confianza de que el software funciona según lo previsto y está libre de vulnerabilidades, ya sea intencionada o no, diseñada o insertada en el marco del software».

En definitiva, sobre la base de las definiciones anteriores y los antecedentes señalados, se puede definir la seguridad del software como: *El conjunto de principios de diseño y buenas prácticas a implantar en el SDLC (System Design Life Cycle), para detectar, prevenir y corregir los defectos de seguridad en el desarrollo y adquisición de aplicaciones, de forma que se obtenga software de confianza y robusto frente ataques maliciosos, que realice solo las funciones para las que fue diseñado, que esté libre de vulnerabilidades, ya sean intencionalmente diseñadas o accidentalmente insertadas durante su ciclo de vida y se asegure su integridad, disponibilidad y confidencialidad.*

Hasta principios de la década anterior, la mayoría de las aplicaciones se desarrollaban sin tener en cuenta requisitos y pruebas de seguridad específicos. Los desarrolladores de software no eran conscientes de las vulnerabilidades que se pueden crear al programar y descuidaban los aspectos de seguridad, dando prioridad al cumplimiento de las especificaciones funcionales, sin tener en cuenta casos en los que el software fuera maliciosamente atacado. Este proceso de desarrollo de software ofrece, aparte de los errores no intencionados producidos al codificar anteriormente referidos, oportunidades de insertar código malicioso en el software en origen.

Como se ha comentado anteriormente las tecnologías de seguridad en la red pueden ayudar a aliviar los ataques, pero no resuelven el problema de la seguridad real, ya que una vez que el ciberatacante consigue vencer esas defensas, por ingeniería social por ejemplo, y comprometer una máquina del interior, a través de la misma podrá atacar a otras de la misma red («*pivoting*») empezando por las más vulnerables. Éste es el caso de las Amenazas Avanzadas Persistentes (APT) uno de los ciberataques más peligrosos y dañinos hoy en día. Se hace necesario, por tanto, disponer de software seguro que funcione en un entorno agresivo y malicioso.

Un aspecto importante de la seguridad del software es la confianza y garantía de funcionamiento conforme a su especificación y diseño y que es lo suficientemente robusto para repeler las amenazas que puedan comprometer su funcionamiento esperado en su entorno de operación. Para conseguir lo anterior y minimizar al máximo los ataques en la capa de aplicación y, por tanto, el número de vulnerabilidades explotables, es necesario incluir la seguridad desde el inicio del ciclo de vida de desarrollo del software (SDLC). En este sentido es importante el aprovechamiento de las buenas prácticas de ingeniería de software ya existentes.

El desarrollo de software seguro y confiable requiere la adopción de un proceso sistemático o disciplina que aborde la seguridad en cada una de las fases de su ciclo de vida e integre actividades de seguridad como el seguimiento de unos principios de diseño seguro (mínimo privilegio, etc.) y la inclusión de una serie de buenas prácticas de seguridad (especificación requisitos seguridad, casos de abuso, análisis de riesgo, análisis de código, pruebas de penetración dinámicas, etc.). A este nuevo ciclo de vida con prácticas de seguridad incluidas se le denominará *Secure - Software Development Life Cycle* (S-SDLC).

Un beneficio importante que se obtendría de incluir un proceso sistemático que aborde la seguridad desde las etapas tempranas del SDLC, sería

la reducción de los costes de corrección de errores y vulnerabilidades, pues éstos son más altos conforme más tarde son detectados. Acorde a lo publicado por NIST (*National Institute of Standards and Technology*) en la figura 5, el coste que tiene la corrección de código o vulnerabilidades, después de la publicación de una versión mediante la publicación de un parche, es hasta treinta veces mayor que su detección y corrección en etapas tempranas del desarrollo.

Seguridad del software versus aseguramiento de la calidad

Antes de comenzar con las actividades y medidas de seguridad a integrar en el SDLC, es conveniente aclarar las principales diferencias entre aseguramiento de la calidad y seguridad del software:

- El aseguramiento de la calidad tiene como principal objetivo hacer que el software funcione correctamente conforme a las especificaciones del mismo.
- La seguridad del software se refiere a que tanto el software como su entorno de ejecución presenten el mínimo número de vulnerabilidades y, por tanto, su superficie de ataque sea la menor posible, de forma que sea confiable a pesar de la presencia de un ambiente externo hostil con ciberataques en curso.

