Artículo de Investigación. Revista Ciencia e Ingeniería. Vol. 38, No. 3, pp. 209-214, agosto-noviembre, 2017.
ISSN 1316-7081. ISSN Elect. 2244-8780. Universidad de Los Andes (ULA)

IIoT y sistemas de control: oportunidades, desafíos y arquitecturas

IIoT and control systems: benefits, challenges and architectures

Toro, Andy*; Sánchez, Gustavo; Strefezza, Miguel y Granado, Ernesto
Universidad Simón Bolívar. Caracas, 1080, Venezuela
*andytorom@gmail.com

Resumen

El impacto que tendrá en todos los ámbitos el Internet Industrial de las Cosas (IIoT) no puede ser menospreciado. Algunos pronósticos estiman que el número de objetos conectados pudiera alcanzar en 2020 la cifra de 50×10^9*, generando un ROI (Retorno de Inversión) de* 300×10^9\$ *para las empresas que decidan adoptar esta tecnología en sus operaciones. Basta con revisar las principales páginas Web de actualidad tecnológica para constatar que la literatura sobre el tema viene creciendo aceleradamente, lo cual dificulta el análisis del fenómeno. Para intentar aclarar algunos conceptos, en este artículo se presenta un análisis de las oportunidades, amenazas y posibles arquitecturas de los sistemas de control en el contexto del IIoT. En líneas generales, el objetivo consiste en identificar los factores más importantes a considerar y orientar a los posibles usuarios a tomar las mejores decisiones con respecto a su implementación.*

Palabras clave: internet industrial de las cosas, sistemas de control basados en internet, sistemas de control basados en redes.

Abstract

It is difficult to overestimate the impact of Industrial Internet of Things (IIoT). Several authors estimate the number of connected objects in 2020 by 50×10^9*, generating a* 300×10^9\$ *ROI (Return on Investment) for companies implementing these technologies. Moreover, the number of publications on this subject is growing fastly, and hence, it is becoming difficult to understand the phenomenon accurately. In this paper, IIot benefits, challenges and architectures are considered within the framework of control systems. Our goal is to highlight the main issues to consider for potential users.*

Key words: industrial internet of things, control systems.

1 Introducción

El objetivo de un sistema de control consiste en garantizar que un determinado proceso se ejecute de acuerdo con un plan preestablecido, cumpliendo un conjunto de restricciones físicas, lógicas y económicas.

Los primeros sistemas industriales de control automático se caracterizaban por incluir únicamente elementos no compartidos: controlador, sensor y actuador (p.ej. lazo regulador de velocidad de Watts mostrado en la Figura 1). Estos elementos eran considerados parte integral del proceso controlado y prácticamente no hacía falta considerar los retardos introducidos por ellos mismos.

Posteriormente, el desarrollo tecnológico hizo posible que un mismo dispositivo pudiera ser compartido por varios lazos, ubicados en general a corta distancia entre sí (control compartido). Los elementos del lazo pudieron ser interconectados a través de una red de tipo LAN (Local Area Network), constituyendo lo que se conoce hoy en día como *Sistemas de Control Basados en Red* (SCBR).

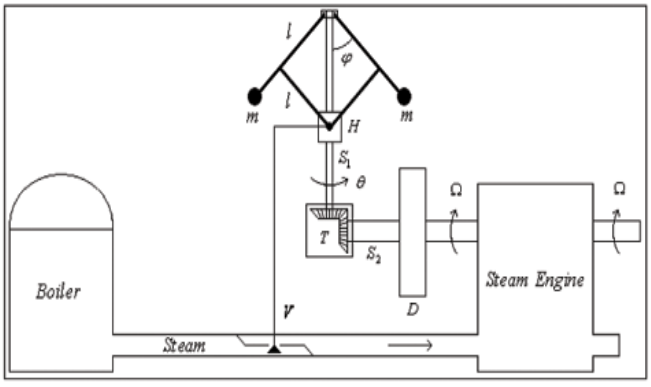

Fig. 1. Lazo regulador centrífugo de Watts

El principal beneficio de este desarrollo consistió en una drástica reducción en los costos de cableado y mantenimiento. Por otra parte, comienza a observarse en las empresas de manufactura la integración de las redes de control con las redes de información a lo largo de la pirámide CIM (Computer-Integrated Manufacturing), representada en la Fig.2. Esta integración permitió adicionalmente mejorar la planificación y el seguimiento de la producción, tomando en cuenta la información en tiempo real obtenida directamente de los lazos de control (Jones y col., 1986).

