On Behalf of LATTICE SEMICONDUCTOR

Bringing Security to 5G ORAN Deployments

By Bob O'Donnell, TECHnalysis Research President

SUMMARY

One of the most interesting and exciting aspects of the evolution to 5G networks is the simultaneous move to open radio access network, or ORAN architectures. Unlike the proprietary architectures that have dominated cellular networks since their inception, ORAN-based networks offer the flexibility of creating best-of-breed solutions by combining elements from multiple vendors. This gives telco companies and other service providers the ability to adapt more quickly, lower their costs, and implement new features and technologies faster and more easily. However, by moving away from a single-vendor solution, they also increase the potential attack surface and open the possibility of security risks to critical infrastructure. To avoid these issues, network equipment vendors and service providers need to think through what elements are necessary to ensure that their networks and the data passing through them remain safe and secure. One critical piece that can be easily overlooked are low-power FPGAs, which can be used for everything from hardware root-of-trust, network function acceleration, and secure communications in an ORAN environment.

> "Building a secure, zero-trust based hardware device in the flexible world of ORAN network architectures requires looking at the smallest of details and low-power FPGAs can play a critical role at many parts of the chain."—Bob O'Donnell, Chief Analyst

INTRODUCTION

When it comes to today's very complex technologies, one of the most important aspects to consider is flexibility. Whether flying people into space, helping navigate the challenge of autonomous driving, or trying to build the infrastructure necessary to power 5G cellular networks, hardware design engineers are always eager to consider component parts that not only provide the functionality they need, but also give them multiple ways to achieve their desired end. That's why FPGAs (Field Programmable Gate Arrays) are such an important part of so many of these types of immensely complex efforts. These chips' inherent ability to be designed and re-designed to provide certain key functions makes them uniquely suited to fit the specific and demanding needs that so many advanced technologies require.

In the case of telecom networks, FPGAs of various types have been relied on for decades to do things like help accelerate network functions, move data across the wire, and much more. Now, as the industry is beginning its transition to Open RAN (Radio Access Network)-type architectures, FPGAs, particularly low-power ones, are once again proving their value for applications like serving as a hardware root-of-trust, synchronization across multiple components, real-time network packet encryption and decryption, and much more.

Before getting into the details, however, it's worth taking a brief step back to understand how cellular networks have evolved and how the transition to virtualized, software-defined, open standard-driven networks has created both new opportunities and new challenges.

NETWORK EVOLUTION

Until recently, major network equipment suppliers like Ericsson, Nokia and Samsung Networks built extremely complex proprietary solutions that allowed the magic of cellular communications and wireless data to blanket the world. With few exceptions, these devices offered no interoperability with equipment from other vendors, forcing telco vendors to rely on a single source for each of their regional subnetworks. Given the inherent complexity of RF (radio frequency) signaling and the relatively fixed nature of the capabilities that each generation of cellular technology offered, most considered this a reasonable solution, despite its inherent limitations. In fact, as a result of the closed-loop, proprietary nature of these systems, some even believed they had a security advantage—because they didn't really have to worry much about security within their own private worlds.

However, a confluence of multiple, overlapping trends gave rise to the concept that a new more flexible, more adaptable means of building cellular networks was needed. First, there was the transition to 5G, a network type that added a range of new frequencies, placed significantly higher expectations on the number and types of devices that were to be connected to the network, and offered the potential for important reductions in latency for data travelling over the network. In addition, within traditional telco environments, the move toward software-defined architectures became apparent, as did the disaggregation of certain key network hardware elements. The standard baseband unit that powered every cell phone tower on previous generation networks, for example, was split into a DU (Distributed Unit), CU (Control Unit) and RU (Radio Unit). This new structure provides more specialized capabilities and flexible architectures as network data traffic and application demands increase.

Next generation networks also brought with them new requirements for functionality such as network slicing (where data packets for an individual organization or even user are digitally cordoned off from other network traffic to reduce latency, improve performance and provide better overall service). Finally, the availability of significantly faster general purpose computing hardware and specialized accelerators that could meet the demands of network performance set the stage for a major transformation of network architectures.

While it’s still in early stages, telcos all over the world are adopting the use of COTS (Commercial Off The Shelf) server hardware from companies like Dell Technologies, HPE, and Lenovo along with software from major players like Microsoft, IBM and Nvidia as well as a host of smaller companies like Mavenir, Altiostar, and Accelleran to power portions of their networks.

Initially, most software-based efforts have been focused on virtualizing network resources, much as virtualization drove the evolution and re-architecting of data centers for the last few decades. With the development of specialized software and, critically, the establishment of open standards for connectivity between cellular network equipment components, however, it’s now possible to piece together cellular networks in entirely new ways. It’s also possible to leverage new software development methodologies like CI/CD (Continuous Innovation/Continuous Delivery) and cloud-native, containerized software architectures to dramatically speed up the pace of innovation. Because of the critical, utility-level reliability that telcos demand, the complete network transformation will likely take a decade or more to complete. The first steps have been completed, however, and that in turn has raised new types of concerns that inevitably come from piecing together elements from different vendors.

