Viewpoint BY JAMES S.B. CHEW

Taking the Right Steps: Understanding 5G for the DoD

A recent Pentagon announcement focusing on 5G network capabilities — based on a Defense Science Board 5G study — will no doubt create many overnight "experts" in the telecommunications field. However, the office of the undersecretary for research and engineering wisely stated that the significant commercial investment in this area should be leveraged.

The importance of leveraging this investment cannot be overstated — the commercial mindset is to be first to market with a reliable, affordable, "crazy great" product and/or capability. It would be fair to say that this is not the Defense Department acquisition process mindset.

For all those clamoring to climb aboard this 5G train, it would behoove all to carefully read the report and take note of this finding: "5G capability is inexorably intertwined with leading-edge microelectronics."

The historical mismatch between trust and assurance policies versus national investment in advanced semiconductor manufacturing has led to a fundamental capability deficit. Simply speaking, the current defense industrial base electronic system development approach and technologies will not work for 5G. Classic field programmable gate-array technologies will not allow for practical or efficient 5G, and the current

> "5G capability is inexorably intertwined with leading-edge microelectronics."

"test, fix, test" electronics development approach will not allow for timely operational capability development.

The first concept to grasp is that 5G isn't just 4G plus one. Yes, 5G enhanced mobile broadband will deliver 10X better performance, but 5G ultra-reliable low-latency communications is designed to deliver extremely short response times, and 5G massive machine-type communications provides for huge numbers of sensor and internet-of-things connections.

5G can enable a whole slew of new applications that 4G simply cannot, and it will come down to working out how to utilize these new capabilities. But there are also challenges, as all these benefits aren't just coming for free. Unlike 4G, there are a variety of different frequencies that 5G will need to get these jobs done. A lot of focus is on the mmWave frequencies — typically 28GHz and above — that deliver most of the 10X data performance, but these frequencies also have a very short reach, no more than 200 meters, which limits their use unless transmitting and receiving equipment can be kept at close quarters. For urban users, this means a lot more equipment installed on buildings, on lamp poles, etc., compared to what we have seen with 4G. For the lower 5G frequencies, the reach is much farther, over several kilometers.

In the context of DoD-type applications, 5G's combination of latency and bandwidth will, for instance, enable never-before-seen augmented reality for the soldier in the battlefield, supporting real-time decision-making. Security and safety are, of course, paramount, so in the 5G world, network operators are already planning for custom networks for industrial applications. Military applications will require similar customization.

As one can imagine, connecting all this new transmitting and receiving equipment to the cloud is going to take a lot of high-speed optical fiber to take the data traffic back and forth, or microwave repeaters if you have line of sight. But it's still typically a long way to the data centers we think of as the cloud, and this becomes a bottleneck if we're trying to get extremely short response times. For urban users, the solution is to bring the cloud capabilities closer to the users, with new edge computing centers dotted around cities, to keep those optical fibers short.

For the military, the solution may be to make the optical fibers even shorter by putting the edge computing and transmitting and receiving equipment together in a mobile vehicle. This vehicle can be connected to remote data or command centers via satellite link.

A fundamental advantage of the mobile vehicle is there is no reliance on equipment already installed in a given region, which could be compromised.

This close-at-hand computing power and the short response times of the 5G protocols will enable augmented reality, for instance, where data and the real world can be blended in a warfighter's field of vision. It means the warfighter is no longer responsible for carrying the compute power, as the computer's heavy-lifting is now done elsewhere, but data and decisions provided to the user are in real time.

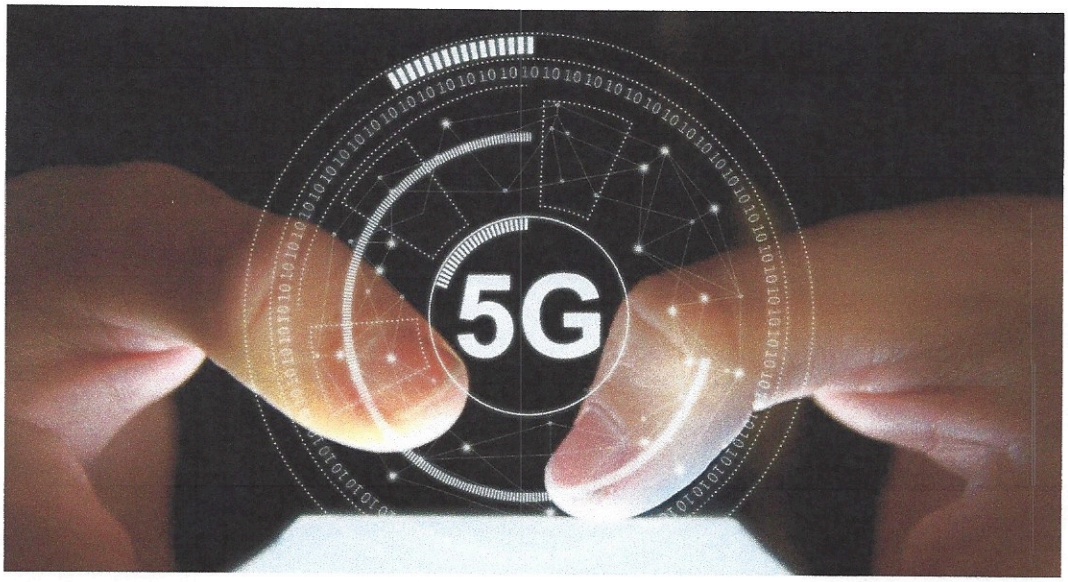
This idea of real-time decision-making, based on information from sensors such as visual cameras, thermal cameras, lidar or radar, is being driven by the explosive progress in artificial intelligence. Much of the compute power and new processors for AI at the edge will be dedicated to processing the data from the user's sensors and providing guidance and decisions in an augmented reality.

