The Digital Twin Advantage in Automotive Manufacturing Systems

Digital twin technology has gained significant traction with the emergence of big data and the Internet of Things (IoT) and is now being utilized in many industries worldwide. A digital twin is a virtual model of a physical object designed to accurately reflect the object.

In digital twin technology, a physical object is outfitted with many sensors across different areas of functionality so that the sensors can effectively measure attributes of the physical object (e.g., temperature).[1] The sensors collect and relay data to the processing system, which applies the data to the digital copy, updating it in real time. With these data, simulations using artificial intelligence (AI) wand machine learning (ML) can be run on the virtual model to further study performance and help make decisions.[2]

The data allow for valuable insights that can be applied to the original physical object, improving its overall condition and performance.[3]

Virtual models are used by industries such as construction and automotive manufacturing to help identify which areas of performance manufacturers should focus on and what possible improvements can be made. For example, the construction industry effectively uses digital models of buildings and bridges to understand their structural integrity better and to pinpoint any issues. In addition, digital twin technology is used in complex projects such as the production of jet engines, aircraft and automobiles to improve the overall efficiency of the products.[4]

Digital twin technology using AI and ML in the automotive industry can enhance the overall design and efficiency of automotives products; however, these technologies pose cybersecurity risk. Therefore, it is essential to understand the mitigation measures organizations can take to protect themselves and their products.[5]

ML Algorithms in Digital Twin Technology

Digital twin technology uses AI, or more specifically, ML algorithms, to effectively analyze and assess the large amounts of data the sensors provide.[6] The aim of both AI and ML is development of intelligent programs that can handle complex tasks. ML algorithms are built on three major components: representation, evaluation and optimization. These components have requirements that must be fulfilled to generate an ML model and algorithm effectively. An ML-based twin of a production root cause analysis (RCA) process is intended to diagnose the root cause

KARTHIK TRICHUR SUNDARAM

Is director of IT solutions management at Applied Materials. He has more than two decades of experience in supply chain and asset management business processes, working with organizations such as SAP. Sundaram has served on the judging committees for many technical awards and published many articles in the media and in the review panel of a leading journal. He has lead projects for global customers in asset intelligence networks, digital twins with the Internet of Things and Industry 4.0. He also recently implemented one of the first digital vehicle hub solutions in North America for a large agricultural automotive leader.

DIVYA KARTHIK

Is a DevOps automation and site reliability engineer at Poshmark. She has experience in working with a variety of new technologies and taking them from proof of concept to production. She has a background in debugging critical site reliability issues, software system design and DevSecOps. She enjoys learning about new products and technologies by participating in judging panels for the Stevie and Globee Awards. She has also been involved in leading a chapter of Women in Computer Science at the University of California, Davis (California, USA) and volunteering with the National Center for Women and Information Technology Aspirations in Computing Scholarship Committee.

of a deficiency or anomaly found in the finished product or during the manufacturing process. It enables line managers to troubleshoot the most likely root causes based on the tool's predictions, identify the problem definitively, and implement corrective and preventative actions (CAPA) without spending too much time and effort searching through machine maintenance records, operator history, processes and IoT sensor inputs.[7] The goal is to minimize machine downtime and loss of production and enhance resource utilization.

Most of the uses of digital twin technology in the automotive industry involve testing the products (namely cars) through simulations.

The Digital Twin Advantage in Automotive Manufacturing

The global digital twin technology market currently stands at US$9.5 billion and is expected to reach US$72.65 billion by the year 2032, at a robust compound annual growth rate (CAGR) of 22.6 percent from 2022 to 2032.[8] North America has the largest digital twin technology market share, with 40 percent.

The transportation and automotive sectors hold more than 15 percent of the market share due to growing demand for automotives. This could be explained by the growing adoption of electric vehicles (EVs) around the world.[9]

The advantages of digital twin technology are numerous, and its application can result in various advantages across industries. Most of the uses of digital twin technology in the automotive industry involve testing the products (namely cars) through simulations. This testing revolves around the manufacturing of automotive vehicles and how their performance can be enhanced.[10] Digital twin technology can provide several benefits for automotive manufacturers including:

- Executing tests using the digital copy of the product or vehicle and simulating crash tests, autonomous driving and other scenarios to enable a better understanding of the various aspects of the vehicle that could be improved.[11]
- Testing with digital twin technology to confirm compliance with standards and automotive industry certifications such as International Automotive Task Force (IATF) 16949[12] and International Organization for Standardization (ISO) standards ISO 9001:2015 *Quality management systems—Requirements*,[13] ISO 14001:2015 *Environmental management systems—Requirements with guidance for use*,[14] and ISO 45001:2018 *Occupational health and safety management systems—Requirements with guidance for use*.[15]
- Improving overall customer satisfaction through the use of digital twin technology by using the sensors and the data digital twin technology provides, for example, to improve the performance, lifespan, safety levels and fuel efficiency of vehicles.[16]
- Enhancing the overall agility and resilience of the supply chain through digital twin technology. To form an understanding of what materials model home manufacturers can use for construction, for example, and what would benefit the product.[17]
- Understanding the overall energy consumption of a product and how it behaves—an electric vehicle for example, by developing a digital copy or model of the product and running the necessary simulations and design changes on the digital model to ensure that there are no issues. Test results and ML algorithms can aid in achieving a superior design with less energy consumption. Manufacturers can also gain an understanding of how they can improve the overall aerodynamics of a car and reduce the vehicle's weight.

- Assessing the effect on a vehicle of environmental factors such as temperature and humidity using predictive ML algorithms. Based on the data, different models can be tailored to the needs of every region and their geographies. Modifications or revisions to an important component or part can be published on the digital twin platform, allowing seamless collaboration by original equipment manufacturers (OEMs), automotive manufacturers, customers and service providers.

These benefits are the primary drivers of digital twin technology implementation in many manufacturing facilities across industries. The US-based automotive manufacturer Tesla uses digital twin technology in every vehicle it produces.[18] Thinkwik, the partner that developed Tesla's digital twin application, states that real-time mechanical issues at Tesla Motors, regardless of their magnitude, are fixed by simply downloading over-the-air (OTA) software updates.[19] It is important for manufacturers to continuously exchange relevant data with the vehicles they produce to improve the quality of their products. The use of digital twins, along with pioneering technologies such as IoT, AI and ML, has made it feasible to perform processes that were once thought to be impossible.

Potential Risk of Digital Twin Technology

The adoption of evolving and emerging technologies to accelerate business growth inevitably creates an additional avenue of cyberrisk. Digital twins represent critical manufacturing assets that can directly affect an organization's bottom line. Though challenging, protecting digital assets is a key requirement organizations must meet when using digital twin technology. Although digital twin simulations can be used to monitor and track performance, they can also be configured to run real-life simulations to ensure that cybersecurity risk is mitigated.[20] However, securing digital twin operations, which are often hosted in the cloud, is another key challenge.

Digital twins represent physical systems, using additional inputs from sensors and controllers to provide a comprehensive summary for analysis. Although the physical assets may have protections such as microcontrollers or firewalls, digital twin representations can be vulnerable to security threats. Hackers can use cybersecurity threat techniques such as malware or spyware to control physical objects through digital twins, which could result in outages or major disasters. Digital twins may also represent objects that require intellectual property protection, such as semiconductors. If the digital twin is a blueprint of a piece of intellectual property, then hackers may be able to reverse-engineer and reproduce that property, bypassing the need for research and development of their own.

The use of digital twins, along with pioneering technologies such as IoT, AI and ML, has made it feasible to perform processes that were once thought to be impossible.

The security of any organization is only as strong as its weakest link. If digital twin credentials are exposed, the organization may be compromised. This is because most digital twins are connected through application programming interfaces (APIs) to IoT and other systems. Hackers can use a weak digital twin to disrupt or bring down an entire organization in a short amount of time.

Recommended Risk Mitigation Techniques

IoT devices are generally less secure than traditional devices such as processors, so using them as sensors in a twin setup creates concerns. Because most organizations already have a cybersecurity framework that does not cater to digital twins or other emerging technologies, new generation digital projects often involve internal cybersecurity experts only on a need-to-know basis. However, cybersecurity experts within and outside the organization can be engaged on a dedicated basis with a proper budget at each stage of a digital twin project to mitigate security risk areas. Security leaders and chief information security officers can teach their employees about authentication, authorization, data integrity, data confidentiality and nonrepudiation using their standard cybersecurity framework. Every apparent and perceived threat should be documented.

An organization's cyberframework should have policies that help its security infrastructure to be scalable and cyberresilient to meet growing security needs. Static security solutions cannot provide adequate security.

The key to scalable security is constant adaptation and redesign—not just expensive security products and specialized security experts. The cyberframework

LOOKING FOR MORE?

