Defensa 4.0: Internet de las Cosas en Sistemas de Batalla (IoBT) en Defensa Naval

Article *in* RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao · May 2020

CITATIONS
0

READS
1,006

5 authors, including:

Jose Riola
Universidad Politécnica de Madrid
35 PUBLICATIONS **134** CITATIONS
SEE PROFILE

Oscar Mayorga Torres
Universidad Francisco de Paula Santander
9 PUBLICATIONS **9** CITATIONS
SEE PROFILE

Carlos Hernán Fajardo-Toro
41 PUBLICATIONS **83** CITATIONS
SEE PROFILE

Miguel Andrés Garnica López
Armada de Colombia
13 PUBLICATIONS **113** CITATIONS
SEE PROFILE

risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 14/11/2019
Aceitação/Acceptance: 19/01/2020

Defensa 4.0: Internet de las Cosas en Sistemas de Batalla (IoBT) en Defensa Naval

José María Riola[1], Carlos Hernán Fajardo-Toro[2], Javier Díaz Reina[3], Oscar Mayorga Torres[4], Miguel Andrés Garnica López[5]

jinvestigacionnaval@escuelanaval.edu.co, cfajardo.toro.academico@gmail.com, jdiazre21466@universidadean.edu.co, oscarmtorres@ufps.edu.co, mgarnica@cotecmar.co

[1] Escuela Naval de Cadetes "Almirante Padilla" – ENAP. Cartagena de Indias, Colombia.

[2] Grupo G3Pymes, Bogotá, Colombia.

[3] Armada República de Colombia – ARC, Bogotá, D. C., Colombia.

[4] Universidad Francisco de Paula Santander, Cúcuta; Colombia.

[5] Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval Marítima y Fluvial – COTECMAR. Cartagena de Indias, Colombia.

Pages: 507–519

Resumen: La cuarta revolución industrial I-4.0 se basa en la digitalización de sus procesos productivos, logísticos y militares, entre otros, permitiendo la interacción entre sistemas físicos y digitales, y logrando el uso de información en tiempo real para la toma de decisiones oportunas, así como la recolección de información para una planificación más precisa. En el campo militar, el empleo de Internet de las Cosas en el Campo de Batalla (*IoBT Internet of Battlefield Things*) ha permitido un acelerado desarrollo tecnológico en las operaciones militares, escenarios de batalla, procesamiento de datos y producción de equipos y maquinaria bélica, lo que en la literatura e industria militar se denomina Defensa 4.0. El presente artículo tiene como objetivo exponer la aplicación de la I-4.0 en el desarrollo, construcción y operación de los buques de guerra para el uso de la defensa naval, explicando su importancia e impactos en la industria militar.

Palabras clave: Industria 4.0, IoT, Buques de Guerra, Defensa 4.0.

Defense 4.0: Internet of Battlefield Things (IoBT) in Naval Defense

Abstract: The fourth industrial revolution (I-4.0) is based on the digitization of all its processes, allowing the interaction between physical and digital systems, thereby achieving the use of real-time information for making timely decisions. In the military field, the use of the Internet of Things in Battle Systems (IoBT – Internet of Battlefield Things) has allowed sped up technological development in military operations, battle scenarios, data processing, and production of war equipment and machinery, which in the literature and military industry is called Defense 4.0. This article aims to expose the application of I-4.0 in the development, construction, and

operation of warships for the use of naval defense, explaining its importance and impacts on the military industry.

Keywords: Industry 4.0, Internet of Things, Warships, Defense 4.0.

1. Introducción

La primera revolución industrial (1780) se caracterizó por la mecanización, la segunda revolución (1870) por el uso dela electricidad, la tercera (1960) por la automatización y la cuarta –I4.0– (2011) por la fusión entre los sistemas digitales y físicos, generando los sistemas inteligentes de producción (Anand & Nagendra, 2019; Hocaoğlu & Genç, 2019). Por otra parte, siempre los desarrollos en ciencia y tecnología han influenciado los conceptos y prácticas militares, en especial después de la revolución científica del Renacimiento (Burmaoglu, Saritas, & Yalcin, 2019).

