# Una visión IIoT para la automatización de procesos

A medida que la funcionalidad se redistribuye de forma segura en la nube y ambientes periféricos, los sistemas de automatización de procesos actuarán de mejor manera y serán también más fáciles de gestionar y mantener.

Honeywell

La Internet industrial de las cosas (IIoT) tiene el potencial para ser la novedad más influyente y disruptiva en automatización desde el advenimiento de los sistemas de control distribuido (DCS) basados en microprocesadores. Los primeros estilos de arquitectura emergen de la ampliación de IoT, en donde el sensado ubicuo se une al análisis de datos en la nube y a los sistemas de almacenamiento. Si bien estas aproximaciones son ciertamente viables para una amplia clase de soluciones IoT —tales como redes inteligentes y aplicaciones a electrodomésticos de consumo masivo— los sistemas de automatización industrial requieren una aproximación más considerada.

Una diferencia fundamental es que IIoT busca mejorar la operación y gestión de los procesos de producción industriales, muchos de los cuales incluyen reacciones exotérmicas en donde la seguridad es una preocupación fundamental. La seguridad en sistemas basados en IIoT es también un tema de suprema importancia no solo desde la perspectiva de seguridad en sí, sino también en casos de producción de importantes bienes y servicios esenciales y estratégicos. Esto concierne requisitos de seguridad más exigentes, confiables y disponibles, tanto como la capacidad de continuar operando con acceso intermitente a los recursos de Internet. Cuando las fallas ocurran, el sistema debe continuar operando en donde sea posible, de forma adecuada segura y determinada.

## Integración con sistemas existentes

Otra distinción de IIoT es que la fábrica o planta de procesos es un bien de capitales de muy larga vida que requiere soporte a largo plazo de cara a los veloces cambios tecnológicos. Esta realidad requiere soporte para infraestructura y equipamiento existente y que envejece y un medio de proteger las inversiones en propiedad intelectual. Como resultado, muchos dispositivos que formarán parte de IIoT continuarán comunicando a través de protocolos ya existentes, a menudo antiguos, y necesitarán mecanismos especiales para integrarse en un ambiente IIoT más amplio.

Llevar las ideas de IoT a la industria significa reconciliarlas e integrarlas con los sistemas de automatización existentes. De hecho, IIoT es, en espíritu, una extensión de conceptos en los que *Honeywell* fue pionera en la década de 1970 con la introducción del sistema de control totalmente distribuido (sistema de control distribuido TDC 2000, o DCS), un precursor del concepto de "informática periférica" *(edge Computing)* de IoT. Las capas inferiores de un DCS tienden a ser autónomas, responsables del control en tiempo real del proceso, mientras que las capas de superiores se encargan de la supervisión, incluyendo control avanzado e interfaces humano-máquina (HMI) más historial de datos y actividades de planificación y programación

Es tentador comparar directamente el DCS de hoy con el sistema de automatización basado en IIoT del futuro y sostener que IIoT ya está en marcha,

