July 15, 2024

Actelis Featured in Forbes Article: The Interplay Of IoT And Critical Infrastructure Security

Author: David Balaban

Source: The Interplay Of IoT And Critical Infrastructure Security (forbes.com)

Published July 14, 2024

When it comes to technology, what seemed to be science fiction several decades ago can now be a mundane thing everyone takes for granted. Could we have imagined in the early 2000s that entire economic sectors would operate in near-autonomous ways under a watchful eye of monitoring sensors, cameras, and a myriad of other connected devices collectively dubbed the Internet of Things (IoT)?

Once a prerogative of incorrigible enthusiasts and dreamers, this hi-tech reality is already here. In areas where human input used to be key, the onus has largely shifted towards internet-enabled devices that provide real-time data collection, remote monitoring, and automation. The number of these objects is predicted to exceed 29 billion by 2030 globally, twice the stats for 2020.

Out of all the domains that IoT has revolutionized, critical infrastructure stands apart as a particularly tangible intersection of the digital and physical worlds. Today, it enhances operational efficiency, reduces costs, and steps up service reliability of electrical grids, municipal utilities, transportation systems, manufacturing entities, military facilities, airports, and more.

This technological leap, predictably enough, comes with its challenges. First, deploying seamless IoT networks over long distances can require hefty engineering, construction, and investment to upgrade the existing wiring infrastructure or even build it from the ground up. Second, operating such networks is a tightrope to walk in terms of security, given the high-stakes assets at the heart of them.

The Cybersecurity Achilles Heel

The vast number of interconnected devices in an IoT-driven infrastructure creates a massive attack surface. These objects often have limited processing power and may miss out on robust security features, which potentially makes them easy targets. Here's a closer look at the specific concerns that shape up the unique threat model of an ecosystem like that:

- **Unauthorized access:** Many IoT devices have notoriously weak authentication protocols and are shipped with easy-to-guess default passwords that network

administrators neglect to change. This leaves them vulnerable to brute-force attacks or credential stuffing.

- **Data breaches:** Without strong encryption in place, sensitive data transmitted between devices and control centers can be intercepted and mishandled.
- **Denial of Service (DoS):** IoT networks can be swamped by malformed queries whose number exceeds the server's processing capacity. This can result in significant downtime and operational issues that end up disrupting critical services.
- **Software vulnerabilities:** Outdated firmware and software on these devices can harbor unpatched security gaps, creating entry points for cyberattacks.

The catch-all thing to understand is that the very nature of interconnectedness creates vulnerabilities. Perpetrators targeting a single device could gain access to a wider network, potentially causing widespread disruptions.

IoT Security Done Right

As cyber threats evolve, overconfidence in defenses at the network perimeter can be a losing strategy. Even with top-notch proactive security measures in place, there's always a chance of well-motivated adversaries breaking in. It's best to prevent them from weaponizing the data they might intercept, in the first place. Call it a plan B, if you will, but it eventually pays off in today's nuanced cyberspace.

A good example of how this works is the logic leveraged by Actelis Networks, a global provider of cyber-hardened, quick-deployment networking solutions for utility, transportation, military, telecom, as well as federal, state, and local government IoT applications. What drew my attention is that their security philosophy combines three layers of protection: end-to-end data encryption with MACsec 256-bit cryptographic standard, data fragmentation, and scrambling.

This means that to cause damage, a malicious actor would need to amass information from all nodes on the network in order to de-scramble it, put the fragments together in the correct order, and decrypt the resulting data with a unique key to make it meaningful. Anyone even remotely familiar with cryptography knows that this mission is close to impossible.

With the well-thought-out security approach (dubbed the Triple Shield) and a breakthrough hybrid-fiber network deployment principle, Actelis is the only company of its kind to be included on the U.S. Department of Defense Information Network (DoDIN) approved products list (APL). This achievement, combined with NIST certification for FIPS 140-2 cryptographic standard, has predictably paved the provider's way towards new niches and projects.

In early June, the company received orders to modernize three U.S. military bases with its secure networking technology. These developments came amid escalating geopolitical tensions manifesting themselves through increased cyberattacks on critical infrastructure. The trend of growing investment in military cybersecurity mirrors broader federal efforts in addressing such concerns. With its DoDIN APL and NIST credentials, as well as proprietary technology in its toolkit, Actelis is in a position to get such initiatives rolling.

"At Actelis Networks, we recognize that robust security requires more than just strong encryption. Our Triple Shield approach integrates end-to-end data encryption, data

fragmentation, and scrambling to create a multi-layered defense system. This ensures that even if one layer is compromised, the data remains protected through additional layers of security," says Tuvia Barlev, Chairman and CEO of Actelis. "By combining these techniques, we make it exceptionally difficult for malicious actors to access and exploit sensitive information, maintaining the integrity and confidentiality of our clients' critical infrastructure," he added.

What's Next for IoT-Driven Critical Infrastructure?

While security is crucial for networks that underlie critical infrastructure, enabling uninterrupted connectivity between IoT devices is another nontrivial challenge. This is especially true of geographically scattered environments that combine fiber, coax, and legacy copper wiring.

The silver lining is that such heterogeneous cabling architectures can be glued together to deliver fiber-grade connectivity without the need to build new high-cost networks from scratch. An illustration of this tactic is Actelis' hybrid-fiber technology harnessing high-performance managed Ethernet access switches and extenders to make the most of existing network infrastructures and provide gigabit speeds via virtually any wireline media. Actelis' hybrid-fiber networking concept includes sections of fiber (for the easy-to-reach-with-fiber locations) and copper/coax that can be upgraded with Actelis' technology to run fiber-grade communication. The company does both and provides management, security, and end-to-end integration for such entire networks, including fiber parts. This is important, as it represents a significant part of the market, selling both fiber and non-fiber networking.

Barlev highlights that "The beauty of Actelis' hybrid-fiber technology lies in its ability to utilize existing network infrastructures to deliver high-speed connectivity. By integrating managed Ethernet access switches and extenders, we can achieve gigabit speeds over virtually any wireline media. This approach not only reduces deployment costs and time but also ensures that our clients can quickly and effectively modernize their networks without the need for extensive new construction."

Connectivity is the major cost and time component in any such IoT modernization project. Actelis' ability to provide power remotely to sensors and cameras over copper/coax is a major cost and time-saving component as well.

As the IoT element becomes instrumental in modernizing critical infrastructure across multiple industries, innovative network design principles come to the fore. The key challenge here is to avoid a tradeoff between deployment speed, ease of maintenance, and security. A safe world without serious technology-borne societal repercussions seems to be a matter of striking that balance for the long haul.

Follow David Balaban on LinkedIn.

Check out David Balaban's website.