Un concepto importante que ha permitido el desarrollo de la I-4.0 es el de Internet de las Cosas –IoT– que está relacionado con los términos M2M (Machine to Machine communications) y CPS (Cyber Phisical Systems). De lo anterior, una definición de IoT es la interconexión física basada en telecomunicaciones para el intercambio de datos entre dos entidades compatibles con M2M como: dispositivo, pasarelas e infraestructura de red (ETSI, 2013), y se le considera una de las seis tecnologías civiles disruptivas según consejo nacional de inteligencia de EE.UU. (Raglin, 2019). La aplicación de IoT en operaciones militares es una realidad actualmente y se le denomina internet de las cosas en Campos de batalla – IoBT – donde las cosas inteligentes no serán extrañas pero sí con una presencia ubicua en los campos de batalla (Kott & Stump, 2019). El campo de batalla del futuro comprenderá una amplia gama de sensores, dispositivos, fuentes de información, análisis, humanos e infraestructura con capacidades computacionales heterogéneas, con inteligencia, capacidades y limitaciones variables en recursos de energía, computación y comunicación, y teniendo un dominio de la información que permita minimizar riesgos (Jalaian & Russell, 2019).

2. Defensa 4.0 e IoBT

La I-4.0 es un tema de tendencia en todas las discusiones sobre perspectivas de futuro cercano. Jazdi (2014) sugiere que el concepto apareció por primera vez en Alemania en 2011, y fue presentado al público en general por la Asociación de Fabricantes Alemanes de Máquinas y Equipos de Producción (Verband Deutscher Maschinen- und Anlagenbau, VDMA) en la Feria de Hannover 2013, donde se combinaban tres innovaciones tecnológicas (automatización, IoT e inteligencia artificial) mediante la creación de modelos comerciales innovadores e ir más allá de la innovación de productos y procesos (Fajardo-Toro, Aguilera-Castillo, & Guerrero-Cabarcas, 2019).

Este nuevo paradigma industrial se basa en el uso de tecnologías asociadas a la Inteligencia Artificial (AI), así como en la unión o relación de elementos físicos a través de sensores permitiendo la conexión entre ellos (M2M y CPS) y que es el fundamento del internet de las cosas (Zona-Ortiz, Fajardo-Toro, Aguilar, 2020). En términos industriales, el uso de estas tecnologías permite la flexibilización y optimización de procesos y servicios, tanto en la planificación con información precisa, control de la cadena de abastecimiento y su

logística, información en tiempo real de las operaciones y cambios en las habilidades y competencias de las personas(Büchi, Cugno, & Castagnoli, 2020; Lins & Oliveira, 2020).

Tanto la logística como el concepto de cadena de abastecimiento tiene un origen militar, y bajo estos términos, todas las organizaciones tienen proveedores, una logística de aprovisionamiento, logística de operaciones o mantenimiento y logística de distribución (Bowersox and Closs, 2002). Ahora, en términos de las operaciones militares, se puede suponer que tiene las características logísticas de las empresas de servicio por su carácter intangible. Bajo este contexto, habrá una logística de aprovisionamiento la cual es fundamentalmente de armamento, personal, alimentos y suministros sanitarios, repuestos, y su logística de producción y distribución están unidas, dado que la ejecución de la operación se hace en el destino asignado, con lo anterior, la figura 1 presenta el concepto de una forma más descriptiva en la industria aplicado a las plataformas militares: buques, aviones y carros desde un punto de vista global aplicable a un Ministerio de Defensa.

Figura 1 – Concepto operativo en el sector militar. (Fuente: Indra)

Uno de los factores que ha dado siempre ventaja a los ejércitos es el desarrollo, mejora y adquisición de tecnologías, tanto en armamento como en sistemas de comunicación y adquisición de información, donde la estrategia se centró desde la década del 2000 hacia el uso extensivo de computadores, satélites y tecnologías sigilosas – stealth - (Compston, 2006). Siguiendo esa estrategia, entra la aplicación del IoBT y de sistema de inteligencia artificial buscando la sincronización de operaciones, disminución de riesgos, labores de inteligencia, mantenimiento de equipos, etc. (Russell & Abdelzaher, 2019).

En el proceso de planificación, el IoBT se utiliza para obtención de Inteligencia (Xi, Lingyu, & Jiapeng, 2019), el análisis y reducción de riesgos utilizando la información

recogida y algoritmos inteligentes (Russell & Abdelzaher, 2019; Sondrol, Jalaian, & Suri, 2019). También se está utilizando tecnología en la toma de decisiones tácticas en función de los distintos componentes del campo de batalla que estarán interconectados, manejando la información que genera cada uno a través de sensores y sincronizándolos en tiempo real para trabajar al unísono (Farooq & Zhu, 2018; Iyer & Patil, 2018; Poltronieri et al., 2019; Sundeep Desai, Varghese, & Nene, 2020; Varghese, Desai, & Nene, 2019), generando desinformación para el enemigo a través de dichos sistemas (Abuzainab & Saad, 2018) y en aplicaciones para registro de solados buscando reducir las bajas, soldados desaparecidos o que puedan ser atendidos en caso de estar heridos (Iyer & Patil, 2018).

