DICIEMBRE / 2017
Num. 6

railgroup LAB

••• EL PRIMER NEWSLETTER QUE TE EXPLICA LO QUE VA A SUCEDER EN EL SECTOR DEL FERROCARRIL •••

EN PORTADA

Blockchain, otra oportunidad para el sector

Blockchain es una tecnología de transferencia de datos digitales totalmente segura y transparente que se está extendiendo a gran velocidad en todos los ámbitos, incluido **el transporte**. El sistema funciona a partir de la descentralización de los datos, que son segmentados en bloques y en diferentes cadenas y que no se pueden ni modificar ni borrar. Esto ofrece una extraordinaria seguridad, dado que la misma información está multiplicada y repartida en multitud de nodos diferentes, haciéndola inexpugnable a cualquier ciberataque. Pero además, *blockchain* también permite prescindir de cualquier intermediario que quiera avalar, certificar o autenticar una transacción o identificación. La misma cadena de bloques compara la información y la valida automáticamente.

Entre las ventajas inmediatas que ofrece al sector ferroviario está la extrema trazabilidad en el **transporte de mercancías**, la seguridad en la gestión de las operadoras y la eliminación de intermediarios para facilitar la compra digital de billetes o títulos de transporte por parte de los usuarios.

Una de las primeras compañías ferroviarias en desplegar la tecnología han sido **Railway Postal Service**, de la India, y **State Railway of Thailand**. A finales de 2018 ambas controlarán mediante *blockchain* la gestión de los paquetes postales que transportan por sus respectivos países.

••• EL PRIMER NEWSLETTER QUE TE EXPLICA LO QUE VA A SUCEDER EN EL SECTOR DEL FERROCARRIL •••

PRÓXIMA ESTACIÓN

Diálogos de movilidad

Bajo el nombre de **Diálogos de Movilidad**, Railgrup ha impulsado un foro de reflexión sobre los retos que debe afrontar el sector del transporte. El primer encuentro de este foro tuvo lugar en la última asamblea general del clúster y que contó con la participación del presidente de Railgrup y de FGC, Enric Ticó; la directora de Creafutur, Charlotte Bouchette; el presidente del clúster de la industria de la automoción en Catalunya (CIAC), Vicenç Aguilera; y el jefe de innovación de IDIADA, José Manuel Barrios. La moderación del debate fue llevada a cabo por el profesor emérito de la Universitat Politècnica de Catalunya (UPC), Jaume Barceló.
Durante la jornada se lanzaron ideas y reflexiones de alta valor. Así, por ejemplo, se puso de relieve que en poco tiempo la red de movilidad será mucho más importante que el medio utilizado, o que el tren es el medio de transporte mejor valorado, menos contaminante y más seguro, cosa que le sitúa en la pole position de la movilidad sostenible.

Trenes inteligentes

La compañía Great Northern Railway está desarrollando un pionero **sistema de mantenimiento preventivo** en sus trenes. Mediante la instalación de sensores en vías, ruedas y cajas de transmisión, consigue un diagnóstico inmediato del estado de cada tren, de manera que ante cualquier variación relevante, el sistema enviará automáticamente un correo electrónico a los ingenieros responsables del mantenimiento del material rodante. De esta manera, los problemas derivados de desgaste se detectaran meses antes de que tengan ninguna gravedad.
El sistema ha sido diseñado por la compañía Perpetuum, una start-up creada por estudiantes de ingeniería de la Southampton University, y se está implementando en los 40 trenes de Great Northern Railway que operan entre Cambridge y Londres. Los responsables de la compañía están convencidos que con esta tecnología evitarán retrasos derivados de mantenimiento e incluso accidentes.

••• EL PRIMER NEWSLETTER QUE TE EXPLICA LO QUE VA A SUCEDER EN EL SECTOR DEL FERROCARRIL •••

EL EXPERTO

Nombre Tiago Bravo Marques
Perfil Ingeniero jefe en ciberseguridad de Bombardier Transportation. Acumula más de 15 años diseñando y desplegando estrategias de seguridad en redes y operadoras de ferrocarril de la Unión Europea. También ha trabajado en África, Índia y Pakistán.