Uno de los primeros protocolos industriales propuestos para la comunicación entre diversos elementos de un lazo de control fue MODBUS, creado en 1979 por la empresa MODICON. Posteriormente, numerosos protocolos han sido propuestos, con distinto grado de complejidad y prestaciones, tales como: Interbus, Profibus, Foundation Fieldbus, EtherCAT, Profinet y muchos otros (Wilamowski, 2011).

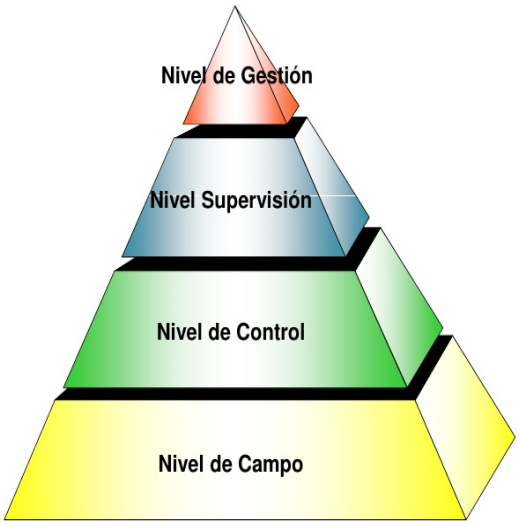

Fig. 2. Pirámide CIM

Desde el punto de vista teórico una de las primeras referencias acerca del estudio de los SCBR aparece en los trabajos publicados durante la década de 1980 por el Dr. Asok Ray y sus colaboradores (Alevi y col., 1990). En dichos trabajos se analizan los problemas típicos del sistema integrado de comunicación y control tales como el retardo en la transmisión, la pérdida de datos y la sincronización, los cuales pueden degradar severamente el desempeño de los lazos (Tan y col., 2016).

Para disminuir el impacto de estos problemas, se han propuesto numerosos procedimientos específicamente adaptados para el diseño y operación de SCBR (Naghshtabrizi, 2016). Uno de los primeros fue publicado en (Luck y col., 1990), en donde se propone un observador/predictor para estimar el retardo y posteriormente compensarlo mediante el cálculo de una señal de control adecuada. Más recientemente un enfoque similar que considera índices de desempeño robusto fue presentado en (Liu y col., 2015).

A partir del desarrollo de Internet, los dispositivos ubicados fuera de la LAN adquieren la capacidad de comunicarse remotamente y compartir información con dispositivos de otras marcas y modelos (inter-operabilidad). Comienza a hablarse entonces de *Sistemas de Control Basados en Internet* (SCBI), que pueden ser definidos como SCBR que utilizan Internet como plataforma de comunicaciones (Yang, 2011).

Recientemente, el siguiente paso en esta evolución, recibe el nombre de *Internet Industrial de las Cosas* (IIoT por las siglas en inglés de Industrial Internet of Things) refiriéndose al conjunto de tecnologías que permiten que la conectividad de Internet se extienda a dispositivos industriales, facilitando el intercambio de información entre los mismos y con usuarios humanos.

El impacto de este fenómeno es difícil de menospreciar. Algunos pronósticos estiman que el número de objetos conectados (sin limitarse al entorno industrial) pudiera alcanzar en 2020 la cifra de 50×10^9, generando un ROI (Retorno de Inversión) de $300 \times 10^9\$$ para las empresas que decidan adoptar esta tecnología en sus operaciones (Ma y col., 2016). Sin embargo, la influencia de la implementación de IIoT va mucho mas allá y abarca desde mejoras puntuales en la vida cotidiana de un individuo (transporte, alimentación, servicios públicos, atención médica, etc.) hasta cambios radicales a nivel planetario.