Respecto a los sistemas navales, se están desarrollando trabajos en especial sistemas de control de ubicación y comunicaciones, (Zhen & Lin, 2019), robotización de entornos de alto riesgo para la tripulación (Nikitakos, Tsaganos, & Papachristos, 2018), buques autónomos (Im, Shin, & Jeong, 2018) y sistemas de control de maquinaria y seguridad de esa información (Sahay, Meng, Estay, Jensen, & Barfod, 2019). La figura 2 presenta un buque que emplea IoBT en una evaluación CSQT de misiles

Figura 2 – Fragata en operaciones CSQT. (Fuente: Real Armada España)

3. IoBT y los Buques de Guerra

Si la Industria 4.0 necesita desarrollarse en un dominio híbrido, en el que el mundo real y el digital se intercambian información a través de una interfaz que procesa aplicaciones de datos entre el usuario y la toma de decisiones, al particularizarlo para el sector naval, el buque es el mundo real que deberá ser capaz de integrar miles de datos de los distintos sistemas y equipos para conseguir darle un valor añadido a la información obtenida de los sensores, que permita poder realizar las operaciones de una forma óptima y, además, conseguir que el ciclo de vida del buque se desarrolle con el menor coste.

Los mercados navales se basan en la personalización al ser los buques de guerra prototipos únicos, a lo sumo series de 4 o 5 buques, y en la creación de servicios tecnológicamente sofisticados e innovadores. Las armadas siempre están hambrientas de tecnología por ser la razón de su supervivencia en un conflicto y por ello exigen una determinada calidad a

sus sistemas, una experiencia individualizada y una buena capacidad de modernización en sus plataformas. Todo ello pasa por mejorar el software y añadir conectividad a cualquier sistema. Así, sus sistemas inteligentes se caracterizan por disponer de mucha electrónica, software embebido y la máxima conectividad, lo que en conjunto dotan al buque de excelentes características, capacidades y funciones.

Por su propio concepto, un buque de guerra es un sistema complejo y costoso, donde casi todo es redundante, con un largo ciclo de adquisición y una vida operativa en torno de 30 a 40 años. Por todo esto la optimización de su ciclo de vida tiene cada vez mayor importancia (Riola et al, 2019) para cualquier armada. Tal es así, que no se debe pensar exclusivamente en el coste de construcción o adquisición de un buque, si no en cuanto costará a lo largo de todo su ciclo de vida, y ahí estará uno de los pilares de la rentabilidad del buque. La figura 3 muestra un buque de guerra OPV con ciclo de vida optimizado, construido por Cotecmar para la Armada de Colombia.

Figura 3 – OPV. (Fuente: Armada de Colombia)

Las Armadas definen la ingeniería del ciclo de vida como el conjunto de las actividades necesarias para la adecuación de las plataformas y los sistemas de armas a sus requisitos operativos, siendo fundamentales para estos procesos el control de la configuración y la determinación, evaluación y mejora del apoyo de los sistemas y equipos que los componen a lo largo de toda su vida operativa. Y además definen el apoyo logístico como el conjunto de acciones para poder proporcionar a sus unidades los medios y sistemas que necesitan para el cumplimiento de las misiones que son la razón de su existencia. Así que se puede concretar, que todas las armadas necesitan enfocar parte de sus esfuerzos en conseguir las herramientas y procesos que le permitan disminuir sus gastos en logística y el ciclo de vida de sus buques, por lo que las tecnologías 4.0 han pasado a ser la esencia misma de las operaciones a bordo de los buques y, además, les aportan las herramientas necesarias para optimizar el adecuado sostenimiento.

Las cadenas de suministro logísticas de las armadas están experimentando una elevada automatización y una integración del software a todos sus niveles, con el añadido de necesitar una comunicación rápida y directa con la industria auxiliar naval. Así, en lugar de la integración horizontal habitual en la industria hoy, la colaboración entre las empresas auxiliares y las armadas en la industria 4.0 se basará en configuraciones ad-hoc para ofrecer soluciones a medida de sus necesidades.