"Las empresas son conscientes de los *riesgos de seguridad*, pero tienden a ignorarlo"

Este especialista en ciberseguridad en el ámbito ferroviario detalla a Railgrup los principales riesgos y amenazas que afronta el sector. Pero también ofrece la receta a fabricantes y operadoras para minimizar-los hasta niveles tolerables. Si trabajan en el sector rail y quieren estar tranquilos deberían, como mínimo, leer esta entrevista.

Usted es el Ingeniero Jefe en Ciberseguridad de Bombardier. ¿Qué hace exactamente en su trabajo?

TB: Soy el ingeniero principal de seguridad en Bombardier Transportation, Rail Control Solutions (RCS), que es la tecnología ferroviaria que orquesta los movimientos del tren de una manera segura. Mi función se relaciona con la estrategia de seguridad: implementar iniciativas internas de ciberseguridad y desarrollar servicios de seguridad cibernética para las necesidades crecientes de nuestros clientes ferroviarios en esta área.

En Bombardier abordamos los desafíos de seguridad implementando estándares, reforzando sistemas, ofreciendo soluciones de detección y evaluaciones cibernéticas adaptadas al entorno ferroviario. Un ejemplo es el servicio de evaluación de seguridad cibernética, que es parte de nuestra solución integral Bombardier OPTIFLO (por ejemplo, mantenimiento preventivo, gestión de activos e infraestructura, capacitación, etc.). Este servicio ayuda a los operadores ferroviarios a identificar sus amenazas, vulnerabilidades y riesgos, junto con la evaluación de sus controles de seguridad existentes contra los requisitos de estándares industriales. Podemos evaluar las posibilidades reales de ser atacado.

También participo, como representante de Bombardier, en una iniciativa de la UE para definir un estándar / guía de seguridad europea para el ferrocarril, en cooperación con otros proveedores, operadores y proveedores de plataformas. Esperamos contribuir a la alineación y la calidad de la ciberseguridad ferroviaria en Europa.

"La Unión Europea está trabajando en un estándar de ciberseguridad ferroviaria"

¿Cuáles son las principales ciberamenazas que afronta el sector?

TB: Un riesgo evidente es el de los sistemas de cobro de tarifas, que pueden ser vulnerables ya que deben estar en Internet y suelen ser los más expuestos. Pero las nuevas áreas de riesgo proceden del crecimiento de la tecnología ferroviaria cuando no se invierte en contramedidas de seguridad adecuadas.

La transformación tecnológica es positiva, pero al mismo tiempo abre nuevas brechas en los sistemas ferroviarios. Las arquitecturas son más complejas e interconectadas (por ejemplo, IoT), lo que aumenta el número de ataques potenciales. Se usa comunicación por radio que podría abrir la puerta para >>

••• EL PRIMER NEWSLETTER QUE TE EXPLICA LO QUE VA A SUCEDER EN EL SECTOR DEL FERROCARRIL •••

EL EXPERTO

>> ataques desde el exterior. Los protocolos estándar TCP / IP ahora se usan, pero también son conocidos por los piratas informáticos. Los sistemas operacionales (SO) bien conocidos son parte de los sistemas de seguridad y requieren parches frecuentes para corregir las vulnerabilidades. Los nuevos servicios están disponibles para los pasajeros, pero eso requiere segregación de los sistemas de pasajeros y seguridad para evitar la piratería. Estos son los que deben ser los más seguros. Con todo, estos cambios requieren medidas de seguridad adicionales para compensar la mayor exposición a amenazas.
Hoy prevemos una variedad de posibles fuentes de ataques que podrían afectar el negocio ferroviario: organizaciones gubernamentales con gran capacidad para atacar e interrumpir una red ferroviaria por razones económicas o estratégicas y organizaciones criminales que tienen motivaciones típicamente financieras. Además, existe el riesgo asociado a varios otros posibles actores de ataque con diferentes niveles de capacidad y motivación, como hackers, competidores e incluso empleados y pasajeros...

