ATMS
Advanced Transportation
Manufacturing Summit Toronto

Cybersecurity for Advanced and Intelligent Manufacturing Environments

By Carla Larkin

In the Industry 4.0 era, companies are increasingly investing in their digital footprint and adopting new technologies to remain current and competitive. As Michael Jobity, Process Improvement and Digital Lead at Airbus explains: ‘The implementation of digital solutions allows users to monitor, control, and track machinery and equipment in real-time. This eliminates waste, improves productivity, creates transparency across the production floor and allows managers to have control of their facilities. The unique capabilities of certain technologies (ex. IoT, AR, VR, Blockchain) give rise to exponential annual benefits when applied correctly.’

However, this rapid transformation towards the latest technology solutions has created a new type of vulnerability. As organisations delve deeper into the digital, opportunities for cyber-attack only increase. Threats ranging from compromised physical security to production downtime; spoilage of products to damaged equipment means that cybersecurity is a vital factor underpinning success in this new age of industry. Dr Mihaela Vlasea, Assistant Professor at the University of Waterloo, Ontario, told us that in additive manufacturing in particular, ‘a large portion of the manufacturing workflow is in the digital domain. Any intentional data disruption/manipulation could result in high losses, as the part quality can be influenced at the micro (material), meso (design feature), and macro (part) scale.’

And while the fourth industrial revolution is clearly and frequently associated with a corporate requirement for cybersecurity, many manufacturers still do not fully recognise or understand their vulnerability against internal and external threats. Walter Garrison, City of Mississauga’s Advanced Manufacturing Business Integrator, points out that ‘there is a common belief that it is not a question of whether you will get hacked but when’. With over 60% of manufacturers subjected to a cyber security incident and almost a third suffering financial loss or disruption to business as a result, how do companies protect their information and assets from cyber-attack as they move towards the adoption of Industry 4.0?

According to Jobity, companies can adopt a number of different tactics to create an effective cybersecurity strategy: ‘Enterprises should conduct audits on a regular basis, use two-factor authentication, identify the major threats, and enforce a strong sign-off policy. Investments into platforms that have a track record of robustness and security strength must be a priority in this information era,’ Similarly, Garrett Austin, Business Development Lead at Rockwell Automation, describes a three-pronged approach to help manufacturers stay safe, which involves ‘determining OT Maturity by increasing visibility and monitoring; establishing an IT/OT Strategy and creating governance around it; and building bridges between engineering, operations and IT’.

Whichever way you decide to tackle it, the key is to remember that every new technology brings new potential risks. For manufacturers in the digital era, cybersecurity is now more important than it has ever been. Companies must encourage an active mindset and a multi-faceted approach towards mitigating the risks in order to secure their factories and workplaces, reduce downtime and minimize losses and privacy breaches.