Estas diferencias se pueden caracterizar también en términos de amenazas. Las principales que afectan a la calidad son internas no intencionadas debidas a errores o descuidos. Es decir, la presencia de defectos en el software que pongan en peligro su capacidad de funcionar correctamente y de manera previsible.

Por otro lado, las amenazas a la seguridad pueden ser internas y externas e incluyen una intención maliciosa materializada en posibles ciberataques que puedan recibir el software o su entorno de ejecución cuando se tiene un comportamiento impredecible por cualquier razón.

En un proceso de desarrollo de software seguro, los profesionales de control de calidad deben tener siempre en cuenta la seguridad y ser exactos y rigurosos en las especificaciones, diseño y verificación de la seguridad del software, sobre la base de los riesgos estimados, de forma que el proceso de garantía de calidad incorpore algunas actividades de su gestión y nuevos procedimientos relacionados con la seguridad.

Mejores prácticas de seguridad del software

Aun así, la seguridad del software es algo más que la eliminación de las vulnerabilidades y la realización de pruebas de penetración. Como ya ha sido citado, un aspecto adicional a considerar es la adopción por los gerentes de un enfoque sistemático para incorporar principios de buenas prácticas de Seguridad del Software («*touchpoints*») en todo el Ciclo de Vida de Desarrollo de Software, para lograr de este modo el doble objetivo de producir sistemas con software más seguro y poder verificar su seguridad. De esta forma se estará adoptando un ciclo de vida del software seguro S-SDLC.

La figura 6, propone un ciclo de vida de desarrollo de software SDLC en cascada basado en el modelo de McGraw [5]. Para otros tipos como los iterativos sería similar, especificando las actividades y pruebas de seguridad a efectuar en cada fase del mismo.

En el siguiente apartado se muestran diferentes tipos de S-SDLC adoptados por diferentes empresas y organizaciones. A este respecto, se enumeran esas actividades o mejores prácticas de Seguridad del Software tomando como referencia las definidas por Gay Mcgraw en *Software Security: Building Security In* [5] añadiendo otras:

- Modelado de ataques. Para conseguir que el desarrollo de una aplicación posea las propiedades y principios de diseño del software seguro presentadas, es necesario que el personal de diseño y desarrollo implemente la perspectiva del atacante modelada de las siguientes dos formas: Patrones de ataque y Árboles de ataque. Los «patrones de ataque» constituyen un mecanismo o medio para capturar y representar la perspectiva y conocimiento del ciberatacante con el suficiente detalle acerca de cómo