Usando redes de colaboración más ágiles, la industria auxiliar puede aprovechar las oportunidades de un mercado globalizado de capacidades, lo que le deberá permitirá a la armada decidir qué externalizar o qué hacer ellos mismos, pudiendo trabajar con los suministradores y proveedores de servicios de ingeniería a través de plataformas compartidas. La base para estas redes logísticas es que los entornos de producción y las plataformas de ingeniería estén conectadas en red con interfaces entre empresas. Así, la cadena de suministro conectada es otra pieza central en toda estrategia 4.0. Para gestionar la complejidad de las cadenas de suministro, los flujos físicos se replican previamente en las plataformas digitales.

Un buque de guerra, el entorno digital más sencillo se conoce como "maqueta digital", la cual debe de ser una versión virtual del barco, un modelo 3D que además de ofrecer disposiciones de compartimentos, capacidades, equipos, manuales de mantenimiento, etc., también puede proporcionar datos de sensorización como temperatura, presión, niveles de tanques, etc. Al citar el término "gemelo digital", se está dando un salto tecnológico en el que el mundo real y el virtual son capaces de interactuar entre si. La idea del gemelo digital surgió en la agencia americana NASA en el año 2012 cuando consiguieron desarrollar unas tecnologías que les permitían operar y mantener los sistemas que estaban fuera de su alcance físico, lo que les llevó a implementar una filosofía de simulación en la cual todo equipo antes de instalarse debe demostrar la evaluación positiva de su prototipo. Todo debe ser simulado, probado y evaluado antes de su posible construcción y específicamente, antes de su colocación definitiva a bordo. La figura 4 hace un comparativo entre el concepto simulado y el real de la construcción de los buques.

Figura 4 – Relación temporal virtual y real. (Fuente: Navantia)

El gemelo digital nace a partir de los requisitos de Estado Mayor que son elaborados por las distintas armadas, estos requisitos son las voces en que definen qué buque se quiere construir, que características deberá cumplir. Y desde ese momento, va robusteciendo de información, señales, conectividad y representaciones virtuales al pasar por las fases de diseño conceptual, funcional, de detalle, producción y sostenimiento. Para que este gemelo digital sea totalmente operativo, todos los equipos que van a ir a bordo deben entregarse por los suministradores con el CAD y la sensórica correspondiente, la cual debe

permitirle al buque integrarla con el resto de las señales. Es particularmente importante que la industria auxiliar naval que rodea al buque de guerra se encuentre inmersa en la digitalización de todos sus procesos logísticos, lo que incluye fundamentalmente a los de mantenimiento.

A medida que los datos van alimentando al gemelo digital, este evoluciona hacia un avatar del producto cada vez más real, permitiendo interactuar con él de manera más sencilla y, además, visualizar su estado remotamente a muchas millas de distancia. La interacción entre el gemelo digital y buque se lleva a cabo mediante la aplicación de tecnologías como "machine learning", "cloud computing" o "IoT", que generará las necesarias simulaciones desde la identificación de acciones correctivas y preventivas de los sistemas, hasta los propios escenarios misionales de operación o posibles emergencias, la figura 5 presenta el ciclo de vida del gemelo digital.

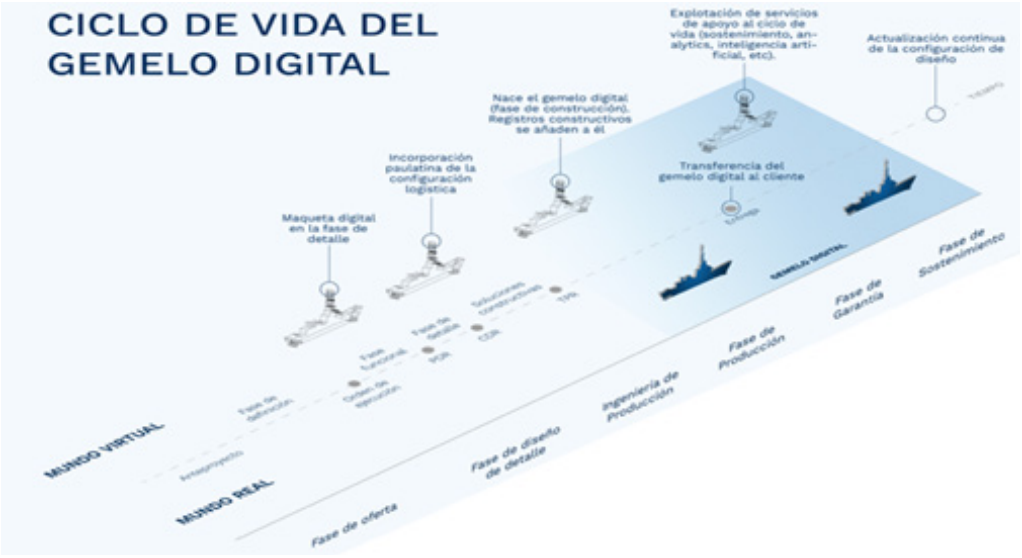

Figura 5 – Ciclo de vida del gemelo digital. (Fuente: Navantia)