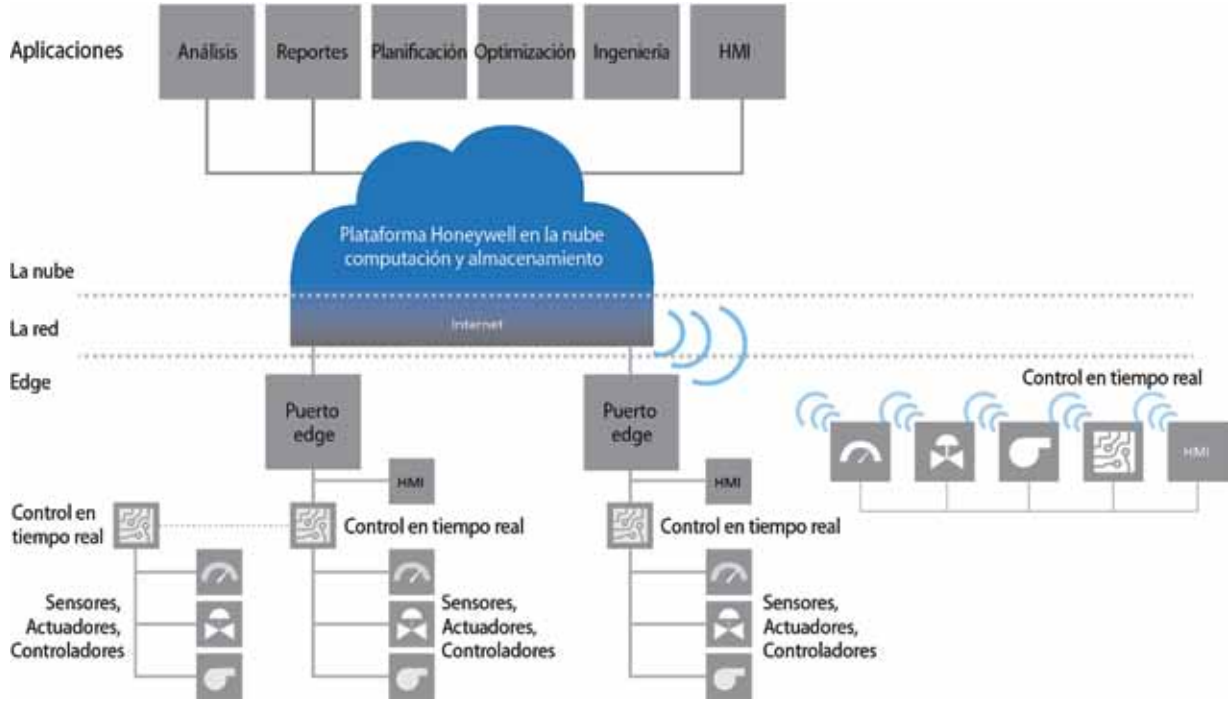



**Figura 1. IIoT surge de la combinación de conceptos nucleares de DCS tales como control de procesos industriales en tiempo real, local, de alta disponibilidad junto con tecnologías y arquitecturas que permiten IoT**


**Figura 2. El típico modelo de Arquitectura de Referencia Empresarial Purdue (PERA) comparado con un modelo de referencia de Internet de las cosas de Cisco, a la izquierda y derecha, respectivamente**

pero eso ignora los cambios significativos del DCS, tal como lo entendemos, que ocurrirán por la introducción de IIoT. IIoT surge de la combinación de conceptos "núcleo" de DCS tales como control de procesos industriales en tiempo real, local, de alta disponibilidad junto con tecnologías y arquitecturas que permiten IoT (figura 1).

Algunas de las diferencias clave entre una arquitectura IIoT y una arquitectura convencional DCS se puede ilustrar comparando ambas arquitecturas en sus niveles más altos (figura 2). La estructura de un DCS y sus aplicaciones asociadas se atienen típicamente a la bien entendida Arquitectura de Referencia Empresarial Purdue (PERA) desarrollada en los '90.

Este modelo abstracto tiene típicamente una realización correspondiente en la topología del sistema en donde los límites entre los niveles se expresan en general como límites de red en los que se puede reforzar la seguridad. La arquitectura IIoT ilustrada en la figura 1 está, en el nivel más alto, separada en dos grandes subdivisiones: la periferia y la nube. Esta estructura se puede dividir en un modelo de siete niveles como muestra la figura 2.