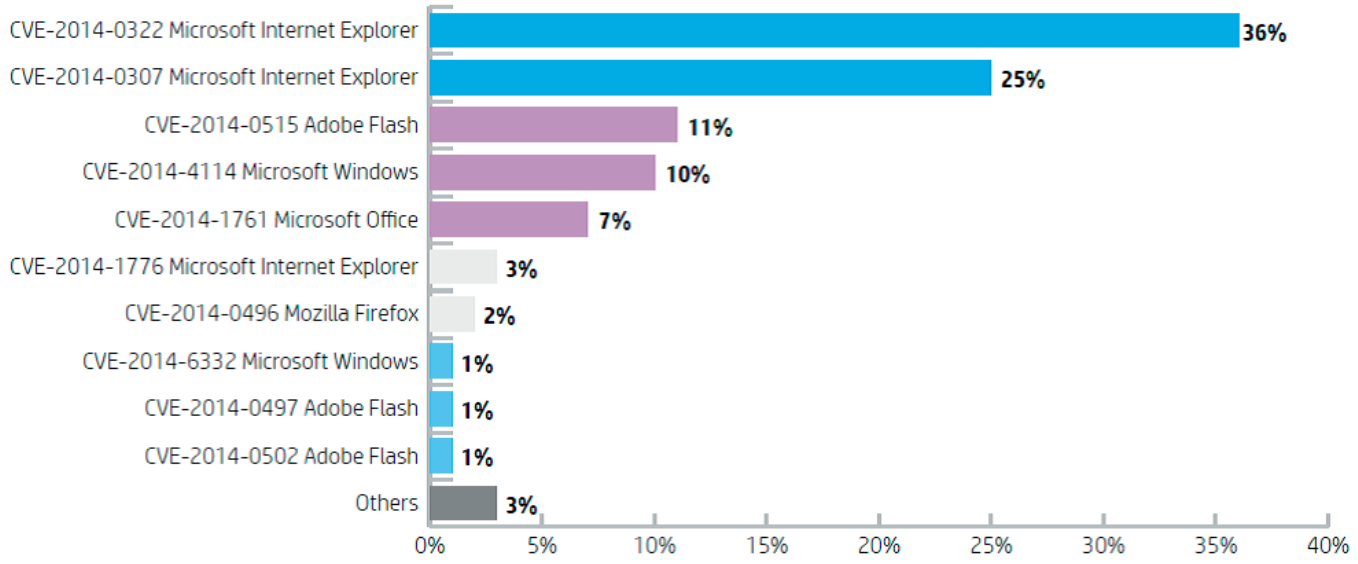

Fig. 4. Vulnerabilidades descubiertas en el año 2014. (Fuente: Referencia [6]).

los ataques se llevan a cabo y los métodos más frecuentes de explotación («*exploit*») y técnicas usadas para comprometer el software. Los «árboles de ataque» son una técnica para modelar las diferentes formas que puede utilizar un atacante para alcanzar un objetivo.

- Casos de abuso. Constituyen otra forma de representar la mentalidad del atacante en base a la descripción del comportamiento del sistema bajo un ataque. El diseño de casos de abuso requiere una cobertura explícita de lo que debería ser protegido, de quién y por cuánto tiempo.
- Ingeniería requisitos de seguridad. La seguridad de un sistema y el software que lo soporta debe especificarse en base a unos requisitos de obligada implementación y trazabilidad durante todas las fases del diseño. Estos requisitos pueden ser extraídos del análisis de riesgo realizado, los casos de uso y los casos de abuso.
- Análisis de riesgo arquitectónico. Es una necesidad en la etapa de arquitectura y diseño, la realización de un análisis del riesgo arquitectónico que documente los posibles riesgos de la arquitectura y diseño e identifique las posibles amenazas.
- Patrones de diseño. Son soluciones generales repetibles a un problema de ingeniería de software recurrente, destinadas a obtener un software menos vulnerable y un diseño más resistente y tolerante a los ataques, normalmente se limitan a funciones y controles de seguridad a nivel del sistema, comunicaciones e información.
- Pruebas de seguridad basadas en riesgo. Consiste en el planeamiento y realización de pruebas de verificación y validación de los diferentes componentes y del sistema completo en base al conocimiento de la arquitectura del software, los resultados del análisis del riesgo, los casos de abuso y los patrones de ataque como forma de estudiar la mentalidad del atacante, al objeto de comprobar el estado de seguridad y la no ocurrencia de funcionamientos incorrectos.
- Revisión de código. La revisión de código es una de las actividades de seguridad más importantes a realizar durante el S-SDLC, pues puede descubrir alrededor del 55% de los problemas de la seguridad. Las herramientas estáticas de análisis de código fuente pueden descubrir fallos de implementación y vulnerabilidades comunes. Sin embargo, aunque es una práctica muy habitual e importante no es suficiente pues, por ejemplo, los problemas arquitectónicos son muy difíciles e incluso imposibles de encontrar revisando solamente el código, sobre todo los que tienen cientos de miles de líneas. Lo anterior implica que el combinar la revisión del código y análisis de riesgos arquitectónico aumenta en gran medida la seguridad del software.
- Test penetración. Son pruebas cuyo principal objetivo es obtener una idea de cómo se comporta el software en su entorno de ejecución final, siempre que se realicen en un entorno que simule perfectamente el entorno de producción donde la aplicación o sistema prestará sus servicios y en el que el software presente su arquitectura definitiva. Son extremadamente útiles especialmente si se precede de un análisis de riesgo arquitectónico y de un plan de pruebas basadas en riesgo. Un fallo en este tipo de pruebas, realizadas con herramientas de prueba dinámicas de seguridad en tiempo de ejecución, significa que el sistema o el software es deficiente.
- Operaciones de Seguridad. Un principio de diseño importante para la seguridad es la «defensa en profundidad», el sistema hay que protegerlo como un todo. Por un lado hay que minimizar al máximo sus vulnerabilidades y diseñarlo de forma resistente para que sea de confianza y por otro hay que securizar su entorno de ejecución y de red al objeto de que la vía de ataque al mismo se deba a su interacción con el software de base (sistema operativo, gestores de base de datos, etc.) y que las acciones maliciosas se puedan detectar en base al tráfico de red. En todo este proceso son fundamentales las habilidades, experiencia adquirida de ataques producidos y conocimiento del personal de administración de la red, sistemas y seguridad.
- Revisión externa. Durante la revisión de la seguridad de los sistemas es conveniente que, aparte de la realizada por el personal interno, se realice también otra diferente por parte de otro equipo externo, ajeno al equipo de diseño y desarrollo. Ello aporta otra visión de la

