Hi everyone, and welcome to IoT Forge Unplugged podcast!

Every two weeks, we pick the most exciting news from the world of IoT and share them with you in this short podcast, where I break down the latest updates and trends. I’d love for you to get involved—whether it’s sharing feedback, suggesting news stories I might’ve missed (because, let’s be honest, my interests sometimes reflect my own hobbies), or joining the conversation about these updates.

So, let’s get started! Today is January 21, 2025, and this is our second episode of the year.

# CES

Let’s kick things off with CES 2025, which just wrapped up a few days ago. As always, this massive tech event was full of cutting-edge innovations, and IoT was no exception.  
CES 2025 gave us a glimpse into the future of IoT, and it’s clear the industry is evolving faster than ever. This year, a big focus was on making IoT devices smarter and more capable, especially with the integration of AI. Qualcomm made waves with its IQ Series, designed for IoT-specific hardware, and its Snapdragon Digital Chassis, aimed at transforming connected vehicles. Meanwhile, Alif Semiconductor showcased its new Ensemble microcontrollers, now enhanced with Arm's Ethos-U85 NPU. These upgrades are all about bringing advanced AI capabilities right to the edge, where data is generated and processed.

Speaking of vehicles, autonomous driving was front and center. NVIDIA unveiled its DRIVE AGX Thor system, a game-changer powered by Arm Neoverse V3AE CPU cores. This technology is set to hit production vehicles later this year, with automakers like Jaguar Land Rover, Mercedes-Benz, and Volvo already onboard. It’s not just about self-driving; it’s about rethinking the car as a software-defined platform, with constant updates and new features long after it rolls off the lot.

Connectivity also took a big leap forward. Satellite IoT was everywhere, with companies like Globalstar and Skylo talking about hybrid solutions that combine cellular networks with low Earth orbit satellites. Release 17 NTN, a new standard for satellite IoT, and innovations in eSIM technology also made headlines, promising more flexible and reliable connectivity for devices in even the most remote locations.

And let’s not forget the wearables. New AR glasses like ThinkAR’s AiLens and XREAL’s One Series are pushing the boundaries of what’s possible in lightweight, AI-powered designs. These aren’t just gadgets; they’re tools with real-world applications, from productivity to entertainment.

Finally, the IoT ecosystem itself is maturing. Qualcomm emphasized its efforts to streamline IoT adoption in industries like retail and logistics while refreshing its Qualcomm Aware platform for asset management and device monitoring. What stood out is how the industry is shifting—moving beyond standalone devices to integrated, vertical-specific solutions that address real-world problems.

CES 2025 was a clear reminder: IoT is no longer just about connecting devices. It’s about rethinking how we live, work, and interact with the world.

# NB Decline

Now, let’s shift gears and talk about an intriguing trend reversal in the IoT space. While the industry is abuzz with innovation, not all technologies are moving forward as expected. Take Narrowband IoT,, for example—a technology once touted as a game-changer for low-power, wide-area IoT deployments.

Recently, AT&T announced its decision to phase out its NB-IoT network in the US. This isn’t just a minor tweak in their IoT strategy—it’s a complete shift. They’ve already stopped selling NB-IoT data plans and certifying devices, with the entire decommissioning process expected to wrap up by early this year. According to AT&T, this move is aimed at "improving" their IoT services for enterprise customers by transitioning them to LTE-M, which they say offers more data capacity for both fixed and mobile devices.

So, why is this happening? There are several underlying factors pointing to a broader decline in the adoption of NB-IoT.

First, AT&T’s exit signals a lack of long-term confidence in NB-IoT, and their influence in the market makes this announcement particularly impactful. But they’re not the only ones. Other operators have reportedly been hesitant to launch NB-IoT networks, citing high implementation costs and uncertain returns on investment.

Second, the financial landscape for mobile network operators (MNOs) has changed drastically. The steady decline in data prices over the years has put significant pressure on MNOs, making it harder to sustain technologies like NB-IoT.

Finally, NB-IoT’s complexity and lack of backward compatibility for global deployments further complicate its adoption. For both customers and operators, the business case for NB-IoT is increasingly difficult to justify, especially when alternative technologies like LTE-M offer greater flexibility and scalability.

In essence, while NB-IoT was designed to power the next generation of low-power IoT devices, its future now seems uncertain. It’s a stark reminder that not every promising technology will find its place in the evolving IoT ecosystem. Sometimes, the market pivots faster than the technology itself can adapt.

And that brings us to an interesting question: What does this mean for other emerging IoT technologies? Are we headed toward a more consolidated landscape where only a few standards dominate? Food for thought as we continue to watch the space evolve.

# Security

And finally, let’s talk about IoT device security, an essential but often overlooked aspect of the industry. A recent article titled *"How to Streamline the IoT Security Lifecycle"* by David Haslam, published by Crypto Quantique, provides an excellent overview of how to safeguard IoT traffic and the methods behind it.

The piece emphasizes that IoT security is a lifecycle challenge, spanning the journey of a device from manufacturing to its end of life. Each stage requires meticulous attention to ensure devices remain secure. For example, secure boot processes, flash encryption, and the use of Public Key Infrastructure (PKI) are critical tools in preventing firmware or data compromises. PKI ensures that every IoT device has a unique, verifiable identity, authenticated through certificates that create a trusted chain back to the manufacturer.

Interestingly, the concept of "late binding" allows IoT devices to enroll into networks well after manufacturing. This flexibility is a huge advantage but requires robust security measures like hardware security modules (HSMs) to prevent attacks during the initial provisioning of encryption keys and certificates.

The article also highlights how OTA (over-the-air) updates play a vital role in maintaining security. These updates need to be carefully managed, ensuring only authenticated devices receive the correct updates while preventing adversaries from exploiting outdated software.

IoT security is complex, but as this article demonstrates, it’s achievable with the right tools and mindset. It’s a crucial reminder that while innovation drives the IoT space, robust security ensures it thrives.

# Wrap up

And that’s a wrap for today’s episode! As always you will find all the links in the description. I hope you enjoyed the insights and updates we shared. Whether you’re exploring the latest IoT innovations or grappling with the challenges of evolving technologies, remember—this podcast is here to keep you informed and inspired.

Don’t forget, your voice matters! If you’ve got news, feedback, or ideas you’d like to share, I’d love to hear from you. This is a community-driven space, and your input helps make it even better.

A quick note: I always strive to bring you fresh, relevant content while steering clear of overlap with our biweekly IoTuesday brown bag sessions. Mark your calendar—we’ll be back in two weeks with more exciting updates, thought-provoking articles, and expert insights.

And if you haven’t already, check out **IoT Forge**—our vibrant community for learning, sharing, and connecting with like-minded enthusiasts. It’s a great place to take your IoT journey to the next level.

Until next time, stay curious, keep innovating, and take care. Cheers!