- Read *Audit Practitioner's Guide to Machine Learning, Part 1: Technology. www.isaca.org/audit-practitioner-guide-to-ML-part-1*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Many tend to overlook the longevity of digital twin technology; however, it can be used over the entire life cycle of the product, from the time of inception until its disposal.

should contain a planning strategy, streamlining, logic, up-to-date organizational policies, and security directives implemented by informed employees.

At both the interface level and the object level, digital twins should be protected with a zero-trust architecture. Multifactor authentication (MFA), microsegmentation and biometrics are additional layers of security that can help mitigate risk and provide returns on investment for secured organizational assets.

The use of ML algorithms for intrusion detection can help organizations identify and mitigate cybersecurity threats in a timely manner. However, it is imperative to train models using high-quality data sets to achieve successful intrusion detection. To build an attack model with high accuracy and low false positives, meaningful data collection and feature extraction are required. A digital twin-based security architecture can be effective for protecting industrial automation and control systems.[21] There are distinct security requirements for different components of the proposed architecture. It is advisable to synchronize clocks between the physical and digital twins at regular intervals to achieve active-state replication. Implementation of intrusion detection is critical to the entire architecture.

Conclusion

Digital twin simulation technologies are used by automotive manufacturers to gain an understanding of different aspects of the vehicle being designed. When applied to vehicle manufacturing systems, this technology can help reduce the cost of the vehicle, the level of carbon dioxide emissions, and fuel and maintenance costs, providing the manufacturer with a competitive advantage. Digital twins also allow manufacturers to improve the comfort, safety and efficiency of vehicles. ML algorithms can be used to develop digital models of a vehicle to test certain scenarios (e.g., vehicle crash, mechanical breakdown) and simulations to understand the various complexities and problems the product may encounter. They may also be able to improve the overall energy consumption of the vehicle, decrease air resistance, and make the vehicle more aerodynamic.

However, any organization that has digital twin capabilities is also at risk of cybersecurity threats. Digital twin projects should include cybersecurity experts at all stages. There should be enhanced security measures in place for all hybrid platforms and the network. Digital twins and their APIs should be tested for security vulnerabilities. Critical digital assets should be tested against hackers and disaster recovery mechanisms. A change agent can enforce security hygiene by implementing security measures such as zero trust architecture with MFA and additional security protection layers.

Digital twin assets security can be enhanced with ML. ML can analyze patterns in cybersecurity systems and learn from them to help prevent similar attacks and respond to changes in behavior. Real-time responses to active attacks can help cybersecurity teams be more proactive in preventing threats. Using ML-based cybersecurity systems to protect digital twin assets can reduce the time spent on routine tasks and enable organizations to utilize their resources more effectively.

Having an effective cybersecurity framework formalizes the subject matter expert's knowledge on anomaly detection. "If the framework has not seen a certain anomaly before, such as digital twin technology, a subject matter expert should analyze the collected data to provide further insights to be integrated into and improve the system," said Efe Balta, a postdoctoral researcher at ETH Zurich.[22]

The expert can either confirm the cybersecurity system's suspicions or teach it a new anomaly to store in the database. And as time goes on, the models in the system would theoretically learn more and more, and the human expert would need to teach them less and less.

Many tend to overlook the longevity of digital twin technology; however, it can be used over the entire life cycle of the product, from the time of inception until its disposal. The technologies composing digital twinning such as IoT, industrial IoT, AI, ML, big data, simulation and cloud computing have been on a path of constant evolution; thus, it can be assumed that digital twin technology will continue to evolve in parallel to these technologies.

Endnotes

1 Batty, M.; "Digital Twins," *Environment and Planning B: Urban Analytics and City Science*, vol. 45, iss. 5, 2018, p. 817–820, *https://journals.sagepub.com/doi/full/10.1177/2399808318796416*

2 Tao, F.; Q. Qi; L. Wang; A. Y. C. Nee; "Digital Twins and Cyber–Physical Systems Toward Smart Manufacturing and Industry 4.0: Correlation and Comparison," *Engineering*, vol. 5, iss. 4, 2019, p. 653–661, *https://www.sciencedirect.com/science/article/pii/S209580991830612X*

3 Tao, F.; Q. Qi; "Make More Digital Twins," *Nature*, 25 September 2019, *https://www.nature.com/articles/d41586-019-02849-1*

4 Rosen, R.; G. Von Wichert; G. Lo; K. D. Bettenhausen; "About the Importance of Autonomy and Digital Twins for the Future of Manufacturing," *IFAC-PapersOnLine*, vol. 48, iss. 3, 2015, p. 567–572, *https://www.sciencedirect.com/science/article/pii/S2405896315003808*

