Letter from the Editor - July 2025

By: [Scott St. John - Pipeline](#)

The proliferation of connected devices permeates every aspect of our daily lives, and we may not even notice. Sure, we may know the PC on our desk, watch on our wrist, or the doorbell on our home may be connected to the internet. You may even have a connected device implanted in your body. But the explosion in IoT connected devices encompasses even more than that.

There is an IoT revolution underway. Recent estimates put the number of IoT connected devices at just under 20 billion. The cities we live in, streets we drive upon, cars we drive in, and the buildings and factories in which we work are all connected, and the momentum doesn't show any signs of slowing.

Today, enterprise robotics is opening the door to new, tangible use cases for a wide range of connected devices including hospitality, sanitization, security, and service robots. Deliveries by drone, robots, and autonomous cars will soon be commonplace. Both Walmart and Amazon are deploying drone delivery services, and Google's Waymo and Tesla's autonomous cars are being rolled out in key markets now.

The combination of robotics, Artificial Intelligence (AI), Augmented or Virtual Reality (AR/VR) devices, and digital twins, is transforming industries such as aerospace and automotive. Industrial robotic applications – such as Industry 4.0 and 5.0 – are continuing to pick up steam. The impact to engineering and manufacturing alone creates an incredible opportunity for companies looking to escape the high cost of tariffs by building in the United States – such as Nike, Apple, and Taiwan Semiconductor – while offsetting the historically high cost of labor.

Billions of connected IoT devices are now peppered throughout homes, businesses, and factories around the world. This creates tremendous new opportunities for monetization, and risks. For example, connected devices can open a window into your home or business, that can be publicly accessed by malfeasants. Not even your vacuum cleaner can be trusted. In 2020, it was alleged private bathroom photos of a woman taken by a Roomba vacuum, were posted to Facebook. In a Reddit post, Roomba claimed that the sensitive photos were leaked by Scale AI, a company that it uses to optimize its algorithms, and the photos were taken from test robots, not from commercially sold units. But still.

Trust, safety, and security are paramount as more companies and people are increasingly embracing connected devices. And it's not just virtual. As more companies roll out drone, robotic and autonomous delivery fleets, the risk of bodily injury or death may be at stake. Which are just a few of the reasons that make this edition of *Pipeline* so important.

In this issue of *Pipeline*, we explore IoT and the device revolution. RobotLAB provides us with real-world enterprise robotic applications. Avnu Alliance tells us how Time-Sensitive Networking (TSN) is being used for automotive, aerospace, and robotic IoT use cases. Gridraster illustrates how AI, AR/VR, cloud and digital twins are being used to streamline aerospace manufacturing. Telit Cinterion demonstrates how IoT, edge, and AI technologies are being used to enable smart buildings. SAS underscores the importance of trusted data for IoT and smart cities, and how AI can help. Iridium demonstrates how satellite and cellular connectivity can be combined to create new IoT opportunities. Apptium examines ways to harness the cloud for edge IoT monetization. *Pipeline*'s Dr. Mark Cummings shows us how Gen AI can be used to prevent drone collisions, and Digi provides methods to mitigate DIY IoT risks. In a special feature, we also give you a snapshot of what you might have missed at the DTW Ignite! 2025 event in Copenhagen. All this, plus the latest enterprise IT and telecommunications industry news and more.

We hope you enjoy this and every issue,

Scott St. John
Managing Editor
Pipeline

Follow on X | Follow on LinkedIn | Follow Pipeline