Se predice, por ejemplo, que esta tecnología contribuirá con la disminución de los requerimientos de energía y recursos naturales del planeta. Organismos como el World Economic Forum, predicen que en los próximos años, el IIoT modificará de manera significativa el desempeño de las industrias manufacturera, de energía, de agricultura y de transporte, entre otras, afectando a más del 60 % de los sectores de la economía mundial (World Economic Forum, 2015). Otros autores como (Wollschlaeger y col., 2017) se refieren incluso al comienzo de la cuarta revolución industrial y utilizan la expresión *Industria 4.0* .

Basta con revisar las principales páginas Web de actualidad tecnológica para constatar que la literatura sobre el tema viene creciendo aceleradamente, lo cual dificulta el análisis del fenómeno. Para intentar aclarar algunos conceptos, en las siguientes secciones se presenta un análisis de las oportunidades (sección 2), amenazas (sección 3) y posibles arquitecturas (sección 4) de los sistemas de control en el contexto del IIoT. En líneas generales, el objetivo consiste en identificar los factores más importantes a considerar y orientar a los posibles usuarios a tomar las mejores decisiones con respecto a su implementación.

2 Oportunidades del IIoT para sistemas de control

La conexión a Internet de una enorme cantidad de dispositivos conlleva a la generación de grandes volúmenes de datos, los cuales contienen información valiosa esperando

ser aprovechada. Una de las principales aplicaciones del IIoT consiste en la capacidad para supervisar una planta desde cualquier ubicación en el planeta usando un navegador Web convencional. Por ejemplo, sería posible verificar la evolución de las variables de un proceso ubicado físicamente en Caracas utilizando una tableta o teléfono móvil conectado desde Beijing, lo cual facilitaría las tareas cotidianas de operación.

Desde el punto de vista del mantenimiento, un sistema permanentemente supervisado, aprovechando la infraestructura IIoT, permitiría la detección y el pronóstico de anomalías (maquinaria, instrumentos y equipos) de forma temprana, confiable y económica. La empresa multi-nacional pudiera concentrar sus especialistas en una localidad, disminuyendo costos de traslado y viáticos. Éstos pudieran dar asistencia remota a otros operadores con menor experiencia presentes físicamente en cada planta: los beneficios son evidentes en el caso de empresas cuyos activos se encuentran distribuidos en sitios distantes geográficamente.

Desde el punto de vista de la producción, los responsables de la misma pudieran modificar su planificación en menor tiempo, adaptándose a variaciones en la demanda o en función de acciones de la competencia. Otras aplicaciones relevantes se relacionan con el seguimiento de la logística de distribución, el manejo del tiempo de vida de productos, la medición del desempeño de procesos, seguimiento de las condiciones y el estado de sus pedidos por parte de los clientes, etc (Breivold y col., 2015).

En general, el análisis inteligente de las diversas bases de datos ahora disponibles (tanto internas como externas a la empresa) permitiría la optimización en tiempo real de las operaciones, por ejemplo mediante la detección de correlaciones antes ocultas entre las variables y la ejecución de las acciones más adecuadas en cada instante.

3 Obstáculos y potenciales riesgos del IIoT para sistemas de control

Existen numerosos obstáculos y potenciales riesgos para las empresas que decidan implementar sistemas de control basados en el IIoT. En primer lugar la mayoría de los SCBR operan sobre redes cuyos elementos son todos operados por la propia empresa, lo cual garantiza la confiabilidad del sistema de comunicaciones. Internet, por el contrario, es un recurso público compartido, con usuarios transmitendo y recibiendo datos de forma simultánea. La ruta de transmisión entre dos equipos no es fija y pueden generarse atascos en el tráfico de datos (Cardwell y col., 2000).

Un reto particularmente importante es el de la seguridad de la información transmitida, pues es posible que un tercero, terrorista cibernético (*hacker*), pueda interceptarla y usarla para cometer algún delito. El hecho de que múltiples usuarios puedan acceder a un servicio genera incertidumbre acerca de quiénes son y dónde se encuentran realmente. Es posible además que múltiples usuarios autorizados pueden tratar de controlar simultáneamente un parámetro en particular, lo que requiere un mecanismo para resolver los problemas de conflicto y coordinar las diversas solicitudes.

