Industria 4.0 y Ciber Seguridad en las Fundiciones

JOHN HALL
Presidente
CMH Manufacturing Company

PUNTOS SOBRESALIENTES DEL ARTÍCULO:

- Defienda su compañía frente a ciber ataques
- Cómo combinar alta tecnología de seguridad dentro de su lugar de trabajo
- Cómo crear un plan de seguridad

McKinsey define a la industria 4.0 como "la siguiente fase en la digitalización del sector de manufactura, impulsado por cuatro disrupciones: el asombroso aumento en los volúmenes de datos, el poder computacional y conectividad, especialmente nuevas redes de área extensa y baja potencia; el surgimiento de las capacidades de análisis y e inteligencia empresarial (Business Intelligence "BI"); nuevas formas de interfase hombre-máquina como las pantallas táctiles y los sistemas de realidad aumentada; y mejoras en la transferencia de instrucciones digitales al mundo físico, como la impresión 3D y robótica avanzada."

La Industria 4.0 y la IIoT (Internet de las cosas Industrial) va a cambiar la forma de hacer negocio de las fundiciones. En las fundiciones tradicionales los departamentos de informática (IT) y de Ingeniería de operaciones (OT) eran cuartos traseros con cablería y que utilizaban acrónimos que nadie de la gerencia comprendía. Estas dos áreas de especialización tienen diferentes prioridades y objetivos que llevan a lograr la pieza terminada. Hoy ya no podemos manejarnos así. En la Industria 4.0 y la IIoT se crean y comparten cantidades ingentes de datos de las operaciones de fundición como, por ejemplo:

- Cronogramas
- Fabricación de Corazones
- Moldeo
- Fusión/manejo del metal líquido
- Acabado
- Tratamiento térmico
- Mecanizado
- Despachos
- Cuentas a pagar
- Cuentas a cobrar
- Nómina salarial
- Control de Inventario
- Mantenimiento (quizás el más importante)

Esta amplia cantidad de información será compartida mediante IoT, la nube, hilos digitales y análisis de datos en tiempo real. Confiaremos en nuestras computadoras, laptops y dispositivos electrónicos de mano para hacer memos y comunicarnos cara a cara. Obviamente, necesitamos reforzar nuestra seguridad cibernética.

Toda esta nueva tecnología y flujo de datos, ha dado a los criminales nuevas formas de atacarnos y robarnos. Los ciber ataques son una amenaza real independientemente del tamaño de su negocio. Conozco de esto de primera mano porque la cuenta bancaria de mi compañía fue asaltada por ciber ladrones. Este penoso incidente es prueba de que los ciber criminales son innovadores, organizados y no tienen moral. Dicho esto, su defensa debe ser aun más creativa y organizada. A pesar de esta nueva amenaza, muchas fundiciones se toman su tiempo en actuar, pensando que están bien protegidas o bien, que esto no les sucederá a ellas. No hay una fórmula simple para proteger los datos de su fundición. Debemos combinar seguridad tecnológica con una cultura de seguridad en el trabajo y de capacitación a los empleados.

Las Fundiciones deben adoptar un enfoque universal a la ciber seguridad de la Industria 4.0; un método de funcionamiento seguro que incluye personas, procesos y tecnología. Deben desarrollar un plan de seguridad e identificar los mayores riesgos a las operaciones de la fundición a las que nos referimos previamente. Algunas de las preguntas son:

- ¿Qué prácticas/procedimientos/ equipos pueden afectar los procesos de la fundición?

continúa en la página siguiente...

- ¿Qué sucedería si falla una práctica/procedimiento/máquina?
- ¿Qué se necesita y cuánto tiempo tomará recuperarnos de la falla?
- ¿Es segura nuestra red?
- ¿Está a salvo nuestra propiedad intelectual?
- ¿Es segura nuestra cadena de suministros?
- ¿Qué hacemos a continuación?

Crear una matriz de riesgos tradicional es una buena manera de planificar por si hay una falla. Como ejemplo:

Alta probabilidad				
Probable				
Poco Probable				
Altamente Improbable				
	Bajo Impacto	Impacto Medio	Alto Impacto	Muy Alto Impacto

Una vez completada la matriz para todas las operaciones de la fundición, pueden monitorearse los eventos en tiempo real y emitir un informe que indique el riesgo. Luego consejos sobre cómo mejorar sus procedimientos e implementar una Industria 4.0 de manera segura en su fundición.