Hace dos años, el BART de San Francisco fue víctima de un ciberataque en el que se solicitaron 100 bitcoins (unos 700.000 euros) como rescate. Ese ataque generó pérdidas cercanas a medio millón de dólares. ¿Pueden repetirse episodios de este tipo?
TB: El riesgo cibernético siempre existirá, pero se puede minimizar a un nivel tolerable para el nivel esperado de amenazas. La industria ferroviaria tradicionalmente era una red cercana con poca exposición a los riesgos cibernéticos y el "bajo apetito" de los atacantes. Incidentes como Stuxnet y el que

"Los nuevos riesgos proceden del crecimiento de la tecnología ferroviaria sin invertir en las contramedidas de seguridad adecuadas"

"Los terroristas saben que los ataques físicos son probablemente una forma más fácil de lograr daños que los ciberataques"

••• EL PRIMER NEWSLETTER QUE TE EXPLICA LO QUE VA A SUCEDER EN EL SECTOR DEL FERROCARRIL •••

EL EXPERTO

"Las empresas son conscientes de los riesgos de seguridad, pero tienden a ignorarlo porque la seguridad tiene un impacto no solo en el coste, sino también en la gestión de las operaciones"

>> mencionan crearon conciencia en el sector sobre los riesgos cibernéticos y la importancia de fortalecer los sistemas ferroviarios. Este es un proceso que lleva tiempo y todavía hay mucho por hacer.

¿Los trenes pueden ser objetivo de los ciberterroristas?
TB: Potencialmente sí, pero el terrorismo está más relacionado con las amenazas de seguridad física que los incidentes cibernéticos. Su objetivo es interrumpir el servicio, y los terroristas saben que los ataques físicos son probablemente una forma más fácil de lograr daños que los ciberataques.

¿Cree que las grandes compañías y las operadoras son conscientes de todos estos riesgos?
TB: Las grandes empresas tienen diferentes niveles de madurez, pero la mayoría de las empresas son conscientes de los riesgos cibernéticos. Sin embargo, las personas en el negocio ferroviario todavía piensan que los sistemas ferroviarios son seguros porque sus redes están cerradas y usan protocolos propietarios. Esto no es del todo correcto. Las redes ferroviarias no están tan cerradas como solían estar y el oscurantismo de los protocolos se ve ahora como una mala práctica de seguridad. Además, el panorama de amenazas ha cambiado en términos de la motivación y la capacidad del actor de la amenaza.
También sucede que las empresas son conscientes de los riesgos de seguridad, pero tienden a ignorarlo porque la seguridad tiene un impacto no solo en el coste sino también en la gestión de las operaciones.

¿Cree que invierten lo suficiente en ciberseguridad? ¿Qué porcentaje de la facturación debería invertir una compañía del sector ferroviario en ciberseguridad?
TB: Hay una escasez de conocimiento y capacidad de seguridad en el negocio ferroviario, pero los tiempos están cambiando y las compañías ferroviarias en los últimos años están incrementando la dotación de personal y la inversión en iniciativas de ciberseguridad. Quizás las empresas aún deberían gastar más en seguridad para superar el retraso tecnológico y organizativo. No solo el porcentaje del presupuesto es importante sino también gastarlo sabiamente de acuerdo con un plan de seguridad razonable.

Algunos expertos señalan que la tecnología blockchain puede ayudar mucho a mejorar la seguridad informática. ¿Qué opina al respecto?
TB: *Blockchain* es un concepto disruptivo con potencial para minimizar los problemas de seguridad en las transacciones financieras, pero también para mejorar la autenticación e integridad de la comunicación de sistemas. Quizás *Blockchain* no es una prioridad en el desarrollo ferroviario, pero nuestros ecosistemas ferroviarios se están volviendo muy innovadores, explorando el uso de IoT y el almacenamiento de datos en la nube. >>

••• EL PRIMER NEWSLETTER QUE TE EXPLICA LO QUE VA A SUCEDER EN EL SECTOR DEL FERROCARRIL •••

EL EXPERTO

>> Posiblemente *blockchain* sea el próximo reto a explorar y a adoptar en firme por la indústria.

¿Qué recomendaciones haría a las empresas del sector, especialmente a las operadoras?

TB: Aconsejaría a las operadoras que construyan una base sólida sobre los estándares industriales ya existentes, también a nivel de país y las directivas de la UE (Agencia NIS y ENISA). Las operadoras son propietarias de activos de riesgo y deben desplegar sistemas de seguridad y gestión de riesgos en sus organizaciones basadas en la serie ISO 27000 o IEC 62443. El nivel de madurez y el compromiso de la organización con la seguridad es un elemento clave para un plan de seguridad efectivo.