Por otra parte, el incremento de la complejidad de las operaciones conlleva a la necesidad de personal especialmente preparado, lo cual debe tenerse en cuenta con suficiente antelación. En la Tabla 1 se presenta un resumen de las oportunidades y obstáculos asociados al IIoT.

El tema de la seguridad e integridad de los datos puede ser atacado a través del uso de protocolos creados para trabajar en redes no confiables, lo cual incluye encriptación de los datos y autenticación de los usuarios. Entre estos se encuentran AMQP (Advanced Message Queuing Protocol) y MQTT (Message Queue Telemetry Transport), protocolos diseñados para la comunicación con dispositivos con poca capacidad de cómputo (Cardwell y col., 2000).

Para los problemas de retardo y pérdida de datos se han planteado soluciones como TSN (Time Sensitive Networks) en las cuales se incrementa la prioridad para la entrega de datos correspondientes a información considerada crítica (ElKalam y col., 2016).

Otra posibilidad consiste en la infraestructura denominada *fog computing* que consiste en el uso de servidores ubicados los más cerca posible al sitio donde se encuentran instalados los sensores y actuadores, al contrario de lo que sucede con la conocida como *cloud computing*. Esta misma solución permite manejar el problema de la escalabilidad cuando se incrementa el número de dispositivos conectados (ver Figura 3). Algunos autores consideran que como consecuencia de estas nuevas arquitecturas, ya sea *cloud* o *fog*, el modelo piramidal clásico se ha *difuminado* dando paso al concepto de automatización como servicio (Hegazy, 2015).

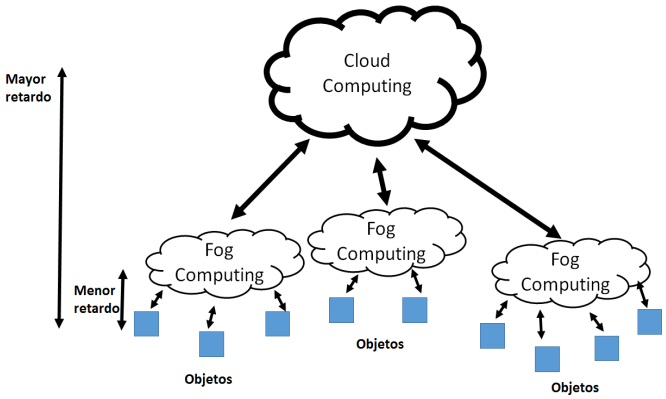

Fig. 3. Cloud computing vs Fog computing

Para garantizar la confiabilidad del sistema de control, en algunos casos es conveniente considerar redundancia, tanto en servidores, controladores, sensores, e incluso redes. Un sistema de control local independiente puede activarse en caso de emergencias o cuando el retardo en la comunicacón

Tabla 1. Oportunidades y Retos de IIoT para sistemas de control

Oportunidades	Retos
Supervisión de dispositivos distantes geográficamente	Mantener la seguridad, confiabilidad integridad y privacidad de los servicios
Disminución de costos de implementación, operación y mantenimiento	Garantizar desempeño de los lazos
Disminución del consumo de energía y recursos naturales	Escalabilidad e interoperabilidad de los servicios
Optimización de procesos en tiempo real. Mejores decisiones	Garantizar la compatibilidad con dispositivos actualmente operando

sobrepasa el máximo permitido. Note que el problema de seguridad funcional de los sistemas instrumentados seguirá siendo específico de cada línea de producción.

La creación de un estándar IIoT es fundamental para que los dispositivos de distintos fabricantes puedan entenderse entre sí, más allá de la selección del mismo protocolo de información. Lamentablemente no pareciera estar cerca la definición del mismo, debido a la diversidad de fabricantes y usuarios con visiones y requerimientos súmamente diversos.

La compatibilidad con los dispositivos actualmente en operación, también constituye un reto a considerar. El uso de máquinas virtuales puede ser suficiente, pero en general cada caso requiere una solución particular, que puede llegar incluso al remplazo total del sistema obsoleto.