Aplicar una arquitectura IIoT en un proyecto industrial requiere reconciliar estas dos arquitecturas organizacionales diferentes de modo tal que las cualidades arquitecturales clave provistas por el modelo Purdue (seguridad, confiabilidad, eficiencia) se mantengan y mejoren dentro de una estructura basada en IIoT. El nivel 1 del modelo Purdue, "control básico", se muda a la periferia en el modelo IIoT, mientras que el nivel 4, "planificación de negocios y logística", se muda a la nube. Existe también un argumento fuerte para mover mucho del nivel 2, "área de control", a la periferia por cuestiones de rendimiento, seguridad y confiabilidad. La funcionalidad representada en el nivel 3, "operaciones de fabricación", se repartirán entre la nube y la periferia en función del balance de los atributos clave del sistema. Gestión de alarma, *control barch*, control avanzado de procesos e historial son todos ejemplos de funciones que se pueden desarrollar ya sea en la nube, en dispositivos integrados, o en ambos.

Trasladar la funcionalidad ya sea a la nube o a la periferia representa un balance entre un número de cualidades del sistema. Por ejemplo, trasladar la funcionalidad a la periferia puede mejorar el rendimiento y la confiabilidad a expensas de tener que gestionar la funcionalidad distribuida entre una gran cantidad de dispositivos. Por otro lado, trasladar la funcionalidad a la nube facilita la instalación, el escalamiento, las actualizaciones y el retiro a expensas de que la funcionalidad está lejos de los dispositivos y controladores de los que quizá depende. En general, el traslado a una arquitectura basada en IIoT resultará en un sistema sin las restricciones de la estructura jerárquica de un DCS.

## Soporte mejorado para objetivos operacionales clave

La preocupación predominante en cualquier proyecto industrial es la seguridad, para lo cual existe un conjunto bien desarrollado de prácticas y estándares. Por ejemplo, el modelo de nivel de seguridad integridad (SIL) provee una medición cuantitativa de la reducción de riesgo gracias a sistemas instrumentados de seguridad (SIS) que son responsables de la seguridad básica de un proceso y están formalizados en IEC 61511. SIS seguirá teniendo un rol clave en la periferia de cualquier sistema de automatización basado en IIoT.

Una cuestión estrechamente relacionada a la seguridad es la protección, tanto física, como cibernética. A menos que un sistema de automatización esté protegido contra actividad y acceso no autorizados, no se puede garantizar la seguridad. Las operaciones de ciberseguridad requieren una combinación de medidas de protección, comunicaciones inherentemente protegidas y sistemas de monitoreo activos para detectar y mitigar cualquier actividad no autorizada en la red. Además de que prevenir implica la seguridad de la planta, la protección también sirve para proteger la propiedad intelectual inherente a un proceso industrial en sí y los procedimientos de planificación, agenda, ejecución, mantenimiento y optimización de la producción durante el proceso.

Muchos de los componentes existentes de DCS no cuentan con ninguna protección inherente. Por ejemplo, quizá carezcan de cualquier mecanismo de control de acceso explícito y transmitan datos a la red en texto plano.

Tal legado de componentes no desaparece en un sistema basado en IIoT pero se restringe al área de informática perimetral, en donde el acceso se controla de forma estricta. El acceso a componentes DCS, a través de compuertas perimetrales, incluye tanto control de acceso, como comunicaciones protegidas.

Otro aspecto vulnerable en los sistemas de automatización actuales se enraiza en el uso de

plataformas de sistemas abiertos, particularmente en nivel 2 o más alto en el modelo Purdue. Estas plataformas implican riesgos debido a su uso extendido en varios dominios, haciendo bien comprensibles sus vulnerabilidades y problemas asociadas. IIoT ayuda a atender estas cuestiones trasladando la funcionalidad del sistema de automatización ya sea hacia abajo, hacia la informática periférica, o hacia arriba, hacia la nube. La zona de la nube cuenta con un rico control de acceso y mecanismos integrados de protección de las comunicaciones; además, la naturaleza centralizada de la infraestructura la hace mucho más fácil de mantener para que pueda atender los aspectos vulnerables que se descubran.