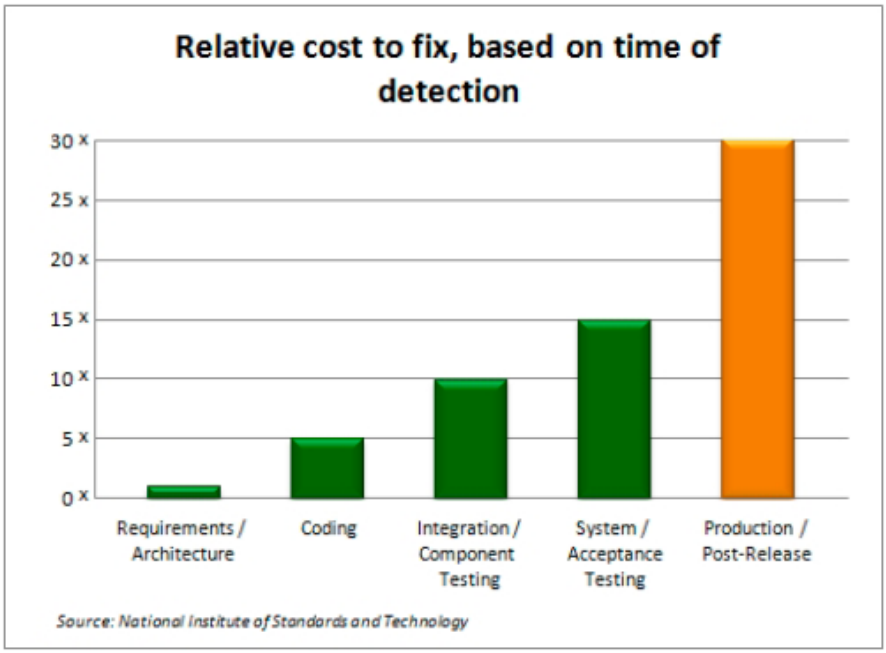

Fig. 5. Coste relativo de corrección de vulnerabilidades en función de la etapa de desarrollo. (Fuente: http://www.microsoft.com/security/sdl/learn/costeffective.aspx).