En cuanto a la infraestructura, las normas IEC 62443 imponen requisitos a los sistemas industriales y les asignan a niveles de seguridad. Se debe comenzar con una evaluación de riesgos y vulnerabilidades para identificar y clasificar las amenazas y los riesgos y adoptar las contramedidas necesarias para minimizar el riesgo a un nivel tolerable.

La detección de vulnerabilidades y ataques también juega un papel importante, ya que nunca es posible protegerse contra todas las amenazas posibles. Hay innovación en esta área que se puede usar en Rail, por ejemplo, algoritmos de detección de intrusión en el comportamiento. Estos sistemas aprenden cómo se comporta la señalización ferroviaria normalmente y levantan alarmas en caso de un ataque.

En términos de respuesta y recuperación del incidente, es importante estar preparado y capacitado sobre cómo lidiar con incidentes cibernéticos, tanto en el nivel CIRT (equipo de respuesta a incidentes informáticos) como a nivel operativo. Finalmente, es importante que las operadoras ferroviarias trabajen cerca de la entidad que coordina la gestión de incidentes nacionales de ciberseguridad.

"Las empresas aún deberían gastar más en seguridad para superar el retraso tecnológico y organizativo"

"Posiblemente blockchain sea el próximo reto a explorar y a adoptar en firme por la industria"

TICKETS

↓01

Hyperloop, a toda máquina

El ambicioso proyecto de transporte ultrarrápido mediante cápsula de vacío avanza a gran velocidad. Hyperloop One ha recibido con los brazos abiertos a un nuevo inversor, el multimillonario Richard Branson y con experiencia en compañías de transporte aéreo y ferroviario. Esta nueva inyección económica ha disparado el valor de la compañía, que los expertos ya sitúan alrededor de los 700 millones de dólares.

Por su parte, el equipo de ingenieros español surgido en la Universitat Politècnica de Valencia (UPV) ya dispone de un tubo de vacío para probar y mejorar el prototipo con el que están participando en la **competición mundial**.

↓02

Red de innovación

Cien millones de euros. Este es el presupuesto destinado a innovación que tendrá el **UK Railway Research and Innovation Network**, un centro de referencia mundial en investigación ferroviaria que acaba de crear el gobierno británico en colaboración con la Rail Safety and Standard Boards, las empresas privadas de componentes ferroviarios y un consorcio integrado por ocho universidades británicas.

En el centro se investigará en tres ámbitos diferentes: los sistemas digitales, incluyendo el big data, la ciberseguridad y las simulaciones; el material rodante, focalizándose en el ciclo de vida y la optimización y gestión de los trenes; y, finalmente, en la infraestructura.

UKRRIN
UK RAIL RESEARCH AND INNOVATION NETWORK

↓03

Contra la congestión, gamificación

Diferentes ciudades de todo el mundo están experimentando con la gamificación para modificar los hábitos de uso del transporte público de los usuarios. La idea es ofrecer incentivos a los pasajeros a cambio de que se desplacen en horas, líneas o estaciones menos congestionadas para así optimizar la capacidad de la red de transporte.

San Francisco (Estados Unidos), **Singapur** o **Bolzano** (Italia) son claros ejemplos de ciudades que han planteado "juegos" de movilidad a sus usuarios. Los resultados de estas pruebas marcarán hasta qué punto se pueden condicionar las necesidades de movilidad de los usuarios.

PRÓXIMAS CITAS

SHIFT2RAIL & H2020

Jornada internacional de networking ferroviario

Fechas: 12 y 13 de diciembre de 2017
Lugar: Bruselas
+info: aquí

PROGRAMA CPI LOCAL ACCIÓ

Presentación del servicio de Contractación Pública Internacional (CPI)

Fechas: 15 de febrero de 2018
Lugar: Barcelona
+info: aquí

COMISIÓN I+D+I EN STADLER

Reunión de la Comisión de I+D+I de Railgrup en las dependencias de Stadler

Fechas: 27 de febrero de 2018
Lugar: Albuixech, Valencia
+info: aquí

+ INFO