4 Arquitecturas del IIoT para sistemas de control

La arquitectura básica de un SCBR se muestra en la Figura 4. En la misma es posible apreciar la presencia de codificadores y decodificadores, los cuales sirven de interfaz entre el proceso controlado y el sistema de control. Comúnmente estas funciones pueden ser realizadas por un mismo equipo denominado "*gateway*".

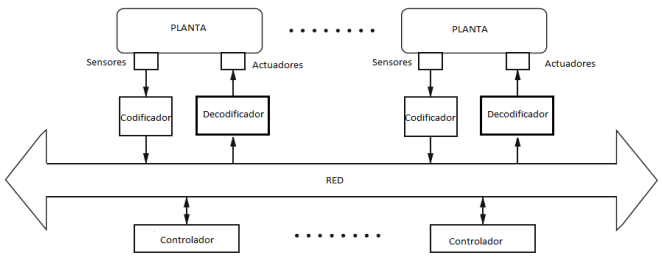

Fig. 4. Arquitectura general de un SCBR

En el caso de los SCBI, los diferentes esquemas para su implementacón se diferencian por la ubicación del controlador y el modo de utilización de Internet. El primero de estos esquemas, ver Figura 5, utiliza un solo controlador ubicado localmente. Dado que el lazo cerrado no depende de Internet, la estabilidad no es afectada por los problemas de transmisión.

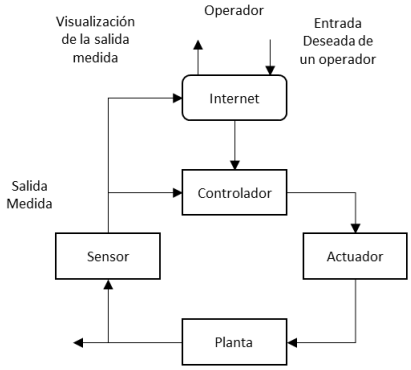

Fig. 5. Esquema de control local - supervisión remota

En el siguiente esquema, ver Figura 6, el controlador se ubica de manera remota, lo cual requiere que la información de campo y la acción de control se envíen a través de Internet. En este caso los retardos asociados a la transmisión si afectan la estabilidad del lazo.

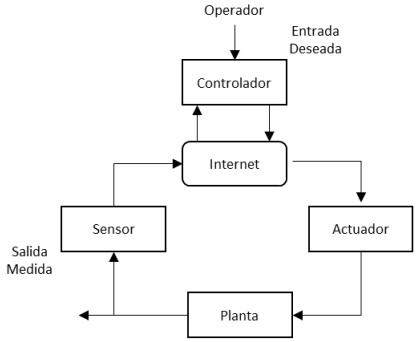

Fig. 6. Esquema de control y supervisión remota

Una tercera configuración utiliza dos controladores, uno local que puede ser usado por ejemplo para asegurar la

estabilidad y seguridad de la planta y otro remoto usado para optimizar la referencia del lazo. Este esquema es mostrado en la Figura 7 y en la Tabla 2 se muestra una comparación entre los distintos esquemas.

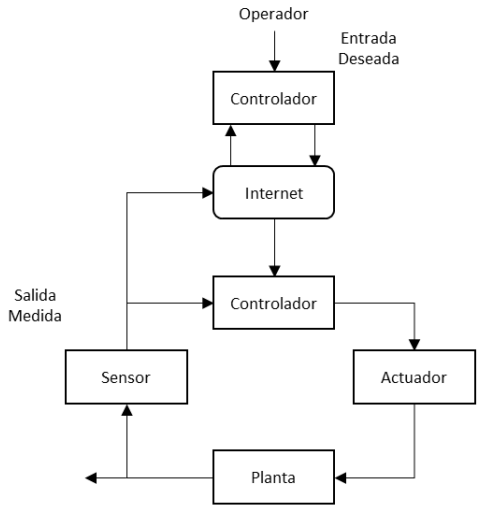

Fig. 7. Esquema de control bilateral

En (Cardwell y col., 2000) se ilustra el funcionamiento del SCBI mediante un *diagrama de eventos de control de procesos* como el que se muestra en la Figura 8. El modelo propuesto por estos autores está constituido por seis capas denominadas: Operador, Interfaz Web de Usuario, Internet, Computador Local, Sensores/Actuadores y Proceso. Note que otros autores prefieren diferentes nomenclaturas (Voas, 2016).

