Sistemas de control industrial y riesgos

Caminar por la calle debería ser suficiente para darse cuenta del afán de los humanos por controlar todo. El tiempo, el clima, la calidad del aire, el numero de plazas en el parking de debajo de tu casa. Está por todos los lados. En las farmacias, en los escaparates de tu tienda de ropa o en el bar con tus amigos. Y lo cierto es que todo este control tiene un sentido. El control nos ayuda a comprender nuestro entorno, y por consiguiente predecirlo. Esto es algo que el ser humano no ha tardado mucho en darse cuenta, ya que la intención de controlar nuestros alrededores se remonta muy atrás, pero es actualmente cuando más controversia. Ante el control que el gobierno quiere imponer a los ciudadanos, estos se revelan para proteger su privacidad. Y siempre es por lo mismo, el afán de controlar y predecir. Este control también se extiende al mundo de la empresa y de la industria. Sería ideal controlar todas las variables que pueden inferir en el negocio, pero entran en juego dos variables que limitan este sueño: el tiempo y los recursos. Por ello, es cada vez más importante saber gestionar estos recursos e identificar las variables más importantes a controlar.

Antes de comprender el presente, intentemos comprender el pasado. Uno de los primeros mecanismos de control, se cree que fue un antiguo reloj de agua Ktesibios en Alejandría, Egipto. Sin embargo, se considera que el *boom* de los sistemas de control industrial se inicio a medidos del siglo XVIII. Fue a finales de siglo cuando realmente se avanzó en la industria y campos específicos notaron considerables mejoras. En la industria naval, por ejemplo, se permitió la construcción de barcos más grandes gracias a la invención de los servomecanismos o servomotor. A mediados de 1950, empiezan a aparecer lo que conocemos como sistemas de control modernos. Los ingenieros se dieron cuenta de que las mediciones reales contienen errores y están contaminadas por el ruido, por lo que empezaron a aparecer nuevas formas de medir. Emergen también los PLC, o los controladores lógicos programables y términos como SCADA (*Supervisory Control and Data Acquisition*). Automatizar

el control hizo que incrementara muchísimo la producción del sector industrial, pero de la misma forma que la tecnología y la información trae nuevas oportunidades, trae consigo también nuevos riesgos.

Los sistemas de control industrial se habían convertido en un activos muy fiables. Si bien es cierto que podían tener algún fallo interno, estaban completamente cubiertos en cuanto a los ataques externos se refiere. Sin embargo, los sistemas computacionales no son inmunes a las ciber-amenazas. La entrada del Internet en la industria, se abre un nuevo mundo para los ciberataques. Esto es una grave amenaza, que algunas empresas han sabido identificar mejor que otras, ya que se ha demostrado que un ataque de este tipo puede tener las mismas o peores consecuencias que un ataque físico. Ejemplos muy actuales demuestran la capacidad devastadora con la que cuentan. En esta imagen se muestran los 8 mayores ciberataques del 2016 según Forbes. Los sistemas de control industrial han pasado literalmente de tener cero días de ataques, a tener ataques de día cero.

A medida de que la industria avanza surgen nuevas tecnologías con las que controlar los procesos. Los sistemas de computación en la nube son cada vez más populares en el mundo de la industria, y términos como IIoT o la industria 4.0 están dejando de ser novedosos. El mundo de la industria está viviendo su cuarta revolución hacia un mundo totalmente nuevo, en el que las fábricas son más productivas, más flexibles y más eficientes. La computación en la nube ya es una realidad también en el mundo industrial. Nuevamente vuelven a surgir oportunidades y amenazas. En un mundo tan competitivo, donde se le otorga un altísimo valor a la información y el dato, ¿qué pasa cuando esos datos están en *la nube*? Los sistemas de control se tienen que extender mucho más allá de los límites de la organización.

Ciertamente, como con cada revolución, se plantea un futuro incierto pero ilusionante, donde se permite que el desarrollo y la innovación puedan volver a ser factores determinantes. Sin embargo, tenemos que aprender del pasado y aplicar esas lecciones al presente y al futuro. Innovación y desarrollo y control y seguridad tienen que ir de la mano. Olvidarlo es ser olvidado.

Referencias:
<<JOnline: Security of Industrial Control Systems>>, Acceso el 8 de octubre de 2017, https://www.isaca.org/Journal/archives/2010/Volume-4/Pages/JOnline-Security-of-Industrial-Control-Systems.aspx

<<Industrial Control Systems and Risks>>, Acceso el 8 de octubre de 2017, https://blogs.deusto.es/master-informatica/industrial-control-systems-and-risks/

<<Breaking Down the Risk of Industrial Control Systems Security>>, Acceso el

8 de octubre de 2017,http://www.aberdeenessentials.com/techpro-essentials/breaking-down-the-risk-of-industrial-control-systems-security/

<<Control system>>, Acceso el 8 de octubre de 2017, https://en.wikipedia.org/wiki/Control_system

<<Industrial Control Systems: A Primer for the Rest of Us>>, Acceso el 8 de octubre de 2017, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/industrial-control-systems-a-primer-for-the-rest-of-us.aspx

<<An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity>>, Acceso el 10 de octubre de 2017, https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf

<<8 Major Cyber Attacks Of 2016 [Infographic]>>, Acceso el 10 de octubre de 2017, https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/

<<Industria 4.0>>, Acceso el 10 de octubre de 2017, https://es.wikipedia.org/wiki/Industria_4.0