

Unveiling the AI Revolution: Advancements, Threats, Opportunities

For Related Articles Search

artificial intelligence

at geartechnology.com

Mary Ellen Doran, AGMA Director, Emerging Technology

Artificial Intelligence (AI) has gotten a lot of buzz lately, and rightly so—as James McQuiggan put it in our December emerging tech webinar, “I’ve never seen a technology advance and change so much in one year than I have with AI.” While AI is not new, recent advancements in computing power have allowed developers to unleash very powerful AI tools to the public. Our IIoT Committee is exploring how this technology is being utilized in manufacturing in everything from task automation, predictive maintenance, and fraud detection to chatbots and other customer service-style tools. We hope you join us in these discussions.

While most will use these tools for average work, there is already an increased threat as this technology aids those with more nefarious intentions. AI helps generate things quickly and is being used to generate phishing emails and attack programs. Again, James cites in his webinar that from 2022 to 2023 malicious phishing messages increased by 1,265 percent. On average, 31,000 phishing attacks are sent daily, and there has been a 967 percent increase in credential phishing. This just makes it ever more important to have policies in place to train your staff to watch for these threats. And it is not just learning to spot bad emails. There are examples of AI being used in voice generation to have accounting departments transfer money for what they think is an executive. Awareness is crucial. Always take a breath when getting a message that is outside the normal practice of business and double-check sources.

The committee will be following NIST’s Artificial Intelligence Risk Management Framework and the development of the AI Security Center at the National Security Agency. We hope to bring in presenters, like James, to continue the discussions this year to keep you aware of the constant changes in this space. If you have not watched his webinar, it is on-demand on the AGMA website: agma.org/event/ai-steered-safety-geared-ais-voyage-with-gear-manufacturing

In the AGMA Robotics Committee, we are having a similar conversation about the pace of technology. The topic is humanoid robots. As recent as July of last year committee members were hoping to see advanced developments of these new types of robots in three to five years. But in our meeting in early March, just days ago, many committee members commented on the number of developments that have been in the news in recent weeks. A video shows Tesla’s Optimus moving at speeds 30 percent faster than previously shown last year and with more agility. Humanoid robots are going to work in factories for NIO and Amazon. Even in the days since that

meeting news has come out about researchers at Carnegie Mellon University developing real-time human-to-humanoid teleoperation. This project is based on reinforcement learning (RL) which is an AI/Machine learning technique that teaches a software program to do something by trial and error. This technique, which has been used to teach computers to play video games, is now being applied to teach them how to walk more humanly. It will still be a while before these robots come into mass production, but the pace at which the industry is moving should be noted. And while the committee discusses all aspects of these projects, make no mistake that we are laser-focused on what is happening with hardware.

Currently, robot developers are feeling constraints with the limits of torque in gearboxes that are being used in joints. Committee members are watching this space and watching companies that are out in front in finding solutions. Committee members are also discussing backdrivability—which will be crucial to safety when these types of robots are used next to humans. We are working to bring experts to discuss this in more detail for the AGMA audience. And you are always welcome to join the committee to add to these discussions.

The AGMA Emerging Technology work continues to monitor advancements that may disrupt or positively impact the gear industry. Watch out for our upcoming webinars, and more information on a face-to-face event happening this summer.



Social Engineering Defense in Depth

Mitigate	<ul style="list-style-type: none"> Aggressively Mitigate Social Engineering People, Processes, Technology
Patch	<ul style="list-style-type: none"> Patch Exploited Software & Firmware Monitor the CISA KEV Catalog (Known Exploited Vulnerabilities)
MFA	<ul style="list-style-type: none"> Use MFA Wherever Possible Non-phishable MFA too, Avoid SMS and verify all requests that you didn't initiate
SPOT	<ul style="list-style-type: none"> Learn how to Spot Rogue URLs No longer – don't click on links, or check your links, make sure they know how
DiNGS	<ul style="list-style-type: none"> Remember to use DiNG style of passwords Different, Non-Guessable, Strong



KnowBe4

Cyberdefense techniques outlined in James McQuiggan’s Emerging Technology webinar “AI Steered, Safety Geared: AI’s Voyage with Gear Manufacturing.”