



Digital Twin in Industry: A Cybersecurity Blind Spot?

Digital Twins are transforming industry by creating real-time virtual replicas of physical systems for monitoring and optimization. However, this innovation also introduces a hidden cybersecurity blind spot where compromised digital models could impact real-world operations.

By **Abdullah Tariq** | University of Agriculture | Published: September 2026

✉ abdullahtariq5044@gmail.com | Software Engineering

Introduction

The Digital Twin is one of the most transformative technologies for industries to implement in the process of digital transformation and is especially impacting the manufacturing, energy and logistics industries. A digital twin is a virtual model of a physical object like a manufacturing facility, supply chain, aircraft engine or power grid that exists in real time. These systems incorporate sensors, Internet things, cloud computing, and AI-powered investigation to replicate the genuine world procedures in a virtual space.

Digital twins have a huge impact on operational efficiencies, predictive maintenance and cost optimization, but they also present a new and largely unrecognized cyber security threat. Manipulated, corrupted, or compromised digital twins can have consequences that go beyond cyberspace to the physical infrastructure. This begs an important question: Is digital twin an industry cybersecurity dark spot?

Understands the concept of Digital Twin in industrial contexts

The digital twins are based on a continuous data collection from the sensors embedded in physical assets. This information is sent to a cloud or edge-based platform for analysis and visualization. An engineer or a decision maker uses these simulations for testing changes in operation, predicting failure and optimizing performance without the risk of damaging the actual device. Some of the industries that are currently taking advantage of digital twins are:

- Smart manufacturing plants
- The electricity generation and transmission infrastructure. The electricity generation and transmission grid.
- Oil/gas facilities
- Transportation systems
- Aerospace engineering
- Global supply chains

These systems are extremely intelligent, with the addition of artificial intelligence and machine learning. They can predict equipment failures, simulate environments and even suggest corrective actions. But that intelligence is solely based on accurate and trustworthy data.

The Cybersecurity Blind Spot

Most of the organizations invest a lot of their time and efforts to secure their operational technology (OT) systems and IT networks. Physical systems are protected by firewalls, endpoint detection systems and intrusion



monitoring. Digital twins, however, are typically stored in cloud platforms that communicate with each other through API, IoT gateways and third-party services. This additional attack area gives rise to several vulnerabilities.

Unlike the traditional systems, a digital twin is not only a place of data but it also guides decision making. Once the twin is accessed, attackers can manipulate simulation outputs, forge predictive analytics and/or insert bogus sensor readings. Potential Attack Scenarios:

1. Manipulated Simulation Data

Engineers may assume systems are safe if a cyber attacker alters any of the temperature, load or pressure parameters in the digital twin. This can result in the equipment breaking.

2. False Predictive Maintenance Alerts

A hacker could send spurious maintenance alerts that would force equipment to stop working and result in lost revenue. But on the other hand, they could dampen down true warnings, enabling the systems to fail.

5. Intellectual Property Theft

Digital twins may include designs, performance models, and operating information that are proprietary to the company. If there's a breach, it could lead to the disclosure of sensitive industrial information.

Will fake simulation data create a real-world disaster?

Yes. The primary risk is that of decision dependency. If executives and engineers are making operational decisions based on a digital twin dashboard, then inaccurate data can have real-world repercussions.

If a digital twin incorrectly reports that a structure is safe to operate, for instance, then the infrastructure can continue to operate in an unsafe condition. In aviation or power generation, these errors can have very serious economic and safety consequences.

Digital twins have the power to make the line between cyber and physical systems indistinct. It doesn't have to be an attack that has direct control on the hardware as manipulating the virtual layer can be sufficient to cause disruption.

Key Vulnerabilities of Digital Twin Systems

- The lack of secure communication between IoT devices. Insecure communication between IoT devices.
- Support for weak authentication methods
- Cloud misconfigurations
- The lack of adequate encryption of real-time data streams. The lack of the adequate encryption of real-time data streams.
- Third-party integration risks
- A lack of Zero Trust architecture implementation.

Future of Digital Twin Security

Digital twins will play a pivotal role in the smart factories and intelligent infrastructure of Industry 4.0 as it expands. More reliance on digital replicas will grow as IoT, AI and cloud come together.

But the strategies for cybersecurity need to be evolving at the same time. Specific guidelines and standards for digital twin security are in the process of development. There is a need for governments and technology providers to focus on frameworks that include both the physical and cyber risk aspects.

Businesses that don't address this blind spot could face disruptions in operations, losses of money and reputation. Organizations that act now to establish digital twin ecosystems will have a competitive edge and operational resilience.



Conclusion

Digital twins are one of the most game-changing innovations of the current industry. They facilitate predictive intelligence, cost efficiency, and safe experimentation. They, however, bring in a new category of cyber-physical vulnerabilities when incorporated into critical infrastructure.

Digital twins can mislead decision-making, lead to failure in operation, and even lead to a large-scale disruption in infrastructure if they are compromised. So, digital twins are not just analytics tools—they are mission-critical systems that need strong cybersecurity measures.

About the Author

Abdullah Tariq studying Software Engineering and is particularly interested in digital twin, cybersecurity, and future developments in decentralized data storage systems. He can be reached at abdullahtariq5044@gmail.com.

Keywords: Digital Twin; Cloud Server; Cyber Security; Software Engineering; Pakistan Tech

References

- [1] IBM Institute for Business Value. (2023). Digital Twin and Industrial Transformation Report.
- [2] Gartner Research. (2023). Security Considerations for Digital Twin Platforms.
- [3] NIST. (2024). Cyber-Physical Systems Security Framework.