La confiabilidad general del sistema de automatización puede mejorar llevando las funciones hacia la periferia y hacia la nube. Tal como con la seguridad, las funciones que se trasladan hacia la periferia, especialmente las de control, pueden actuar de forma más autónoma, reduciendo las causas potenciales de fallas. Trasladar las funciones hacia la nube les permite una gestión, mantenimiento y actualización más sencillos. Además, la división entre funciones en la nube o en la periferia permite una gestión más independiente, otra vez, permitiéndole al sistema continuar siendo operativo en varios eventos del ciclo de vida.

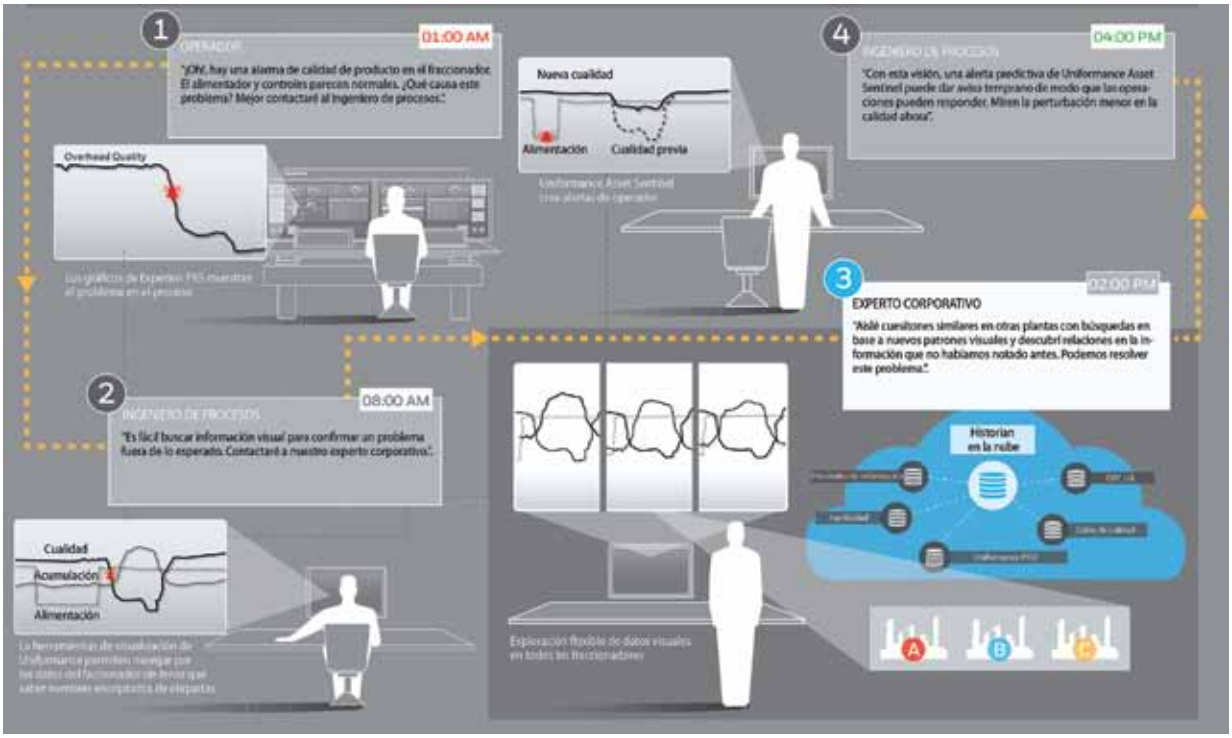
Con un proceso de producción que funciona de forma segura, protegida y confiable, la atención puede concentrarse en hacer a la producción tan eficiente como sea posible a fin de maximizar la rentabilidad de la empresa. La propuesta IIoT puede colaborar para mejorar la toma de decisiones entregando información a tiempo, en el formato adecuado y a la gente (y sistemas) que corresponde, donde sea que estén situados.

La capacidad de juntar más datos desde fuentes no correlacionadas también abre oportunidades de aplicación de análisis de datos, modelado, y técnicas de aprendizaje de máquinas para obtener un panorama más certero acerca del estado actual y futuro de la empresa.