5 Singh, M.; E. Fuenmayor; E. P. Hinchy; Y. Qiao; N. Murray; D. Devine; "Digital Twin: Origin to Future," *Applied System Innovation*, vol. 4, iss. 2, 2021, p. 36, *https://www.mdpi.com/article/10.3390/asi4020036*

6 Zhou, G.; C. Zhang; Z. Li; K. Ding; C. Wang; "Knowledge-Driven Digital Twin Manufacturing Cell Towards Intelligent Manufacturing," *International Journal of Production Research*, vol. 58, iss. 4, 2020, p. 1034-1051, *https://www.tandfonline.com/doi/abs/10.1080/00207543.2019.1607978*

7 Kritzinger, W.; M. Karner; G. Traar; J. Henjes; W. Sihn; "Digital Twin in Manufacturing: A Categorical Literature Review and Classification," *IFAC-PapersOnLine*, vol. 51, iss. 11, 2018, p. 1016–1022, *https://www.sciencedirect.com/science/article/pii/S2405896318316021*

8 Dyson, L.; "Digital Twin Market to Grow 22.6 Percent Annually in Next Decade," Traffic Technology Today, 3 November 2022, *https://www.traffictechnologytoday.com/news/data/new-report-suggests-transportation-and-automotive-sector-will-sway-the-digital-twin-market.html*

9 Future Market Insights, Inc., "Transportation and Automotive Sector to Sway the Digital Twin Technology Market, Reaching US$ 72.65 Bn by the Year 2032," *GlobalNewswire*, 11 October 2022, *https://www.globenewswire.com/en/news-release/2022/10/11/2531840/0/en/Transportation-Automotive-Sector-to-sway-the-Digital-Twin-Technology-Market-reaching-US-72-65-Bn-by-the-year-2032-Future-Market-Insights-Inc.html*

10 Jiang, Y.; S. Yin; K. Li; H. Luo; O. Kaynak; "Industrial Applications of Digital Twins," *Philosophical Transactions of the Royal Society A*, vol. 379, iss. 2207, 2021, *https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2020.0360*

11 Damjanovic-Behrendt, V.; "A Digital Twin-Based Privacy Enhancement Mechanism for the Automotive Industry," Institute of Electrical and Electronics Engineers, *2018 International Conference on Intelligent Systems (IS)*, September 2018, p. 272–279, *https://ieeexplore.ieee.org/abstract/document/8710526/*

12 Automotive Industry Action Group, "IATF 16949:2016," *https://www.aiag.org/quality/iatf-16949-2016*

13 International Organization for Standardization (ISO), *ISO 9001:2015 Quality management systems—Requirements*, Switzerland, 2015, *https://www.iso.org/standard/62085.html*

14 International Organization for Standardization (ISO), *ISO 14001:2015 Environmental management systems—Requirements with guidance for use*, Switzerland, 2015, *https://www.iso.org/standard/60857.html*

15 International Organization for Standardization (ISO), *ISO 45000:2018 Occupational health and safety management systems—Requirements with guidance for use*, Switzerland, 2018, *https://www.iso.org/standard/63787.html*

16 Piromalis, D.; A. Kantaros; "Digital Twins in the Automotive Industry: The Road Toward Physical-Digital Convergence," *Applied System Innovation*, vol. 5, iss. 4, 2022, p. 65, *https://www.mdpi.com/2571-5577/5/4/65*

17 Fleisher, G.; "Four Technology Shaping the Future of Modular Construction," Modular Home Coach, 11 March 2022, *https://modularhomesource.com/four-technologies-shaping-the-future-of-modular-construction/*

18 Rais, A.; "Digital Twin in the Automobile Industry," Maschine Markt International, 8 January 2019, *https://www.maschinenmarkt.international/digital-twin-in-the-automobile-industry-a-851549/*

19 Tesla, "Software Updates," *https://www.tesla.com/support/software-updates*

20 Glocker, G.; "A Primer on Digital Twins in the IoT," Bosch Digital Blog, October 2018, *https://blog.bosch-si.com/bosch-iotsuite/a-primer-on-digital-twins-in-the-iot/*

21 Gehrmann, C.; M. Gunnarsson; "A Digital Twin Based Industrial Automation and Control System Security Architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, 2020, p. 669–680, *https://ieeexplore.ieee.org/document/8822494*

22 Staff, "How Digital Twins Could Protect Manufacturers From Cyberattacks," *Homeland Security Today*, 3 March 2023, *https://www.hstoday.us/subject-matter-areas/cybersecurity/how-digital-twins-could-protect-manufacturers-from-cyberattacks/*