El gemelo digital es la pieza clave de la transformación digital de los buques, especialmente en la explotación de datos y modelos, además de ser la pieza clave en la transformación de las propias armadas. La importancia de los gemelos digitales consiste fundamentalmente en ayudar a que las decisiones estén basadas en modelos que aprenden de los datos que pueden ser: descriptivos, decisivos, diagnósticos, predictivos o prescriptivos y que hay que saber cuales hay que tomar y desechar. El producto inteligente tiene la ambición de ser autónomo, por lo que se necesita una algorítmica especialmente robusta.

Las armadas, siempre conservadoras y preocupadas por sus altos costes logísticos, han encontrado en estas tecnologías la capacidad de mejorar la eficacia operativa de sus buques reduciendo los costes asociados a su ciclo de vida en los tres pilares de sus funciones logísticas: mantenimiento, aprovisionamiento e ingeniería a lo largo del ciclo

de vida. Y los centros tecnológicos de Defensa con capacidad de I+D+i, como lo es la Escuela Naval de Cadetes “Almirante Padilla” (ENAP), deben orientar sus líneas de investigación hacia esta área.

Los avances tecnológicos que han desarrollo el gemelo digital dependerán cada vez más de las comunicaciones, lo que junto con las nuevas tecnologías basadas en software para operaciones como el posicionamiento dinámico o la toma de aeronaves abordo, incrementan la vulnerabilidad de los sistemas de información para la defensa, haciendo que la ciberseguridad considere que nuestros hardware/software son posibles puntos débiles que deben asegurarse, por lo que la ciberdefensa deberá apoyarse y basarse en “cybersecurity, cybersafety & cyberperformance” (Pancorbo et al, 2020).

Dada la complejidad de sistemas y equipos, los buques de guerra tienen dos cerebros en su interior, en primer lugar, el Sistema de Combate (SdC) que integra sensores y armas, de altísimas prestaciones cuando se le requiere, pero que suele permanecer en reposo durante largas temporadas y el Sistema Integrado de Control de Plataforma (SICP) que trabaja constantemente las 24 horas (ver figura 6). Este SICP tiene como finalidad la monitorización y el control remoto de todos los equipos y sistemas que lleva en su interior el buque, con base a componentes hardware y software. Para cumplir su cometido, el SICP deberá estar conectado con todos ellos y en un doble lazo o anillo que recorre ambos costados para seguir funcionando en caso de avería o de un posible impacto en su superestructura, asegurando su continuidad en las operaciones y su supervivencia en la mar. Desde el SICP se supervisa y controlan todos lo sistemas de abordo con tecnología 4.0 como la propulsión, la generación y distribución eléctrica y el funcionamiento de todos los sistemas auxiliares y de averías del buque, etc.

Figura 6 – Los dos cerebros SdC y SICP. (Fuente: propia)

El SICP debe ser capaz de establecer los criterios necesarios para priorizar las tareas de mantenimiento y evitar las innecesarias, y además, debe predecir las situaciones que produzcan tiempos muertos que afecten la seguridad de la dotación y conduzcan a posibles fallos catastróficos, así mismo, debe reducir las duración de los tiempos muertos por la gestión dinámica de las tareas en tierra basada en diagnósticos esperados del sistema y actualizar los procedimientos operativos basados en el análisis de incidentes que puedan

influir sobre la disponibilidad operativa del buque. Además, deberá complementar el mantenimiento tradicional preventivo mediante el registro de horas de funcionamiento de los equipos y su envío a las herramientas de apoyo logístico para proporcionar un mantenimiento predictivo o basado en condición, en tiempo real, por la medición de parámetros como pueden ser las vibraciones de los equipos rotativos, condiciones de los aceites lubricantes, presión de los cilindros de los motores diésel, etc. (Navantia, 2019)

El software del SICP está compuesto de algoritmos y secuencias de control, propias de los autómatas y controladores lógicos, junto a un sistema integrador que organiza y relaciona los datos para presentárselos al operador mediante interfaces hombre-máquina. Este sistema debe de constar de consolas de operación, subestaciones locales, unidades de transmisión remota, paneles locales de operación y red de transmisión de datos. Su hardware se suele basar en elementos disponibles en el mercado (COTS): PLC, PC, LAN y Bus para las comunicaciones.

