

# Industrial Control Systems and Risks

## Industrial Control Systems and Risks

Evolución, podríamos describir esta palabra de muchas formas y adjudicarle palabras que pueden hacer referencia a la evolución, como por ejemplo: innovación, futuro, mejorar... pero, hay una concretamente que para mi humilde opinión enfoca de mejor manera la evolución del ser humano, **EL CONTROL**.

La mayoría estaréis extrañados, ya que, normalmente solemos tender a pensar en mejoras y futuro, pero cuanto más evoluciona el hombre más se acentúa su ansia de control. Hemos pasado de preocuparnos por comer y no pasar frío (en la prehistoria) a querer controlar hasta el más mínimo detalle de nuestro entorno, hasta el punto de querer controlar cosas como la naturaleza (el cambio climático sería un buen ejemplo), los animales o incluso a otras personas (podemos crear rasgos de nuestros hijos genéticamente). Cada paso que damos en la evolución significa controlar algo nuevo.

Viendo que el control nos causa una obsesión nerviosa, cabe destacar que las empresas no se quedan atrás, la necesidad de controlar el trabajo lleva mucho tiempo establecido entre el ser humano, y a causa de ello, se crean los sistemas de control (control en el trabajo = más dinero). ¿Pero, que son los sistemas de control? Son un conjunto de dispositivos encargados de administrar, ordenar, dirigir o regular el comportamiento de otro sistema, con el fin de reducir las probabilidades de fallo y obtener los resultados deseados.

Los primeros sistemas de control aparecen en el siglo 3 antes de Cristo, en Grecia, cuando Ktesibios crea un reloj de agua, conocido también como Clepsydra, algo parecido al reloj de arena pero con agua. Con esto empezamos a controlar el tiempo. Pero el verdadero salto e impulso, se da junto con la revolución industrial, nace la máquina de vapor y se mejoran los sistemas de control. Watt crea reguladores centrífugos para regular el vapor de las máquinas y eso da el pistoletazo de salida para la mejora y evolución de los sistemas de control industrial (ICS).

La rapidez con la que evolucionan crece, los sistemas mecánicos se

desarrollan hasta 1900, entonces son superados por sistemas hidráulicos y los motores eléctricos además el desarrollo de la electrónica adquiere gran relevancia durante la segunda guerra mundial. En 1960 aparecen los primeros autómatas programables (antes existían los armarios eléctricos formados por relés, temporizadores y contadores), y junto con ellos aparecen los primeros PLC (controladores lógicos programables), robustos para aguantar el contexto industrial, fácilmente programables y modulares.

Todo era fantástico, los sistemas de control industrial (ICS) evolucionaban bien y sin problemas graves, no tenían amenazas grandes y todas las mejoras eran implementadas con la única pega de los problemas internos en su montaje o creación. Era probablemente la rama más segura dentro de la industria, siempre libres de peligros externos y fuera del alcance de los ciber peligros. No eran infalibles, pero externamente nadie podía dañarlos.



Los sistemas de control de procesos y SCADA (Supervisory Control And Data Acquisition) se consideraban inmunes a los ataques de red gracias a la dependencia de las redes propietarias y hardware, pero, por desgracia la llegada de Ethernet, TCP/IP y las tecnologías Web los ha dejado al descubierto ante los ataques de los hackers. No es simplemente el hecho de que estén desprotegidos lo preocupante de este tema, sino que, la inexistencia de amenazas anteriores, había provocado que las empresas se acomodaran a la hora de proteger sus sistemas de control industrial, y ahora se ven sobrepasadas por este problema, ya que son totalmente ignorantes en este campo.

Mientras otros sectores de las empresas evolucionaban para protegerse de los ciber ataques, ¿qué pasaba con los sistemas de control industrial? en mi opinión no ejecutaron una buena planificación, cuando internet irrumpe tan fuertemente en la industria y empiezan a verse los problemas que gente externa puede causar en diferentes sectores, creo que mínimamente tendrían que haberlo contemplado y tener una posible solución o escapatoria al menos. Afortunadamente muchas buenas iniciativas están en marcha para la mejora de la seguridad en los ICS.

Después de leer este párrafo anterior, me acuerdo de cosas dichas en clase: me recuerda, porque las auditorias, a pesar de ser no muy bien recibidas son importantes dentro de las empresas, concretamente me viene a la mente la evaluación de riesgos. Pero también me surgen algunas dudas sobre cual es realmente el origen del problema de los ICS: ¿Falta de planificación? ¿Un mal análisis de riesgos dentro de la empresa? tal vez consideraban ese riesgo pero les costaba más ponerle solución o no le dieron la importancia que realmente tenía. Sea lo que sea, ahora mismo la situación de los ICS podría describirla en una frase:

Los controladores sin control.

Referencias:

[https://es.wikipedia.org/wiki/Sistema\\_de\\_control](https://es.wikipedia.org/wiki/Sistema_de_control)

<http://isa.umh.es/asignaturas/asc/temasautomatas/Tema1.pdf>

<http://iaci.unq.edu.ar/materias/laboratorio1/archivos/Clases/Evoluci%C3%B3n%20Hist%C3%B3rica%20de%20los%20Sistemas%20de%20Control.pdf>

<http://automata.cps.unizar.es/Historia/Webs/IntroduccionI.htm>

<https://keats.kcl.ac.uk/pluginfile.php/1251665/course/section/414590/byres-myths-and-facts-cyber-security-scada.pdf>

[http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800\\_82\\_r2\\_draft.pdf](http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800_82_r2_draft.pdf)

<http://cds.cern.ch/record/532624/files/mcli01.pdf>

<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/industrial-control-systems-a-primer-for-the-rest-of-us.aspx>

<http://www.isaca.org/Journal/archives/2010/Volume-4/Pages/JOnline-Security-of-Industrial-Control-Systems.aspx>