AI already has a significant impact in mobile devices that serves as a glimpse into the broader future of intelligent edge computing through 5G. Deloitte has estimated that half a billion smartphones, tablets and other mobile devices use onboard AI chips. This is the first wave of AI on the edge, with 5G opening up additional waves that will proliferate artificial intelligence to a whole new range of consumer and commercial use models across equipment, machines and distributed sensor networks, such as IoT. These next waves, like their smartphone counterparts, will require continual improvements in power consumption and reliability.

In fact, a study by ABI Research forecasts that 43 percent of all AI inference will be done on edge devices with a range of use models that span a variety of requirements in terms of power and compute needs. Today, the edge is limited by the latency in transferring edge data to the cloud for both inference and training. The ramp of 5G will fuel the growth of AI-based edge computing in devices, machines and systems all around us, creating pervasive intelligence.

The term "intelligence" is not used lightly here. One of the early challenges for edge computing, and IoT in particular, has been the inability for deployed systems to be flexible and adaptive to their environment. IoT and other edge-compute technologies may work great in a controlled laboratory setting but not work nearly as well in a broad range of industrial or outdoor environments. As such, the persons responsible for these deployments have also experienced the harsh challenge of "test, fix, test," which is even more challenging when scaled up to a massively distributed network of interconnected components. All of this capability necessitates the use of leading-edge semiconductor manufacturing that provides the only path to tight power and performance envelopes required for the warfighters.

To address this, IoT and other edge devices will need to independently detect and adapt to changes in their environment; in other words, they need the ability to learn as well as infer. This will require continual improvements to existing chip designs and architectures to allow them to more efficiently compute AI software algorithms in terms of power and performance. As intelligence is embedded into these devices and their associated gateways, these large interconnected networks of systems communicating through 5G become adaptive as well. Thus, the proliferation of 5G and AI technologies will usher in a new wave of pervasive intelligence in the connected world.



ISTOCK

While the promise of 5G-enabled intelligent systems and devices seems attractive, pervasive intelligence does not come without risks. There is a commensurate responsibility to verify that these intelligent systems don't evolve in ways that are unintended or create risk for others. Verification of AI software and hardware to ensure overall system robustness is a growing concern that requires more investment and attention into the verification of intelligent systems and the combined use of 5G-driven AI.

So where do leading-edge microelectronics play in the 5G ecosystem?

The different parts of the 5G ecosystem play together to enable new capabilities not possible with 4G, but these different parts are all different flavors of microelectronics. There is a parallel microelectronics industry ecosystem, with designers of semiconductor chips for AI, baseband, RF, antennas, photonics and graphics that integrators assemble into targeted microelectronics solutions. But key parts of this supply chain are not domestic, and this is something that must be addressed. For the military to be able to reason about what goes into their systems, they should understand the microelectronics and the products used from the semiconductor supply chain. And, where necessary, they need to source or design their own.

5G is being rolled out as a civilian infrastructure, but the 5G protocols can be readily re-purposed for other applications, supported by a more mobile and secure 5G infrastructure.

From a development perspective, the electronic design automation and technical software industries are already widely used in the commercial world to enable the development and integration of semiconductor IP, systems-on-chip, systems and systems of systems, hardware and software. Given the complexity of these networks, system simulation, virtual and physical prototyping and emulation are necessary to ensure functional correctness of infrastructure and devices prior to fabrication.

Additionally, this allows for the integration of software and hardware at the earliest possible time during development. Commercial best practices can readily be adopted and transferred to aerospace and defense applications. The development ecosystem also includes electronic design automation-adjacent areas like secure, safe software development as well as network and device testing as an extension to the familiar test environments from the 3G and 4G worlds. They typically use physical testers in addition to virtual connections to allow testing to happen in a "shift-left" fashion well before silicon is physically available. This investment includes interleaving security and safety functionality into the verification process.

As noted, 5G can enable a whole slew of new applications, and the first step is to work those out and understand the microelectronics infrastructure they will need. That's going to require experts in microelectronic and semiconductors on the payroll who can assess what's already out there, what can be securely repurposed and what needs to be redesigned.

This same microelectronics and semiconductor design enablement will be needed by those who are looking at what works and what doesn't work for new 5G applications. ND

James S.B. Chew is chair of NDIA's Science and Technology Division and group director of aerospace and defense at Cadence Design Systems. Ian Dennsion, David White, Frank Schirrmeister and Steve Carlson of Cadence contributed to this article.