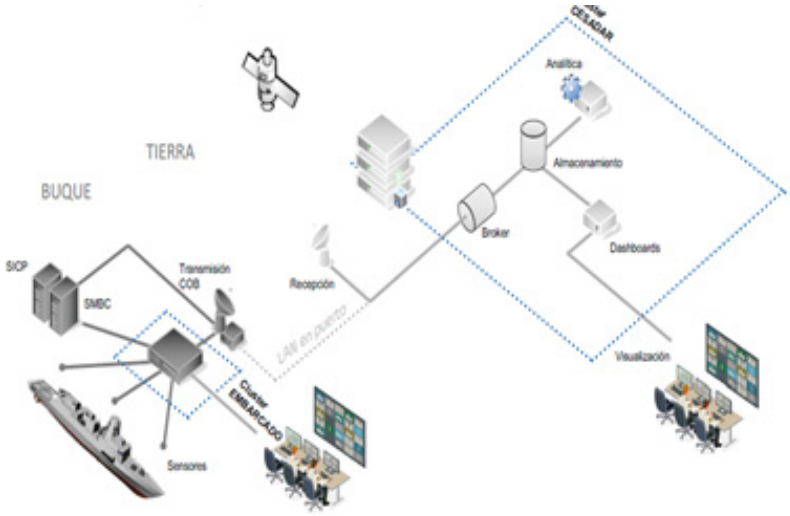

Figura 7 – Análisis de datos a distancia. (Fuente: CESADAR)

En el caso de algunas armadas, como la Española, se cuenta con centros en tierra como el CESADAR (ver figura 7), para el cual el SICP trabaja y se encarga del envío de los datos recogidos a bordo para transmitírselos y así puedan recibir, almacenar y analizar en tierra lo que está pasando en tiempo real en el buque, utilizando técnicas de minería de datos capaces de extraer información de los datos registrados utilizando inteligencia artificial y diversos tipos de análisis de datos. Este tipo de centros supone un esfuerzo por complementar a los sistemas SICP y se fundamentan en conseguir sistemas con mantenimiento basado en la condición (SMBC), encargándose de recolectar y almacenar de forma segura todos los datos generados diariamente, mediante servidores y equipos de almacenamiento, para ser evaluados y procesados por el personal del centro. El año pasado, el CESADAR recibía información de 35 buques con una media de más de 30 000 señales por buque, lo que implicaba más de 300 MB de datos por día y buque. En

la actualidad, esta información es evaluada por diversas aplicaciones desarrolladas al efecto y distintas herramientas externas como, por ejemplo, las diseñadas por Windrock 23 o por OneProd.24 (García, 2017).

La industria naval se encuentra inmersa en la digitalización de sus procesos logísticos, incluyendo los de mantenimiento, principal objetivo de reducción de costes de cualquier armada. El objetivo buscado es la predicción de las tareas de mantenimiento basado en confiabilidad, por lo que cualquier señal como puede ser la monitorización de la vibración de un motor embarcado puede ayudar a prever las tareas de mantenimiento y disminuir con ello el coste del ciclo de vida. Existen diversos métodos de AI para clasificar patrones o hacer regresiones de un determinado parámetro mecánico que son la base del análisis en estos centros. Resumiendo, se puede concretar el lineamiento en el que están trabajando las distintas armadas:

- Diseñar y crear el gemelo digital del buque.
- Desarrollar un Sistema Integrado de Control de Plataforma que monitorice e integre todas las señales de sistemas y equipos de la plataforma.
- Integrar un sistema de comunicaciones satelitales que permita el análisis en tiempo real de lo que le ocurre a los sistemas y equipos de buque.
- Disminuir el coste del ciclo de vida con base en el análisis de las señales y en la programación del mantenimiento basado en confiabilidad.

Si se particulariza el entorno naval, los buques desarrollados por la Armada de Colombia deberán cumplir con los requisitos “Shipping 4.0” que se muestran en la figura 8 y que resume estos retos tecnológicos a incluir a bordo, y a los retos que las armadas del siglo XXI se tienen que adaptar.

Figura 8 – Shipping 4.0. (Fuente: Haugesundkonferansen)

4. Conclusiones

Un entorno tecnológico y digitalizado es característico de la I-4.0. Esto ha impactado de forma directa en los diferentes sistemas y organizaciones a nivel mundial, entre estas, a los Ministerios de Defensa que por su propia naturaleza requieren estar actualizados con los últimos desarrollos e innovaciones tecnológicas, informáticas y de comunicaciones, para

fortalecer sus mecanismos de seguridad, tiempos de respuesta, preparación y reacción de tropas, desarrollo de equipos a entorno propio e incorporación de conocimiento científico-tecnológico en sus sistemas militares.