Aunque sin ordenarlos por importancia, debajo hay una lista de algunas debilidades encontradas en las operaciones de mi fundición:

- Falta de conciencia del problema entre el personal
  - o No tenemos un programa formal de capacitación en ciberseguridad. Los individuos que utilizan una PC de la compañía reciben instrucciones verbales de qué hacer y qué no, pero es muy informal.
- Uso de internet, dispositivos de mano y con USB
  - o Tenemos algunas reglas acerca del uso de teléfonos celulares, pero son casi imposibles de hacer cumplir. Ahora que los teléfonos inteligentes pueden hacer cualquier cosa incluyendo email de la compañía y trabajo en redes, los riesgos aumentan. En una Industria 4.0/IIoT las máquinas de la fundición se comunican con los dispositivos del gerente de mantenimiento por tareas de mantenimiento prescriptivo.
- Backups inadecuados
  - o Tuvimos una caída de un servidor y nos llevó a descubrir que nuestro servidor de copias de respaldo había estado inoperativo durante algunos meses. Enviamos los discos a una compañía de reparación/recuperación y logramos un 65% de éxito al recuperar archivos. El resto se perdió.
- Estándares y protocolos inadecuados
  - o Este punto se relaciona con el primero, sin embargo, la dirección hizo poco para mejorar los estándares. La dirección debe involucrarse, asumir el liderazgo y fijar las pautas.
- Configuración pobre del cortafuegos o acceso remoto sin gestionar
  - o Tenemos una buena protección de cortafuegos (firewall), pero nuestra protección para acceso remoto es promedio. Tenemos clientes que nos dan acceso remoto a sus PLCs para asistencia técnica de problemas de manera remota. A medida que esta práctica gana popularidad debemos considerar la protección de la red de trabajo.
- Pobre protección contra malware
  - o Hay cientos de aplicaciones contra software malicioso en el mercado actualmente. Un problema que experimentamos en mi compañía es que los usuarios discontinúan la utilización de protección contra malware con la excusa de que "enlentece mucho mi computadora." Otra buena medida contra el software malicioso son las copias de respaldo de calidad realizadas a diario.

Ahora que se identificaron los riesgos, debemos desarrollar procedimientos de seguridad. Debido a la criticidad de la ciberseguridad, se creó la Agencia de Ciberseguridad e Infraestructura de Seguridad (Cybersecurity and Infrastructure Security Agency - CSISA) por el gobierno federal de los EE. UU. Su catálogo está disponible en https://www.cisa.gov/publication/cisa-services-catalog

Adicionalmente, en Dic/04/2020 el Congreso aprobó la Ley Nº:116-207 "The Internet of Things Cybersecurity Act of 2020". Este proyecto de ley requiere que el National Institute of Standards and Technology (NIST) y la Office of Management and Budget (OMB) tomen acciones específicas para aumentar la ciberseguridad de los dispositivos con Internet de las Cosas (IoT). IoT es la extensión de la conectividad de internet a los dispositivos físicos y objetos diarios. Otros trabajos de marco de referencia y estándares como IEC 62443, ISO 27001 y 27002, NIST Special Publication 800-82 y el marco de referencia NIST para la mejora de la infraestructura crítica de Ciberseguridad se crearon como guías.

Aunque tanto la tecnología de la información (IT) como la tecnología de operaciones (OT) son importantes, los gerentes de la fundición deben marcar una clara distinción entre la gestión de IT y la de OT. Esto puede ser difícil ya que las prioridades de IT y OT a veces son diferentes.

Las tablas debajo ilustran como pueden diferir en nueve puntos clave:

IT	OT
Priority #1: Confidentiality	Priority #1: Availability
Priority #2: Integrity	Priority #2: Integrity
Priority #3: Availability	Priority #3: Confidentiality

IT		OT
Automation of information	Versus	Automation of foundry processes
Logical	Versus	Physical
Cybersecurity	Versus	Physical security and safety
Recent technology (max. five years)	Versus	Mix of new and old technology (up to thirty years)
Average to good cybersecurity awareness	Versus	Limited to no cybersecurity awareness
TCP/IP	Versus	Modbus/Profibus

Ahora que identificamos las diferencias clave entre IT y OT, el gerente de la fundición debe:

- Identificar quién es responsable – En la mayoría de las fundiciones la ciberseguridad es responsabilidad del gerente de IT, sin embargo, su tarea a menudo termina al comienzo de la producción. El gerente de seguridad e higiene es normalmente el responsable de la seguridad física. Esto deja el vacío de quién es responsable de la seguridad de OT. Alguien en la fundición debe tomar formalmente la responsabilidad de la seguridad de OT.
- Capacite a sus empleados en ciberseguridad – Cada empleado con acceso a IT y OT debe comprender los riesgos de ciberseguridad. La simple instalación de un dispositivo no crítico como una impresora con conectividad Wi-Fi puede abrir una debilidad. Una amenaza aun mayor puede ser el uso de teléfonos inteligentes personales y dispositivos USB para realizar tareas de la compañía. El acceso sin controlar a los servidores puede resultar también en varios gigabits de basura almacenada. El entrenamiento también debe ajustarse a las capacidades de cada empleado. La comprensión sobre ciberseguridad de sus moldeadores podría no se la misma que la de su joven programador de PLC.
- Desarrolle una cultura de vigilancia – La mayor debilidad de la seguridad de OT se encuentra dentro de la misma fundición. Al desarrollar un plan de seguridad de OT, el riesgo mayor es de parte de los empleados, contratistas y otras personas que puedan acceder al sistema desde dentro. Si se permite a las visitas acceder a la red Wi-Fi, debería haber una red de visitas monitoreada de cerca.