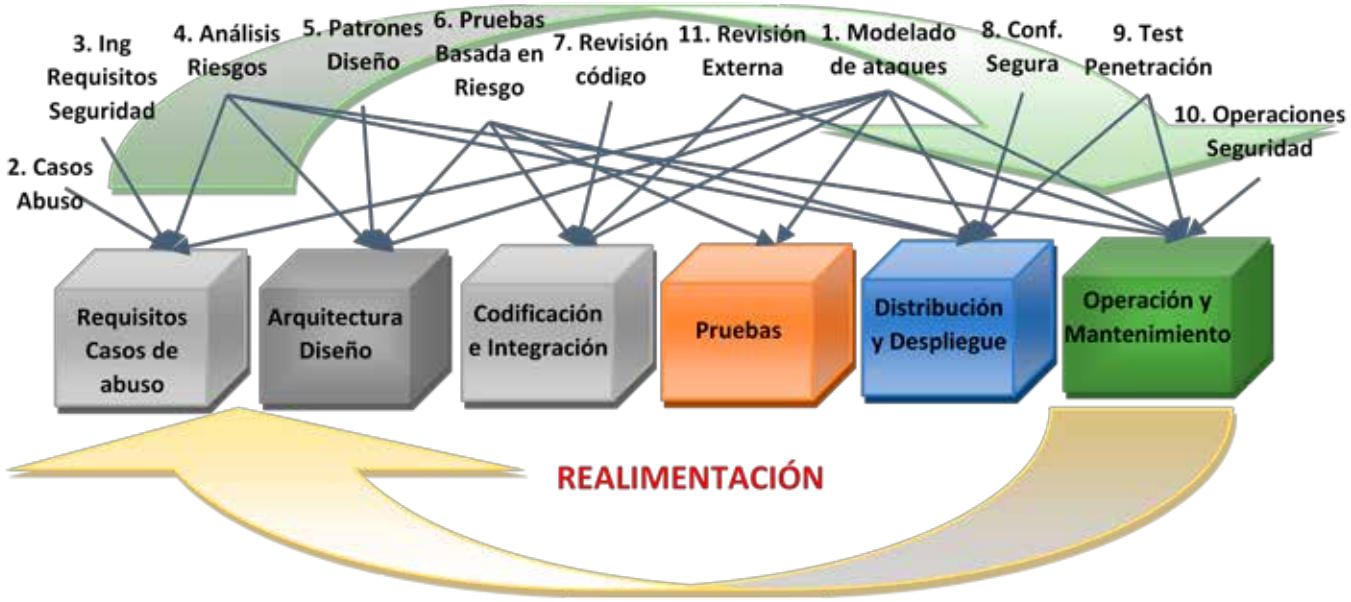

Fig. 6. Mejores prácticas de seguridad del software en el SDLC. (Fuente: Adaptación referencia [5]).

seguridad del sistema y del riesgo y contribuye a mejorar la seguridad al descubrir amenazas y riesgos residuales existentes, que pueden pasar desapercibidos para el equipo interno. Una vez finalizadas ambas revisiones y en función de los resultados obtenidos habrá que revisar el análisis de riesgos y su gestión, incorporar nuevas amenazas e incluso modificar las especificaciones del sistema.

Al igual que la gestión de riesgos, las actividades o buenas prácticas presentadas anteriormente hay que realizarlas de forma continua a lo largo de las diferentes iteraciones del ciclo de vida. Conforme se descubren nuevas amenazas, se introducen cambios adicionales o nuevos componentes, se reparan defectos o bugs detectados, hay que rehacer el análisis de riesgos con nuevos casos de abuso asociados, e incluso se pude llegar a tener que modificar las especificaciones iniciales del sistema.

Conclusiones

Actualmente las tecnologías de seguridad de red pueden ayudar a aliviar los ciberataques, pero no resuelven el problema de seguridad real ya que una vez que el ciberatacante consigue vencer esas defensas, por ingeniería social por ejemplo, y comprometer una máquina del interior, a través de la misma podrá atacar a las demás empezando por las más vulnerables.

Se hace necesario por tanto disponer de software seguro que funcione en un entorno agresivo y malicioso.

Para conseguir software confiable que solo realice las tareas para las que está diseñado y minimizar al máximo los ataques en la capa de aplicación y, por tanto, el número de vulnerabilidades explotables, es necesario seguir un proceso sistemático o disciplina que aborde la seguridad en todas las etapas del ciclo de vida de desarrollo del software que incluya una serie de buenas prácticas de seguridad (S-SDLC), como la especificación de requisitos seguridad, casos de abuso, análisis de riesgo, análisis de código, pruebas de penetración dinámicas, modelado de amenazas, operaciones de seguridad y revisiones externas, necesarias para asegurar la confianza y robustez del mismo.

En este sentido los profesionales de las Tecnologías de la Información y Comunicaciones tienen que ser conscientes de la seguridad del software, en cuanto a los beneficios que produce, su importancia en la seguridad global de un sistema, las propiedades de un software seguro, los ataques a los que se tiene que enfrentar y las metodologías aplicables a los procesos de desarrollo seguro de software. Todo un ciclo de seguridad iterativo y en paralelo al propio desarrollo del software.

Referencias

[1]. Hewlett-Packard Development Company (2011). Top Cyber Security Risks Report.

[2]. Karen Mercedes Goertzel. (2009). Introduction to Software Security. Edición en español. Recuperado el 27 de marzo de 2013 de: https://buildsecurityin.us-cert.gov/bsi/547-BSI.html

[3]. Klocwork Inc. Improving Software By Reducing Coding Defects Investing in software defect detection and prevention solutions to improve software reliability, reduce development costs, and optimize revenue opportunities.

[4]. SAFECode. (2010). Software Integrity Controls. Assurance-Based approach to minimizing risks in the software supply chain. Recuperado el 27 de marzo de 2013 de: http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf

[5]. Gary McGraw. (2005). Software Security: Building Security In. Addison Wesley Professional.

[6]. Hewlett-Packard Development Company, L.P. HP Security Research. Cyber Risk Report 2015. Año 2015. http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

[7]. DoD Software Assurance Initiative, CNSSI 4009 Terms National Information Assurance (IA) Glossary. Año 2006. http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.pdf

Boletín de Observación Tecnológica en Defensa

Disponible en

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

http://publicaciones.defensa.gob.es/inicio/revistas

SOPT
SISTEMA DE OBSERVACIÓN Y PROSPECTIVA TECNOLÓGICA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL