Nexton Technologies

2025 TRENDS

Cybersecurity and Process Automation for the Automotive Industry

nextontech.io

2025 Trends in Cybersecurity and Process Automation for the Automotive Industry

The automotive industry is poised for significant transformation by 2025, with electric and autonomous vehicles (EVs and AEVs) driving the future of mobility.

According to recent projections, global electric vehicle sales are expected to reach nearly 25% of total vehicle sales by 2025, with autonomous driving technologies also gaining widespread adoption.

As vehicles become more intelligent and interconnected, automakers face growing concerns about cybersecurity and the need for greater automation in manufacturing processes. The threat of cyberattacks on connected vehicles and digital supply chains requires the industry to implement advanced defense mechanisms.

This report examines the key trends in cybersecurity and process automation that will shape the automotive landscape, with a focus on the cybersecurity challenges of autonomous electric vehicles (AEVs) and the electric car industry spotlight for 2025.

The Rise of Autonomous Electric Vehicules: A New Cybersecurity Landscape

The introduction of autonomous electric vehicles (AEVs) marks a milestone in automotive innovation. However, this also introduces new cybersecurity risks. AEVs rely heavily on vehicle-to-everything (V2X) communication, which allows vehicles to interact with each other, infrastructure, and pedestrians. These connections create multiple entry points for cybercriminals.

A notable example is the 2021 remote hacking of a Tesla vehicle by researchers at Keen Security Lab. They managed to exploit vulnerabilities in Tesla's autopilot system, remotely controlling the vehicle's steering and braking. This incident highlights the severity of cybersecurity threats in AEVs and how even advanced automakers are not immune to these challenges.

As the number of connected and autonomous vehicles on the road increases, so does the complexity of the threat landscape. Hackers can exploit vulnerabilities in sensors, cameras, and AI systems. In a future where fully autonomous vehicles navigate roads without human intervention, a cyberattack could result in catastrophic outcomes, including collisions and system failures.

Automakers are investing heavily in cybersecurity solutions such as AI-based threat detection, blockchain for secure data exchanges, and secure Over-The-Air (OTA) updates. These technologies are crucial to securing AEVs and preventing unauthorized access to sensitive systems.

Automation in Manufacturing: Revolutionizing Production Processes

Automation is revolutionizing automotive manufacturing, driven by advancements in robotics, artificial intelligence (AI), and the Internet of Things (IoT). Industry 4.0 technologies are enabling smart factories, where real-time data, predictive analytics, and robotics optimize production workflows.

At Tesla's Gigafactory in Nevada, automation plays a critical role in the company's production process. The factory uses advanced robotics to assemble batteries and vehicle components, significantly increasing production speed while minimizing human error. Robots handle tasks that require high precision, such as welding and component placement, contributing to overall efficiency.

AI-powered systems are also transforming quality control. At BMW's Munich plant, an AI-driven quality inspection system analyzes images of assembled parts to detect defects that are invisible to the human eye. By identifying potential issues early in the production process, manufacturers can reduce waste and avoid costly recalls.

Another breakthrough in manufacturing automation is the rise of collaborative robots, or cobots. Unlike traditional industrial robots, which operate in isolation, cobots work directly alongside human workers. They assist with repetitive tasks, such as material handling, assembly, and inspection. Cobots increase overall productivity while allowing human workers to focus on more complex tasks.

Securing the Supply Chain: Challenges and Solutions

The automotive supply chain is vast and complex, involving numerous suppliers and vendors. As automakers digitize their operations and integrate more technology into their vehicles, the supply chain becomes a critical area of vulnerability.

One of the most notable supply chain disruptions occurred in 2021 when a cyberattack on a key semiconductor supplier led to a global shortage of chips, forcing many automakers to halt production. This incident highlighted the fragility of the supply chain and underscored the importance of securing third-party vendors.

To mitigate supply chain risks, automakers are increasingly adopting multi-layered security strategies. Blockchain technology is gaining traction for its ability to provide transparency and traceability across the supply chain. By recording every transaction on an immutable ledger, automakers can verify the authenticity of parts and track their origin.

SUPPLY CHAIN SECURITY

Automakers are turning to blockchain for transparency and adopting zero-trust architectures to safeguard against growing cybersecurity threats.

In addition, many automakers are implementing “zero-trust” security architectures. This approach assumes that no user or system is trusted by default, regardless of whether they are inside or outside the network. By enforcing strict access controls and continuously monitoring for anomalies, automakers can reduce the likelihood of a supply chain breach

2025 Spotlight: The Electric Car Industry and its Challenges

The electric vehicle (EV) market is experiencing rapid growth, with automakers racing to develop more affordable, longer-range electric cars. However, this expansion brings its own set of challenges, including the need for improved battery technology and the development of a robust charging infrastructure.

Solid-state batteries, which promise higher energy density and faster charging times, are expected to be a game-changer for the EV industry. Automakers like Toyota and Volkswagen are investing heavily in solid-state battery research, with commercial deployment anticipated by 2025. These batteries could extend the range of EVs to over 600 miles on a single charge, making electric vehicles more competitive with gasoline-powered cars.

The expansion of charging infrastructure is another critical factor. While major cities in the US, Europe, and China are investing in fast-charging networks, rural and less-developed areas still face challenges in providing adequate coverage. In addition, cybersecurity concerns surrounding charging stations are growing. Hackers could target EV charging networks, disrupting services or even compromising the grid.

Governments are also playing a key role in accelerating EV adoption by offering incentives such as tax credits and subsidies for consumers and manufacturers. However, the global EV market faces challenges related to the availability of raw materials, such as lithium and cobalt, which are essential for battery production. Automakers are increasingly looking for ways to reduce their dependence on these materials by developing more sustainable battery technologies and recycling programs.

Regulatory and Compliance Considerations in 2025

As autonomous and electric vehicles reshape the automotive industry, governments and regulatory bodies are introducing new laws to ensure safety, data privacy, and environmental sustainability.

In the United States, the National Highway Traffic Safety Administration (NHTSA) is expected to introduce new cybersecurity standards for connected and autonomous vehicles by 2025. These regulations will require automakers to implement robust cybersecurity measures, including end-to-end encryption, secure software updates, and threat monitoring systems.

In Europe, the General Data Protection Regulation (GDPR) continues to have a significant impact on how automakers collect, store, and process personal data. Automakers must ensure that their connected vehicle platforms comply with GDPR's strict data privacy requirements, or face hefty fines.
Meanwhile, China is emerging as a global leader in EV adoption. The Chinese government has implemented aggressive emissions targets and is offering substantial subsidies to automakers that produce electric vehicles. However, foreign automakers entering the Chinese market must navigate complex regulatory frameworks and ensure compliance with local cybersecurity and data privacy laws

The automotive industry is set for a major transformation by 2025. As autonomous and electric vehicles rise, automakers must tackle cybersecurity, automation, and supply chain challenges. Technologies like AI-driven cybersecurity, quantum-resistant encryption, and blockchain will be key to protecting vehicles and infrastructure.

Evolving regulations will shape how companies secure and deploy these technologies. Those that adapt and comply will thrive in the digital future. Collaboration between governments, manufacturers, and tech providers is vital to creating a safe and sustainable automotive ecosystem.

Nexton Technologies

https://nextontech.io
info@nextontech.io