Industry 4.0 and Foundry Cyber Security

JOHN HALL
President
CMH Manufacturing Company

ARTICLE TAKEAWAYS:

- Defending your company against cyber attacks
- How to combine high tech security within your workplace
- How to create a security plan

Casting process simulation has been used by many foundries to design the process for production of castings before castings are made or before equipment is built or altered. Computer modeling has the ability to evaluate process designs in much less time, and at much less cost, than building equipment and producing sample castings.

McKinsey defines industry 4.0 as "the next phase in the digitization of the manufacturing sector, driven by four disruptions: the astonishing rise in data volumes, computational power and connectivity, especially new low-power wide-area networks; the emergence of analytics and business intelligence capabilities (BI); new forms of human-machine interaction such as touch interfaces and augmented-reality systems; and improvements in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing."

Industry 4.0 and IIoT will be changing the way foundries do business. In traditional foundries the information technology (IT) and operational technology (OT) departments were back room wire heads that no one in management understood their use of unheard-of acronyms. These two areas of expertise have very different priorities and goals that lead to a finished casting. We cannot live like that today. In Industry 4.0 and IIoT huge amounts of data are being created and shared in foundry operations such as:

- Scheduling
- Core making
- Molding
- Melting/liquid metal handling
- Finishing
- Heat treating
- Machining
- Shipping
- Accounts payable
- Accounts relievable
- Payroll
- Inventory control
- Maintenance (perhaps the most important)

This vast amount of information will be shared via IIoT, the cloud, digital threads, and real time data analytics. We will rely on our desktops, laptops, handheld devices to do things that were once done with memos and face to face communication. Obviously, there is a need for heightened cyber security.

All this new technology and data transfer have given the criminals new ways to attack and rob us. Cyber attacks are a real threat regardless of the size of your business. I know this firsthand because my company's bank account was robbed by cyber thieves. This painful incident is proof that cybercriminals are innovative, organized, and have no morals. That being said, your defense must be more innovative and organized. Despite this new threat many foundries have been slow to respond, often thinking we are well protected, or it cannot happen to us. There is no simple solution to protecting your foundry's data. We must combine high tech security with a culture of workplace security and employee training.

Continued on next page

Foundries must take a universal approach to Industry 4.0 cybersecurity; a policy method that includes people, process and technology. They must develop a security plan and identify the biggest risks to the foundry operations referred to previously. Some of the questions include:

- What practices/procedures/equipment can affect foundry processes?
- What will happen if a practice/procedure/equipment fails?
- What is required and how much time will it take to restore the failure?
- Is our network safe?
- Is our intellectual property safe?
- Is our supply chain safe?
- What do we do next?

Creating a traditional risk assessment matrix is a good way to plan for failure. An example is:

Highly Likely				
Likely				
Unlikely				
Highly Unlikely				
	Low Impact	Medium Impact	High Impact	Very High Impact

Once the matrix is completed for all foundry operations, real time events can be in an OT report that states risk. Then clear guidance on how to improve foundry procedures and safely implement Industry 4.0.

Although in no particular order of importance, some of the weakness found in my company's operations are:

- Lack of awareness among the workforces
  - We have no formal cybersecurity training program. Individuals who have a company owned PC are verbally instructed the do's and don'ts, but it is very informal.
- Use of USB devices, internet, and handheld devices
  - We have some rules about cell phone use, but they are nearly impossible to enforce. Now that smart phones can do anything including business email and networking, risks increase. In Industry 4.0/IIoT foundry machines will be communicating with maintenance manager's devices about prescriptive maintenance.
- Improper backups
  - We had a server crash only to discover that the back up drive had been inoperative for several months. We sent the drives to a repair/recovery company with about 65% success. The rest was lost.
- Inadequate protocols and standards
  - This point relates to the first point, yet management has one little to improve standards. Management must be involved, take the lead and set the tone.
- Poor firewall configuration or unmanaged remote access
  - We have good firewall protection, but our remote access protection is average. We have customers who sometimes give us remote access to their PLCs for remote troubleshooting. As this practice grows in popularity network protection must be considered.
- Poor malware protection
- There are 100's of malware applications on the market today. One problem experienced in my company is users discontinue malware protection with the excuse that "it slows my computer down too much." Another good protection from malware is very high-quality daily backups.