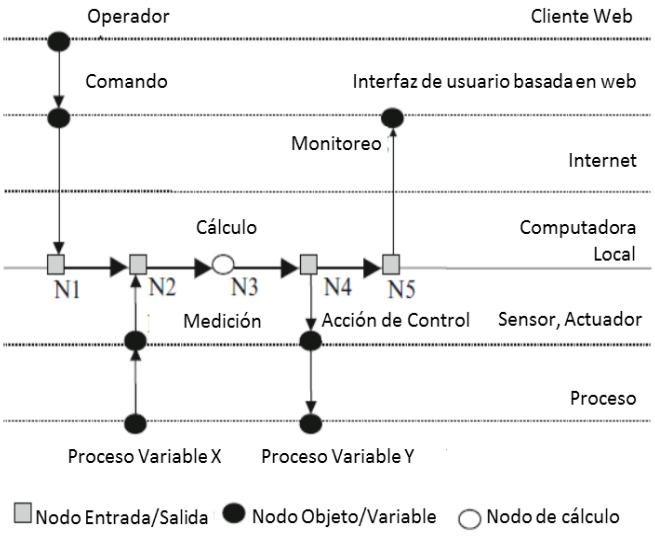

Fig. 8. Diagrama de eventos de control de procesos

El diagrama de la Figura 8 permite entender la secuencia de interacción entre el operador y el sistema de control a través de la arquitectura IIoT: el usuario introduce un comando mediante la Interfaz Web de Usuario y el mismo es llevado al Computador Local. Allí se ejecutan los cálculos de la ley de control en función de la información recibida de los sensores. Posteriormente se envía una orden al actuador y una respuesta, nuevamente a través de Internet, que permite actualizar el resultado en la Interfaz Web de Usuario. Para llevar esta secuencia a la práctica es necesario instalar y configurar un conjunto de elementos, tanto de hardware como de software, para lo cual existe una enorme diversidad de opciones, desde las más sencillas y económicas hasta las más sofisticadas y costosas.

La mayoría de fabricantes de equipos de automatización industrial han incluido la capacidad de conexión a Internet en sus productos de hardware y software. El fabricante Siemens, es capaz de conectar sus controladores PLC con Internet mediante su plataforma *MindSphere*. Otros fabricantes como General Electric, National Instruments, Schneider, Sun Microsystems, Cyberonix, Foxboro, Valmet, Emerson, Honeywell y muchos otras también han presentado productos similares.

Sin embargo, a pesar de los diferentes esfuerzos aún no se ha logrado establecer modelos de funcionales y de arquitectura que permitan la interoperabilidad entre distintos fabricantes. Estos puntos fundamentales, para los cuales aún no hay respuestas convincentes, seguirán captando el interés de los investigadores.

5 Conclusiones

En este artículo se describieron algunas oportunidades, desafíos y posibles arquitecturas de los sistemas de control en el contexto del IIoT. En cuanto a las oportunidades destaca la posibilidad para que las empresas incrementen su eficiencia operacional y mejoren su imagen de marca ante sus clientes.

En cuanto a los riesgos o dificultades destacan los problemas de seguridad tanto de datos como de operaciones, los problemas de comunicación y la falta de compatibilidad entre dispositivos de diferentes fabricantes o heredados. También se analizaron algunas estrategias que pudieran adoptarse para disminuir el impacto de los problemas antes descritos.

Finalmente se presentaron las posibles arquitecturas de SCBI, clasificadas en función de la ubicación del controlador y el modo de utilización de Internet. Note que en el fondo lo más relevante consiste en comprender las implicaciones del momento de transición que vivimos actualmente, hacia un modelo de sociedad en la cual los individuos y las organizaciones disponen de mucha más información para la toma de decisiones, lo cual lamentablemente conlleva una serie de riesgos y obstáculos que deben considerarse cuidadosamente.