Para la fabricación de buques de guerra se está apropiando y desarrollando tecnología que se apoya en sistemas de simulación moderna para mejorar los tiempos de construcción y operación de las naves, donde se adapta la tecnología a las necesidades de la geografía y condiciones climáticas de los países que así lo requieren. Estos buques integran mejoras en el sistema de combate, sistema integrado de control de plataforma, vehículos no tripulados (UAV), aumento del ciclo de vida y empleo del "big data" en las comunicaciones satelitales.

Finalmente, la incorporación de IoBT en la fabricación de buques de guerra optimizará los sistemas de operación, combate, comunicación y navegabilidad de las naves, con sensores, dispositivos y armas modernos con la ventaja de que todo lo anterior puede ser simulado, probado y evaluado antes de su construcción y colocación definitiva a bordo.

Referencias

Abuzainab, N., & Saad, W. (2018). Misinformation Control in the Internet of Battlefield Things: A Multiclass Mean-Field Game. 2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings, 1–7. https://doi.org/10.1109/GLOCOM.2018.8647236

Anand, P., & Nagendra, A. (2019). Industry 4.0: India's defence industry needs smart manufacturing. International Journal of Innovative Technology and Exploring Engineering, 8(11 Special Issue), 476–485. https://doi.org/10.35940/ijitee.K1081.09811S19

Bowersox, D., Closs, D. (2002). Supply chain logistics management. 1st edition. McGraw Hill education. NY

Büchi, G., Cugno, M., & Castagnoli, R. (2020). Smart factory performance and Industry 4.0. Technological Forecasting and Social Change, 150(November 2019), 119790. https://doi.org/10.1016/j.techfore.2019.119790

Burmaoglu, S., Saritas, O., & Yalcin, H. (2019). Defense 4.0: Internet of Things in Military. In Emerging Technologies for Economic Developmen (pp. 303–320). https://doi.org/10.1007/978-3-030-04370-4_14

Compston, H. (2006). Military Technology. In King Trends and the Future of Public Policy (pp. 76–98). https://doi.org/10.1057/9780230627437

ETSI, «Technical Recommendation ETSI TR 102 725: "Machine to machine definitions",» Francia, 2013.

Fajardo-Toro, C. H., Aguilera-Castillo, A., & Guerrero-Cabarcas, M. (2019). Doing More With Less: The Impact of New Technologies on Labor Markets, Economy, and Society. In A. Guerra Guerra (Ed.), Organizational Transformation and Managing Innovation in the Fourth Industrial Revolution (pp. 1–17). https://doi.org/10.4018/978-1-5225-7074-5.ch001

Farooq, M. J., & Zhu, Q. (2018). On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT). IEEE Transactions on Wireless Communications, 17(4), 2618–2632. https://doi.org/10.1109/TWC.2018.2799860

Fdez Jove, A., Mackinlay, A. y Riola, J.M. (2019). Optimización del ciclo de vida en el buque de guerra: plan de mantenimiento y monitorización para la reducción de costes. VI International Ship Design & Naval Engineering Congress CIDIN2019, Colombiamar, Cartagena de Indias, Colombia.

García, P. (2017). Gemelo Digital: Concepto y Aplicación en la Armada. ETSIN. Universidad Politécnica de Madrid.

Hocaoğlu, M. F., & Genç, İ. (2019). Smart Combat Simulations in Terms of Industry 4.0. In M. M. Gunal (Ed.), Simulation for Industry 4.0 Past, Present, and Future (pp. 247–273). https://doi.org/10.1007/978-3-030-04137-3_15

Im, I., Shin, D., & Jeong, J. (2018). Components for Smart Autonomous Ship Architecture Based on Intelligent Information Technology. Procedia Computer Science, 134, 91–98. https://doi.org/10.1016/j.procs.2018.07.148

Indra. (2019). Sostenimiento 4.0. Transformación digital aplicada al sostenimiento de sistemas embarcados. VI Congreso de Seguridad y Defensa DESEi+d, Valladolid, España.