Now that risks have been identified, we must develop security procedures. Due to the critical nature of cybersecurity the Cybersecurity and Infrastructure Security Agency (CSISA) was created by the Federal Government. Their catalog is available at https://www.cisa.gov/publication/cisa-services-catalog

In addition, on 12/04/2020 Congress passed Public Law No:116-207 "The Internet of Things Cybersecurity Act of 2020." This bill requires the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to take specified steps to increase cybersecurity for Internet of Things (IoT) devices. IoT is the extension of internet connectivity into physical devices and everyday objects. Other frameworks and standards such as IEC 62443, ISO 27001 and 27002, NIST Special Publication 800-82 and the NIST Framework for Improving Critical Infrastructure Cybersecurity have been created as guides.

While both IT and OT are important, foundry managers must make a clear distinction between IT and OT management. This can be difficult in that IT and OT priorities are sometimes different.

The following tables illustrates how nine key points can differ:

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

Now that the key differences between IT and OT have been identified, the foundry manager must:

- Identify who is responsible – In most foundries cybersecurity is the responsibility of the IT manager, however his/her role often ends at the start of production. The health and safety manager is normally responsible for physical security. This leaves a void as to who is responsible for OT security. Someone within the foundry must formally take on responsibility for OT security.
- Educate employees on cybersecurity – Each employee with access to IT and OT must understand cybersecurity risks.

The simple installation of a non-critical device such as a Wi-Fi printer can open a weakness. An even greater threat can be the use of personal smart phones and USB devices to conduct company business. The uncontrolled access to servers can also result in many gigabits of garbage being stored. Training must also be tuned to each employee's ability. The molders understanding of cybersecurity might not be the same as your PLC programmer.

- Develop a culture of vigilance – The greatest weakness to OT security is from within the foundry itself. When developing an OT security plan, the greatest risk is from employees, contractors, and other people who can access systems from within. If guests are allowed access to Wi-Fi, there should be a guest network that can be closely monitored.

To help foster heightened OT security, equipment manufacturers that want to help foundries implement Industry 4.0/IIoT should provide hardware, PLC programing, HMI programing, software, and networking that provides segmentation and segregation between foundry systems and non-authorized users. Unfortunately, the more systems connect, the more exposed and vulnerable the underlying sensitive manufacturing layers become. Unless specifically isolated, as network-connected devices, a compromised IIoT device can provide access to the rest of the OT segment it is on. Multiply that times thousands of individual devices, and you can see where the potential security issues proliferate. Therefore, the security of IIoT devices on the OT network is just as important as all the other network-connected components running the machinery.

Equipment manufacturers need to change how we secure networks in an Industry 4.0/IIoT age. As pointed out IT and OT sometimes conflict so how do we connect the lower OT operations directly to the IT operations while maintaining cybersecurity? What role does the cloud play in all this? How can we reconcile the ability of IIoT devices to send data directly to the cloud with the need to properly secure them against the growing potential for compromise?

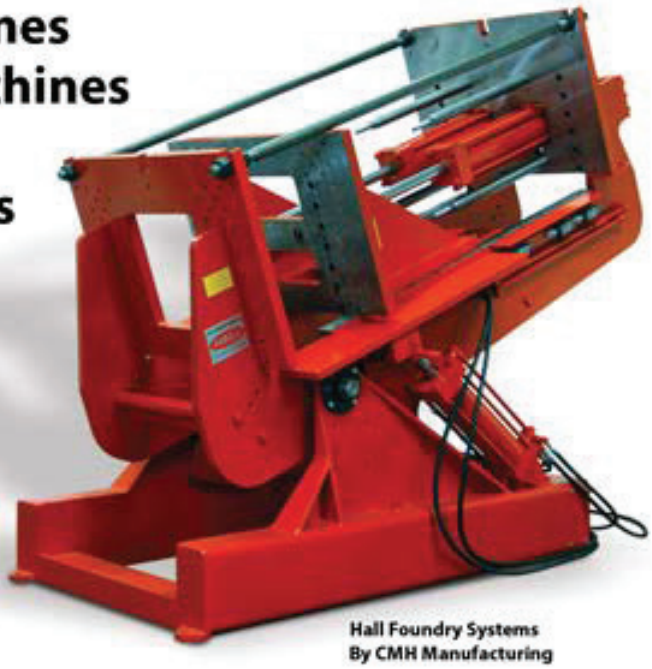
Contact:
JOHN HALL
jhall@cmhmfg.com

HALL

Hall Foundry Systems

By CMH Manufacturing

Permanent Mold Machines
Gravity Die Casting Machines
Tilt Pour Process
Autocast Style Machines
Rotary Tables



Hall Foundry Systems
By CMH Manufacturing

Automation Work Cells
Riser Saws
Casting Coolers
Casting Catchers
Foundry Accessories

3R & 6R — No tie-bars to interfere with robotic core placement or casting extraction.

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