Como continuación de este trabajo los autores se proponen profundizar en algunos de los problemas teóricos y metodológicos anteriormente esbozados, abordando en particular

Tabla 2. Arquitecturas de SCBI

Controlador Local	Controlador Remoto	Controladores Bilaterales
La estabilidad y seguridad no depende de los retardos de Internet. Es el esquema convencional actualmente aplicado	Los retardos asociados a Internet si afectan la estabilidad del lazo. Es más económico dado que no existe controlador local	Los retardos asociados a Internet no afectan la estabilidad del lazo. Es el esquema más costoso puesto que requiere redundancia de controladores

el tema de servicios en la nube tales como aplicaciones para la gestión del desempeño de los sistemas automatizados.

Referencias

Alevi Y, Ray A, 1990. Performance analysis of integrated communication and control. Journal of Dynamic Systems, Measurement and Control, vol. 112, pp. 3685-371.

Tan C, Zhang H, 2016. Necesary and Sufficient Stabilizing Conditions for Networked Control Systems with Simultaneous Transmission Delay and Packet Dropout. IEEE Transactions on Automatic Control.

Naghshtabrizi P, Hespanha J, 2011. Implementation Considerations for Wireless Networked Control Systems. Wireless Networking Based Control, Springer, pp. 1-27.

Luck R, Ray A, 1990. An Observer-based Compensator for Distributed Delays. Automatica, Vol. 26. No. 5, pp. 903-908

Liu L, Liu X, Xu C, 2015. Delayed Observer-based Hinf Control for Networked Control Systems. Neurocomputing.

Yang S, 2011. Internet-based Control Systems, Design and Applications, Londres. Springer.

Breivold H, Sandstrom K, 2015. Internet of Things for Industrial Automation - Challenges and Technical Solutions. IEEE International Conference on Data Science and Data Intensive Systems, Sydney.

World Economic Forum, 2015. Industrial Internet of Things: Unleashing the potential of connected products and services.

Cardwell N, Savage S, Anderson T, 2000. Modeling TCP latency. Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Vol 3. p 1742-1751

Ma H, Liu L, Zhou H, Zhao D, 2016. On Networking of Internet of Things: Explorations and Challenges. IEEE Internet of Things Journal, vol. 3, no. 4, pp. 441-452

Voas J, 2016. Demystifying the Internet of Things. Computer, vol. 49, no. 6, pp. 80-83

Wilamowski M, Irwin D, 2011. Industrial communication systems. CRC Press.

Jones A, McLean A, 1986. A proposed hierarchical control model for automated manufacturing systems. Journal of Manufacturing Systems. Volume 5, Issue 1, Pages 15-25

Hegazy T, Hefeeda M, 2015. Industrial Automation as a Cloud service. IEEE Transactions on Parallel and Distributed Systems. Volume 26, Issue 10, Pages 2750 - 2763

El Kalam A, Ferreira A, Kratz F, 2016. Bilateral Teleoperation System Using QoS and Secure Communication Networks for Telemedicine Applications. IEEE Systems Journal. Year: 2016, Volume: 10, Issue: 2

Wollschlaeger M, Sauter T, Jasperneite J, 2017. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. IEEE Industrial Electronics Magazine, Volume: 11, Issue: 1. Pages 17-27

***Recibido**: 26 de enero de 2017*

***Aceptado**: 20 de junio de 2017*

Toro, Andy: *Ingeniero de sistemas, MBA, estudiante del Doctorado en Ingeniería de la USB, fundador y director de la empresa INGEDACA C.A.*

Sánchez, Gustavo: *Consultor, investigador y docente en las áreas de Optimización y Control. Especialista en proyectos de diseño, instalación y mantenimiento de sistemas de control. Experto en Machine Learning y Ciencia de Datos. Correo electronico: gsanchez@usb.ve*

Strefezza, Miguel: *Obtuvo el grado de Doctorado en Muroran Institute of Technology, Japón en 1994. Su investigación está dirigida al área de control y a la aplicación de lógica difusa y redes neuronales a sistemas de control y en mantenimiento. Correo electronico: strefeza@usb.ve*

Granado, Ernesto: *Profesor Titular del Departamento de Procesos y Sistemas de la Universidad Simón Bolívar. Entre sus áreas de interés están los sistemas de comunicaciones industriales y el uso de nuevas tecnologías para la mejora del proceso enseãnza/aprendizaje. Correo electronico: granado@usb.ve*