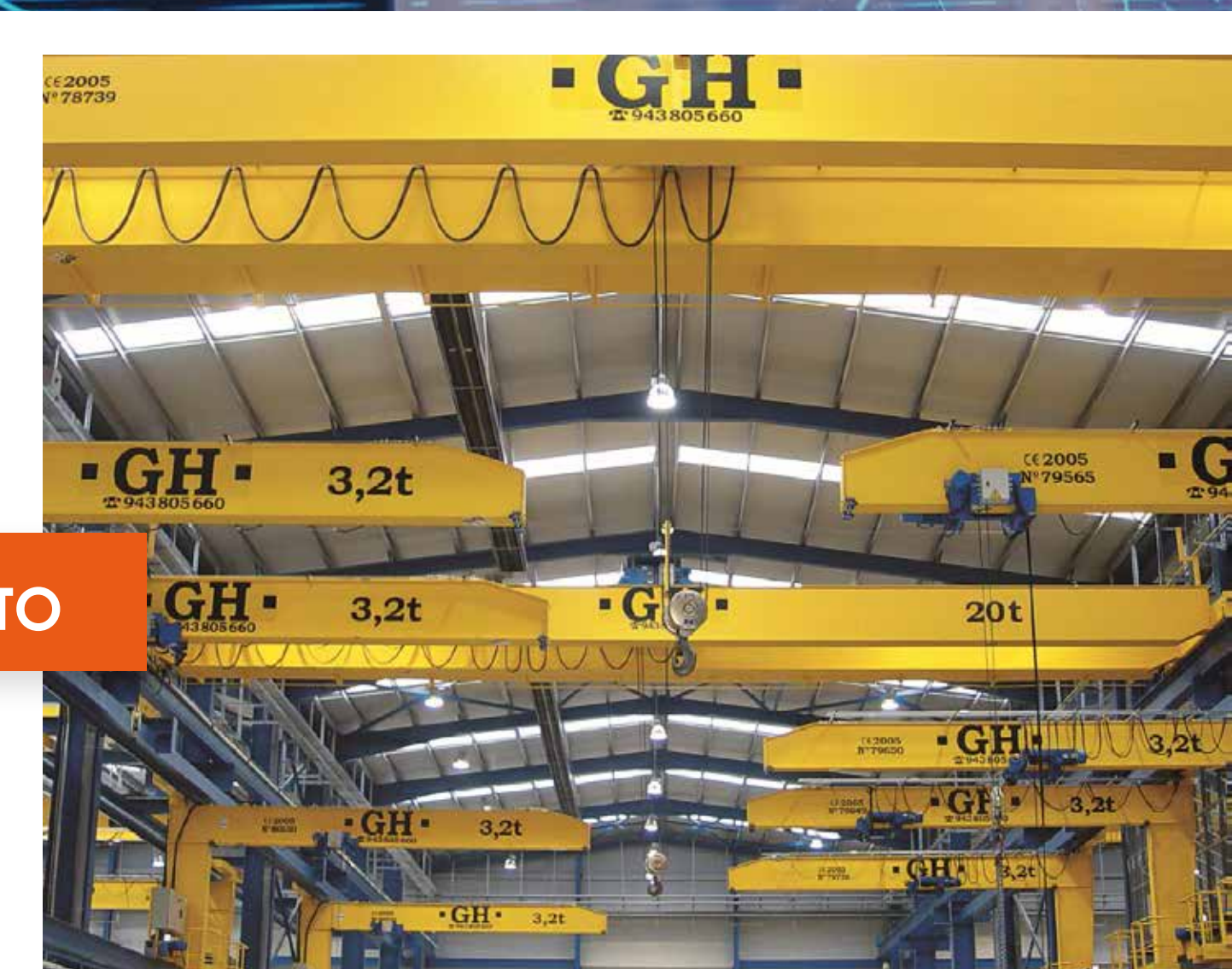


GH Cranes protege sus grúas inteligentes con LAMASSU IoT

La integración de la solución de LKS Next en su sistema **Real Time** permite una **gestión centralizada, trazable y segura** de los dispositivos conectados a lo largo del ciclo de vida

CASO DE ÉXITO



 lamassu IoT
by LKS



EL RETO

GH Cranes & Components es uno de los principales fabricantes mundiales de grúas industriales y soluciones de elevación. Con presencia global y casi 7 décadas de trayectoria, la compañía se especializa en el diseño y producción de grúas puente, pluma, pórticos, polipastos y componentes para sectores industriales clave, tales como la automoción, el sector energético, la siderurgia y la industria naval.

Como parte de su compromiso estratégico con la digitalización, GH Cranes ha desarrollado el sistema Real Time. Dicha plataforma transforma cada grúa en un activo inteligente y conectado, facilitando un nuevo espectro de funcionalidades, entre las que se incluyen la monitorización remota, la implementación de alarmas de seguridad, el análisis pormenorizado del uso y la optimización de las operaciones de mantenimiento del activo.