## Llegando de acá a allá

Los beneficios que surgen de patrones de implementación nuevos y altamente escalables, dispositivos más inteligentes, análisis y recolección de datos más comprehensivos, y acceso ampliado a través de aplicaciones móviles son significativos. Sin embargo, alcanzar estos beneficios requiere una transición organizada del sistema de automatización de hoy, hacia el sistema de automatización del futuro. A medida que avanza la industria, necesitaremos considerar los siguientes aspectos clave:

- Preservación de la propiedad intelectual: muy comúnmente los clientes vierten en sus sistemas de automatización una gran inversión de propiedad intelectual e ingenieril. Las estrategias de control, aplicaciones de supervisión y gráficos de operador deben preservarse en la medida que evoluciona el sistema. La reingeniería de todo esto es costosa y agrega poco valor. Es mucho mejor preservar esta inversión ya sea proveyendo soporte para estos ítems en su forma actual o proveyendo un traslado de alta fidelidad a nuevas formas.
- Preservación del equipamiento in situ: junto a la ingeniería de un sistema de automatización existe una enorme cantidad de equipamiento asociado. Cambiar y reemplazar algo es poco factible o muy costoso, de modo que es imperativo que la evolución de IIoT se adapte a los sistemas existentes. Una estrategia clave acá es proveer soporte a los protocolos de comunicación existentes, que permita que el equipamiento se integre en la arquitectura IIoT de una forma segura.
- Mantener la seguridad: las calificaciones SIL establecidas para equipamiento y sistemas en un sistema de automatización son centrales para mantener operaciones seguras. Cualquier cambio hacia nuevo patrones y nuevos dispositivos debe mantener los niveles SIL. Por supuesto, lo mismo aplica para mantener las operaciones seguras. En ambos casos, la evolución del




**Respuestas rápidas a los problemas más difíciles: la calidad de producto y la confiabilidad en una planta de proceso impactan en la rentabilidad de una empresa. *Uniformance Suite*, de *Honeywell*, en la nube y con análisis avanzado, permite descubrir rápidamente la raíz de un problema y desplegar rápidamente una solución de monitoreo predictivo online.**

sistema debería ser vista como una oportunidad para, no solo mantener los niveles de seguridad y protección, sino también mejorarlos mucho más allá de sus niveles actuales.

» Actualizaciones durante el proceso: como se introducen cambios en un sistema, estos deben efectuarse de modo tal que no interrumpan o comprometan la producción de planta. Las actualizaciones y mejoras de software y hardware deberían hacerse 'durante el proceso'.

» Rendimiento de sistemas existentes: IIoT alienta la recolección de mayor cantidad de datos desde más fuentes. Mientras que más datos alimentan de información para análisis, debe gestionarse el impacto de esta crecida en la demanda de datos en los componentes existentes del sistema de automatización. No tiene mucho sentido permitir nuevas aplicaciones si sus necesidades comprometen la misión "núcleo" del sistema de automatización.

La buena noticia es que las soluciones de proceso de *Honeywell* tienen una larga historia en exactamente este tipo de evolución en el sistema. La evolución de *TDC 2000* a *TDC 3000* y a *Experion Process Knowledge System* demuestra la capacidad de la empresa para instituir cambios arquitecturales significativos en los sistemas de automatización considerando a la vez los principios clave delineados más arriba. Esta evolución continúa como *Experion PKS* y evoluciona hacia IIoT.

Desde muchos puntos de vista, IIoT representa un "país sin descubrir", lleno de promesas pero esperando a que alguien lo explore y pueda hacer un mapa.

La visión de IIoT de *Honeywell* es una nueva forma de arquitectura de sistema de automatización que equilibra los beneficios de ciclo de vida y computacionales de procesamiento en la nube con la premisa de aplicar habilidades necesarias para proveer seguridad, protección y automatización de larga duración para procesos y sistemas de fabricación complejos. ❖