Para ayudar al fortalecimiento de la seguridad OT, los fabricantes de equipamiento que quieran asistir a las fundiciones a implementar la Industria 4.0/IIoT deben proveer hardware, programación de PLC, de interfaz hombre máquina, software y trabajo en red que brinde segmentación y segregación entre los sistemas de fundición y los usuarios no autorizados. Desafortunadamente, cuantos más sistemas conecta, más expuestas y vulnerables se vuelven las capas más sensibles de manufactura. A menos que se aísle específicamente, como los dispositivos están interconectados, un dispositivo de IIoT comprometido puede dar acceso al resto de los dispositivos del mismo segmento de OT. Multiplique por mil veces los dispositivos individuales y podrá ver cómo proliferan las cuestiones potenciales de seguridad. Por lo tanto, la seguridad de los dispositivos con IIoT en la red OT es tan importante como todos los otros componentes de la maquinaria conectados a la red.

Los fabricantes de maquinaria necesitan cambiar el modo de asegurar las redes en una era industrial 4.0/IIoT. Como señalamos, IT y OT a veces entran en conflicto, de modo que ¿ cómo conectamos las operaciones más bajas de OT directamente a nuestro IT manteniendo la ciberseguridad? ¿Qué papel cumple la nube en este esquema? ¿Cómo podemos reconciliar la capacidad de nuestros dispositivos con IIoT para enviar datos directamente a la nube con nuestra necesidad de asegurarlos apropiadamente frente a peligros potenciales?

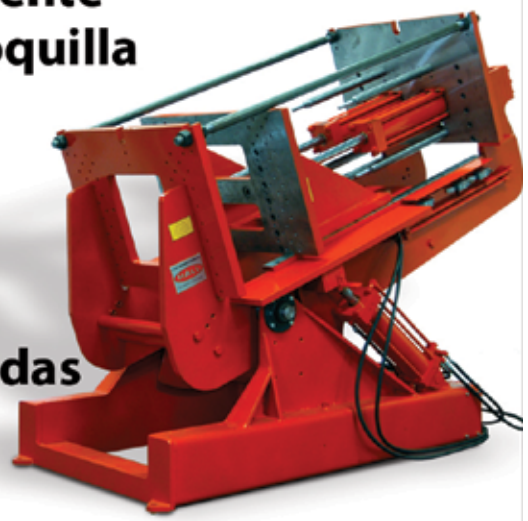
Contacto:
JOHN HALL
jhall@cmhmfg.com

HALL

Sistemas de Fundición Hall

por CMH Manufacturing

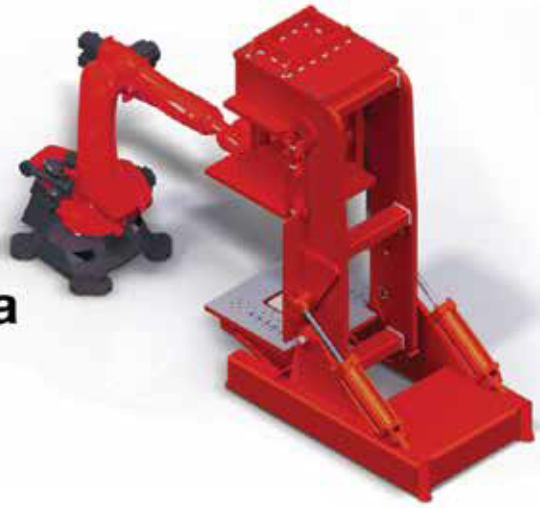
Máquinas para Molde Permanente
Fundición por Gravedad en Coquilla
Proceso de Colada Basculante
Equipos al estilo AutoCAST
Mesas Rotatorias



Celdas de Trabajo Automatizadas
Sierras para Montantes
Enfriadores
Receptor de piezas fundidas
Accesorios para la Fundición

Sistemas de Fundición Hall
por CMH Manufacturing

3R & 6R –Sin barras que interfieran con la colocación o extracción de corazones robotizada



APRIL 23-26, 2022 COLUMBUS, OHIO
AFS CASTEXPO & METALCASTING CONGRESS
connecting SUPPLIERS | METALCASTERS | CASTING BUYERS

VISIT US BOOTH 941

HALL

Tel: 806-744-8003
sales@cmhmfg.com
www.cmhmfg.com