Iyer, B., & Patil, N. (2018). IoT enabled tracking and monitoring sensor for military applications. International Journal of Systems Assurance Engineering and Management, 9(6), 1294–1301. https://doi.org/10.1007/s13198-018-0727-8

Jalaian, B., & Russell, S. (2019). Uncertainty Quantification in Internet of Battlefield Things. In Artificial Intelligence for the Internet of Everything (pp. 19–45). https://doi.org/10.1016/b978-0-12-817636-8.00002-8

Jazdi, N. (2014). Cyber physical systems in the context of Industry 4.0. In Automation, Quality and Testing, Robotics, 2014 IEEE International Conference (pp. 1-4). IEEE.

Kott, A., & Stump, E. (2019). Intelligent Autonomous Things on the Battlefield. In Artificial Intelligence for the Internet of Everything. https://doi.org/10.1016/b978-0-12-817636-8.00003-x

Lins, T., & Oliveira, R. A. R. (2020). Cyber-physical production systems retrofitting in context of industry 4.0. Computers and Industrial Engineering, 139(November 2019), 106193. https://doi.org/10.1016/j.cie.2019.106193

Navantia. (2019). Sistema Integrado de Control de Plataforma (SICP). www.infodefensa.com

Nikitakos, N., Tsaganos, G., & Papachristos, D. (2018). Autonomous Robotic Platform in Harm Environment Onboard of Ships. IFAC-PapersOnLine, 51(30), 390–395. https://doi.org/10.1016/j.ifacol.2018.11.337

Pancorbo, J, Guerrero, L. y González, J. (2020). El "Gemelo digital". Proceso de digitalización desde el punto de vista de una sociedad de clasificación. Ship Science & Technology - Vol. 13 - n.º 26 - (9-18) January 2, Cartagena de Indias, Colombia.

Poltronieri, F., Sadler, L., Benincasa, G., Gregory, T., Harrell, J. M., Metu, S., & Moulton, C. (2019). Enabling Efficient and Interoperable Control of IoBT Devices in a Multi-Force Environment. Proceedings - IEEE Military Communications Conference MILCOM, 2019-Octob, 757–762. https://doi.org/10.1109/MILCOM.2018.8599740

Raglin, A. (2019). Presentation of information uncertainty from iobt for military decision making. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). https://doi.org/10.1007/978-3-030-21935-2_4

Riola, J.M., Díaz-Cuadra, J.C. y Beltrán, P. (2019). Programa de Control de Ruido y Vibraciones para un buque de Guerra: La nueva Fragata Española F-110. VI International Ship Design & Naval Engineering Congress CIDIN2019, Colombiamar, Cartagena de Indias, Colombia.

Russell, S., & Abdelzaher, T. (2019). The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making. Proceedings - IEEE Military Communications Conference MILCOM, 2019-Octob, 737–742. https://doi.org/10.1109/MILCOM.2018.8599853

Sahay, R., Meng, W., Estay, D. A. S., Jensen, C. D., & Barfod, M. B. (2019). CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. Future Generation Computer Systems, 100, 736–750. https://doi.org/10.1016/j.future.2019.05.049

Sondrol, T., Jalaian, B., & Suri, N. (2019). Investigating LoRa for the Internet of Battlefield Things: A Cyber Perspective. Proceedings - IEEE Military Communications Conference MILCOM, 2019-Octob, 749–756. https://doi.org/10.1109/MILCOM.2018.8599805

Sundeep Desai, S., Varghese, V., & Nene, M. J. (2020). Controller Area Network for Battlefield-of-Things. In M. Singh, P. K. Gupta, V. Tyagi, J. Flusser, T. Ören, & R. Kashyap (Eds.), Advances in Data Sciences, Security and Applications Proceedings of ICDSSA 2019 (pp. 211–223). https://doi.org/10.1007/978-981-15-0372-6_16

Varghese, V., Desai, S. S., & Nene, M. J. (2019). Decision Making in the Battlefield-of-Things. Wireless Personal Communications, 106(2), 423–438. https://doi.org/10.1007/s11277-019-06170-y

Xi, M., Lingyu, N., & Jiapeng, S. (2019). Research on urban anti-terrorism intelligence perception system from the perspective of Internet of things application. International Journal of Electrical Engineering Education. https://doi.org/10.1177/0020720918819247

Zhen, W., & Lin, B. (2019). Maritime Internet of Vessels. In Encyclopedia of Wireless Networks (pp. 1–9). https://doi.org/10.1007/978-3-319-32903-1_344-1

Zona-Ortiz, T., Fajardo-Toro, C.H., Aguilar, C. (2020). Propuesta De Un Marco General Para El Despliegue De Ciudades Inteligentes Apoyado En El Desarrollo De IoT En Colombia. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao.