DATA LINKS VENTAJA ESTRATÉGICA Y DESAFÍO PARA LA SEGURIDAD

Introducción

Los enlaces de datos, o Data Links, se han convertido en una **tecnología de referencia para la comunicación en tiempo real entre diferentes sistemas, plataformas y redes**. Pueden ser usados en cualquier sector, desde las telecomunicaciones hasta el transporte y las infraestructuras críticas, donde actúan como facilitadores clave para la coordinación rápida y efectiva de distintos actores involucrados en una operación.

Esta capacidad de ofrecer **información instantánea y precisa** ha convertido a los Data Links en una herramienta estratégica indispensable para agilizar la toma de decisiones y optimizar operaciones, especialmente en el campo de la defensa y la seguridad.

El reverso de la moneda es que los Data Links abren un nuevo frente en el campo de las **comunicaciones seguras**. A medida que los ataques a la ciberseguridad aumentan se presenta un nuevo frente en esta lucha que, debido a la información sensible que manejan, deben atajar cualquier vulnerabilidad para no poner en riesgo una operación comprometida. Todo esto, **en un entorno operativo cada vez más orientado a la integración de distintos medios e interoperabilidad de plataformas y nodos de diversos ámbitos**.

Por qué los Data Links son una ventaja estratégica

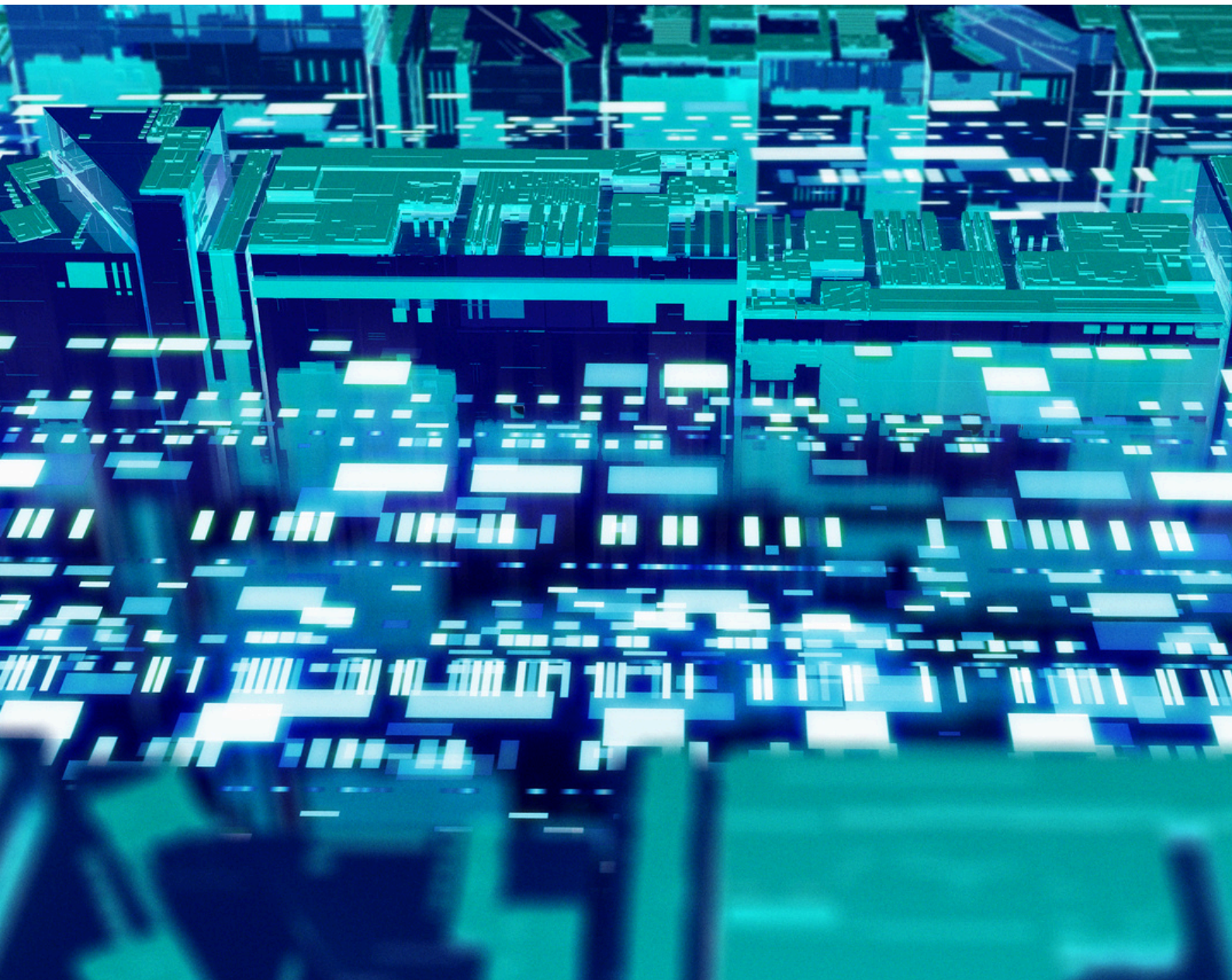
Los Data Links juegan un papel crucial en la coordinación de operaciones en entornos complejos y dinámicos. Su capacidad de interconectar múltiples sistemas y transmitir información instantánea entre ellos **permite una gestión mucho más eficiente de los recursos**. Especialmente en aquellas operaciones que requieren una supervisión constante para tomar decisiones rápidas en función de los datos recibidos en tiempo real.

Uno de los mayores beneficios de los Data Links es su **capacidad para poder gestionar la interoperabilidad entre sistemas dispares**. Por ejemplo, en la gestión de redes eléctricas o sistemas inteligentes de transporte, los Data Links permiten que diferentes componentes (como sensores, vehículos y centros de control) se comuniquen de manera fluida y en tiempo real. Esta capacidad de conectar varios subsistemas en una única red de comunicaciones ofrece una visión integral y en tiempo real de las operaciones, lo que resulta en una mejor toma de decisiones y un uso óptimo de los recursos.

Además, los enlaces de datos son un **habilitador fundamental para los sistemas basados en IoT (Internet de las Cosas)**. A medida que crece el número de dispositivos conectados, los Data Links permiten que estos intercambien grandes cantidades de

datos, proporcionando un flujo continuo de información que facilita la automatización y la inteligencia artificial. Ya sea en ciudades inteligentes, fábricas automatizadas o cadenas de suministro digitalizadas, los Data Links **permiten que todos los componentes trabajen de forma sincrónica para mejorar la eficiencia, la seguridad y la productividad**.

Pero para garantizar una mejor interoperabilidad es fundamental que estos dispositivos incorporen alguna **medida de encriptado y autenticación** para proteger la información que vamos a transmitir.



Desafíos de seguridad y soluciones tecnológicas

Los ataques a la ciberseguridad o nuevos tipos de amenazas como la guerra electrónica pueden comprometer gravemente operaciones críticas que tenemos que llevar a cabo. ¿Cómo afectan estos ataques a los enlaces de datos?

Jamming

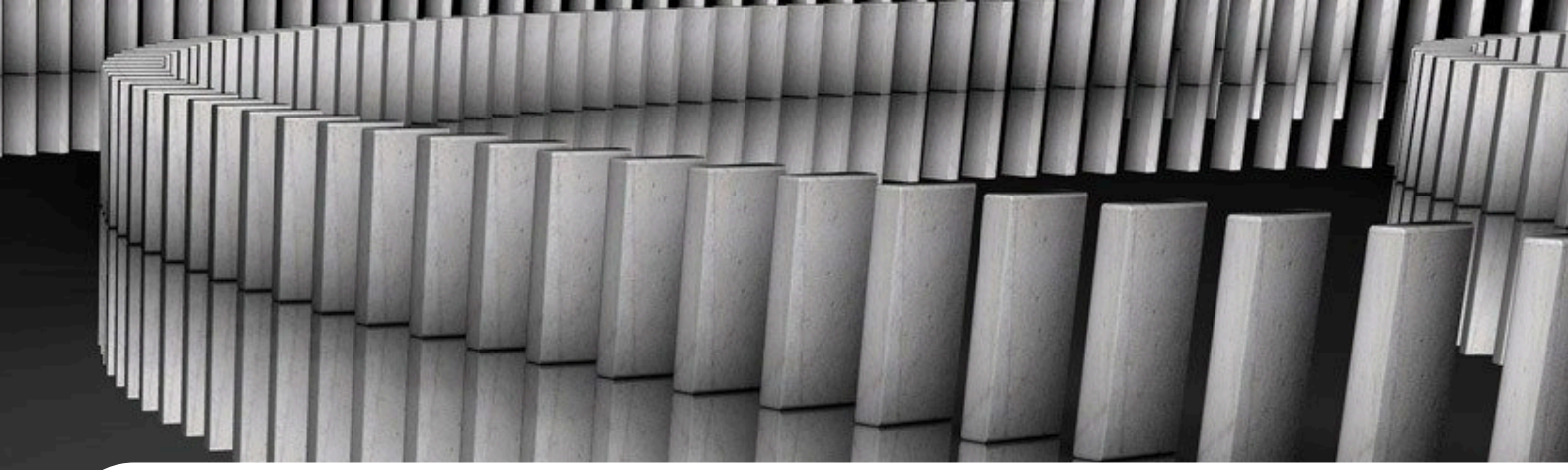
Uno de los principales riesgos son las interferencias o interrupciones en las comunicaciones, especialmente en entornos donde las transmisiones de datos deben ser fiables y continuas. Por ejemplo, en el campo militar. Los ataques de jamming (interferencia deliberada) pueden desactivar temporalmente las comunicaciones entre sistemas, lo que podría llevar a interrupciones significativas en operaciones críticas.

Para mitigar este riesgo, los enlaces de datos modernos implementan tecnologías avanzadas en la securización de la transmisión, como la modulación de frecuencia variable y la resistencia a la interferencia. Estas técnicas permiten que los sistemas cambien de frecuencia de manera dinámica, haciendo más difícil que un atacante bloquee la señal de forma efectiva. De este modo, las comunicaciones pueden continuar de manera fluida, incluso en condiciones adversas.

Hacking

Otro reto clave para los enlaces de datos es el hackeo y la interceptación de comunicaciones. En un mundo donde los ataques cibernéticos son cada vez más sofisticados, los Data Links que transmiten información crítica son un blanco atractivo para actores malintencionados. La intercepción de datos sensibles o el acceso no autorizado a redes de comunicación podría comprometer seriamente la seguridad de operaciones industriales, financieras o incluso gubernamentales.

Para contrarrestar estas amenazas, los sistemas de Data Links avanzados utilizan técnicas de securización de la comunicación, como protocolos de encriptación robustos que aseguran que los datos transmitidos solo puedan ser leídos por las partes autorizadas. Además, los sistemas de autenticación y control de acceso garantizan que solo los usuarios y dispositivos aprobados puedan conectarse y operar dentro de la red de comunicación. Estas medidas de seguridad son esenciales para proteger las infraestructuras críticas que dependen de enlaces de datos confiables.



Debilidad y fallos combinados

Además de la seguridad cibernética, la resiliencia de los sistemas es un factor crucial para asegurar la continuidad operativa. En muchas industrias, la redundancia se ha convertido en una estrategia clave para mantener las comunicaciones activas, incluso en caso de fallos técnicos o ataques externos. Al contar con rutas de comunicación los sistemas pueden seguir funcionando sin interrupciones, lo que asegura la confiabilidad de las operaciones en momentos críticos.

Por último, los enlaces de datos también deben enfrentar el desafío de fallos combinados, es decir, cuando múltiples sistemas o tecnologías fallan al mismo tiempo. Para abordar estos escenarios, los enlaces de datos de última generación están diseñados con capacidades avanzadas de gestión de fallos que permiten que los sistemas identifiquen y respondan a situaciones anómalas rápidamente, minimizando el impacto en las operaciones.

LINPRO: referente internacional en procesamiento de enlaces de datos

En el ámbito de la defensa, la necesidad de contar con sistemas de comunicación tácticos más versátiles y eficientes ha impulsado a muchos países a buscar soluciones que permitan una interoperabilidad real entre diferentes plataformas y fuerzas. Las limitaciones de los sistemas tradicionales, estrechamente acoplados a los sistemas de combate (CMS), han dificultado la evolución y adaptación de los protocolos de comunicación, y han incrementado la complejidad para incorporar nuevos estándares. En este contexto, Grupo Oesía, a través de su marca Tecnobit, desarrolló una solución pionera: LINPRO, un procesador de enlaces de datos que ha transformado el panorama de las comunicaciones tácticas a nivel internacional.

Los sistemas de comunicaciones tácticas existentes, integrados directamente en los sistemas de combate, carecían de flexibilidad para actualizar protocolos y no permitían un funcionamiento simultáneo y efectivo de múltiples estándares. Para solucionar esta limitación, Tecnobit-Grupo Oesía apostó por un enfoque radicalmente diferente: crear un procesador de Data Link externo, modular y escalable, que operara de forma independiente al sistema de mando y control (CMS) de cualquier plataforma. Este nuevo diseño permitió que el “core” del sistema fuera reutilizable en diferentes plataformas, ofreciendo interoperabilidad entre

redes y la posibilidad de adaptar sus funcionalidades sin comprometer la seguridad ni la confidencialidad de la información.

En colaboración con la Armada Española, LINPRO (Data LINk PROcessor) nació en el año 2000 como un avance significativo en el procesamiento de enlaces tácticos, basado en la experiencia adquirida con su predecesor CRETA en los años 90. Desde sus inicios, LINPRO integró los estándares Link-11 y Link-16, y evolucionó para incorporar de manera temprana el nuevo protocolo Link-22, junto con JREAP y VMF, lo que lo convirtió en un sistema multi-protocolo de referencia.

Esta flexibilidad y capacidad de actualización ha permitido que LINPRO se despliegue en casi un centenar de unidades en la Armada Española y en las plataformas de multitud de países, incluyendo Países Bajos, Japón, Bélgica, Portugal, Alemania, Suecia, Bulgaria, Arabia Saudí, Reino Unido, entre otros. Su éxito en mercados internacionales exigentes ha posicionado al procesador como una solución líder en interoperabilidad para buques, centros de tierra y aeronaves, gracias a su capacidad para gestionar y reenviar datos simultáneamente entre los principales estándares de enlace.

Experiencia fuera del entorno OTAN

Inspirados por las capacidades avanzadas del sistema LINK-22 de la OTAN, la Armada de Bangladesh identificó la carencia de una solución similar que permitiera conectar y coordinar sus unidades navales, aéreas y estaciones terrestres. De nuevo, **Tecnobit-Grupo Oesía presentó una propuesta innovadora** para satisfacer estas necesidades con un enfoque diseñado a medida.

La solución incluyó un **sistema integral basado en un protocolo propio y de última generación, denominado Openlink**. La propuesta, además de todos los elementos de la cadena de comunicaciones de un Data Link táctico, **incluía un potente cifrador** para proteger tanto la voz como los datos transmitidos, garantizando que la información estratégica permaneciera fuera del alcance de posibles adversarios. En una segunda fase, se ha proporcionado también un sistema completo de gestión de claves integral para todas las plataformas.

Este proyecto **requería la integración de los nuevos sistemas en dieciséis plataformas distintas**, que incluían buques de superficie, submarinos, aviones de patrulla marítima, estaciones de tierra **y la formación de profesionales** para un traspaso efectivo del conocimiento y una puesta en marcha eficiente.

A partir de esta base, **se desarrolló un sistema completo bautizado como Bangla-22, que combinó un procesador de Data Link específico y consolas de operador para facilitar la actividad diaria de la Armada Bangladeshí.** Esta solución completa ha sido diseñada no solo para cumplir con los requerimientos operativos, sino también para ofrecer un margen de crecimiento y adaptación futura, proporcionando a la Armada de Bangladesh de una solución confiable y de alto rendimiento.

Por

Alfredo Muñoz Isla

Responsable del área Tactical Data Links
de Grupo Oesía

oesia grupo

tecnobit grupo oesia cipherbit grupo oesia UAV Navigation grupo oesia inster grupo oesia

grupooesia.com