GH Cranes dispone en la actualidad de **miles de unidades conectadas**.

GH Cranes se encuentra inmersa en el desarrollo de la segunda generación de este sistema. Esta iteración representa una evolución tecnológica significativa, caracterizada por:

- la incorporación de electrónica de diseño propio,
- la provisión de garantías de seguridad superiores
- y una integración más avanzada con el activo gestionado.

Si bien la digitalización de las grúas genera nuevas oportunidades de negocio para GH Cranes, simultáneamente plantea un desafío de naturaleza crítica: **la necesidad de garantizar de forma robusta la seguridad integral y la trazabilidad de cada dispositivo conectado**.

Miles de dispositivos operando a escala global y en contextos diversos presentan un reto de una magnitud significativa. Esta conectividad masiva no solo representaba un **complejo reto** en términos de **gestión**, sino que también introduce **riesgos de seguridad** de considerable magnitud.



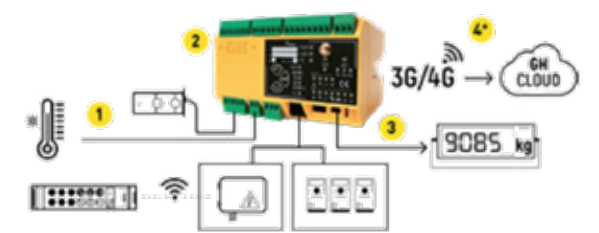
Cualquier vulnerabilidad inherente a uno de estos dispositivos es susceptible de ser explotada, lo cual podría comprometer la integridad del activo principal (la grúa) o, en un escenario más adverso, la totalidad del sistema en el cual dicho activo se integra, como podría ser una línea de producción automatizada o una planta de generación energética.

En consecuencia, resulta imperativo para GH Cranes que la nueva generación del sistema fuese concebida bajo enfoque de seguridad desde el diseño, incorporando las consideraciones de seguridad desde las etapas iniciales tanto para el nuevo desarrollo como para el diseño de las implicaciones de seguridad a lo largo de todo el ciclo de vida del activo, desde la fabricación a la explotación. Esta necesidad se ve acentuada por la exigencia de un entorno normativo cada vez más estricto, marcado por regulaciones como la **CRA (Cyber Resilience Act)** y la directiva **NIS2**.



Frente a este desafío, la infraestructura de clave pública (PKI) se presenta como la solución tecnológica de referencia para proteger ecosistemas de Internet de las Cosas (IoT), proveyendo los mecanismos esenciales de autenticación, confidencialidad e integridad de los datos.

No obstante, la implementación y gestión de sistemas PKI entraña una notable complejidad. Requieren un conocimiento especializado no solo para su despliegue inicial, sino también para su mantenimiento y evolución a lo largo del tiempo, adaptándose a las nuevas amenazas y requisitos operativos. **En el contexto de IoT** esta complejidad se incrementa ya que las peculiaridades del activo obligan a adaptaciones específicas de los procesos de integración con la PKI en función del contexto.



No todas las soluciones PKI están diseñadas para abordar las particularidades y restricciones inherentes a los entornos IoT, como la gestión de dispositivos con recursos limitados o los despliegues masivos en campo.

Es en este contexto donde **Lamassu IoT** aporta un **valor diferencial**, ofreciendo una **plataforma PKI robusta y diseñada** específicamente para las necesidades de los **sistemas IoT**.

La solución de Lamassu proporciona soporte integral durante todo el ciclo de vida del activo. Esto abarca:

- Desde la fase de fabricación, facilitando la inicialización segura del dispositivo.
- Hasta la activación en campo con el primer registro seguro en el sistema.
- Extendiéndose a todos los procesos de mantenimiento y actualización durante su vida operativa, garantizando la seguridad de forma continua.



CONCLUSIONES

- **Máxima seguridad con mínima carga operativa:** equilibrio entre protección avanzada y una gestión lo más desatendida posible.
- **Diseño seguro desde el origen:** recomendamos integrar la infraestructura PKI desde las fases iniciales de diseño del dispositivo, no como añadido posterior.
- **Adaptación normativa asegurada:** nuestra solución está alineada con los requisitos del Cyber Resilience Act (CRA) y otras normativas emergentes.
- **Gestión segura del activo a lo largo de todo el ciclo de vida:** se proporciona una infraestructura para soportar la gestión segura del activo en todas sus etapas, fabricación segura, activación en campo y mantenimiento de la identidad durante la vida activa de del dispositivo.

“La experiencia y el soporte de LKS en la implantación de PKIs para IoT, junto con su solución Lamassu IoT, nos han permitido diseñar y desarrollar nuestros productos conectados con un enfoque integral en seguridad, asegurando la gestión de identidad durante todo su ciclo de vida y el cumplimiento de las normativas europeas vigentes”

José Iraolagoitia

j.iraolagoitia.asesor@lksnext.com