SECURING THE CONNECTIONS

Chief among these concerns are security-related issues. While moving to an ORAN architecture opens up new degrees of flexibility, it also dramatically increases the potential attack surface for a network. Not only is it possible to mix and match hardware and software from different vendors, but the individual elements within a piece of hardware—such as a PCI-based accelerator card inside a server—can be selected from several choices. As a result, network architects and hardware designers must think through every possible connection and ensure that each of those connections is safe and secure. In addition, designers must be certain that the base firmware in each piece of hardware hasn't been tampered with.

To achieve this, multiple different security solutions are needed to tackle each of the different requirements. Step one entails having each piece of equipment attest to its veracity on startup via a hardware root of trust and confirming that the firmware on the device has not been changed. Low-power, security-focused FPGAs such as the Nexus™ platform from Lattice Semiconductor alongside the Lattice Sentry™ solution stack provide platform firmware resiliency (PFR). Hardware companies have been using these capabilities in servers and other critical equipment for many years now and they are being leveraged for ORAN focused hardware as well. In addition, a hardware root of trust can be leveraged to provide attestation that no changes or alterations were made to the device from the time it was built to the time it was delivered and installed, ensuring that cloning, counterfeiting, trojan insertion or any other issue did not occur throughout the supply chain. Finally, thanks to built-in cryptographic capabilities, these low-power FPGAs can encrypt and decrypt data going from and to the firmware, again assuring that firmware updates are performed securely.

The next step in the security chain is securely communicating with any components within a piece of hardware that might be connected to the host CPU or, to put it more succinctly, to "secure the wire". Leveraging a zero trust-based security model, each component needs to confirm its authenticity to the host system, using encrypted messages to do so. This is where the new Lattice ORAN™ solution stack starts to kick in as it can provide secure communications over PCI and other buses to connect the host with these elements. Like the company's other offerings, Lattice ORAN Stack is a comprehensive solution from custom design services, reference design and demos, software tools, IP cores, and hardware platforms that are optimized for a small, low-power FPGA. Designed to be easy to integrate into many hardware designs, it includes a RISC-powered CPU core that can be programmed to implement various cryptographic and secure messaging protocols. In addition, it's specifically designed to co-exist with their Lattice Sentry solution stack to extend the security features of devices which include both of them.

SYNCHRONIZING THE DATA

In addition to securing the hardware elements in an ORAN solution, it's also essential to make sure that the timing of the data being sent across elements remains in lock-step. The reason this is a concern comes back to the disaggregation of the core network elements discussed earlier. In particular, the separation of the radio unit (RU) and the distributed unit (DU) created challenges that needed to be addressed. With traditional closed networks, analog radio signals are received at the antennas attached to the radio elements, then are converted into digital form. After that, several real-time digital signal processing steps are performed on the data to enable functions that are an essential part of modern cellular networks, such as carrier aggregation—which bonds signals coming in at different frequencies into a single "aggregated" chunk of digital data. In an ORAN environment, the same types of steps have to occur. However, while the older proprietary systems had a shared clock signal with which to coordinate these efforts, the ORAN environment has to essentially time stamp the data packets using the IEE1588 standard so that they can be synchronized across components.

Because of the concurrent and consistent manner with which FPGAs operate, they have been used as an ultra-reliable timing resource in many different applications. As a result, they are well-suited to the synchronization demands of ORAN network architectures and specifically the need for functional-split options where the RU and DU are separated. As result, Lattice plans to extend their ORAN solution stack later this year to incorporate these types of timing-based functions. In particular, they intend to add timing and synchronization services capabilities to help with fronthaul connections between the RU and the DU over standard eCPRI (Enhanced Common Public Radio Interface) links.

In addition, because that connection is not secure, Lattice also intends to accelerate the MACsec functions need to encrypt and decrypt Ethernet packets over that connection. Unlike larger FPGAs that have been used in traditional networking equipment for years, however, the Lattice FPGAs on which the stack is implemented are tiny, low power devices that makes them well-suited for many types of applications, including power-sensitive small cell applications, which are an increasingly important part of modern 5G networks.

CONCLUSIONS AND RECOMMENDATIONS

As we witnessed with data center and cloud computing architectures over the last few decades, the world of cellular networks is now evolving from a proprietary hardware-driven world to one being defined by software-driven, virtualized, containerized, and standardized APIs that are unlocking new potential. Companies are looking for the flexibility, speed, and choice that these new types of architectures enable in an effort to make cellular networks more functional and more adaptable. With the rise of 5G, telcos are being driven by the vision of evolving from simple pipe providers to the purveyors of sophisticated and profitable services that can be tailored to the unique demands of different industries and different types of consumers.

Making the transition isn't easy or fast; however, and there are a number of key issues that have to be addressed to ensure that they can achieve these new goals while still retaining the incredibly reliable state of operation they now offer. Key among these is the need for securing the devices, the interconnections, and the data that crosses all these various components. In particular, it's essential to secure the data in transit, in use and at rest so that these more flexible architectures can be as safe as the proprietary ones they've started to displace.

Achieving the trust to make that move requires looking at the smallest of details and ensuring that all aspects of the solution are fulfilling their role. Complete security solutions built on small, lower power FPGAs can play a critical, though little seen role in making that happen. The trick is to ensure that network designers are thinking through all the elements they need to build solutions that can offer the flexibility that telcos want while still giving them the security, synchronization, and the low power acceleration they demand.