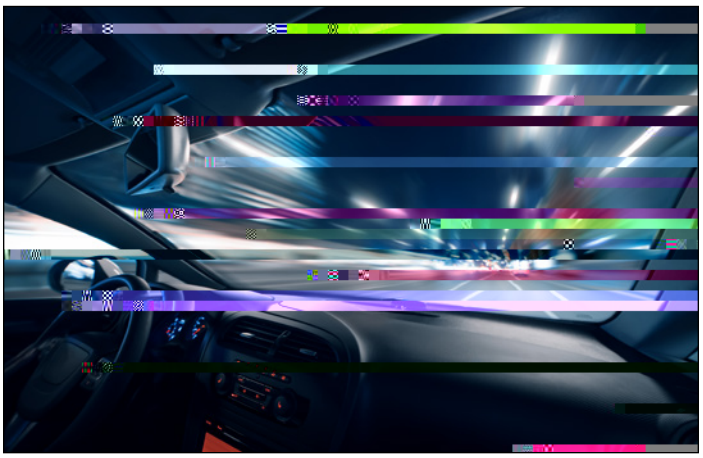
SYNOPSYS



These shortages have caused chaos on the assembly line. As of December 2022, U.S. automakers had an improving 1.8 million units of inventory on the ground, a half-million more vehicles than at the end of September, but with 58 days' supply, still less than the industry norm. At the end of December 2020, supply stood at 2.87 million vehicles (a 68-days supply) — and for pre-pandemic November 2019, U.S. inventory stood at 3.50 million vehicles (an 82-days supply), according to Cox Automotive (Figure 1). Where a 60- to 70-day supply of vehicles is considered normal, the industry average at the end of 2022 was 58 days — although that nonetheless was the highest inventory since March 2021, said Cox. Toyota finished 2022 with the lowest inventory of any brand, at around 25-days supply.

"None of us has ever seen anything like this," said Bob Carter, Toyota Motor North America Executive Vice President, Sales, during the company's first-quarter 2022 earnings call with the media. Even if semiconductor supplies reach more traditional levels, it will take time for factories to catch up with demand, meaning it will likely take until "late in 2023, perhaps the third quarter," added Carter, before things return of anything close to "normal."

Ongoing supply chain disruptions aren't just leading to inventory shortages; they're having a major impact on costs, both at the factory and retail levels. Production costs have, on some models, risen by $5,000 or more since the pandemic began, a figure compounded by surging raw material prices. For consumers, average transaction prices are setting new records seemingly every month. Average transaction prices — the average of prices paid for all new light vehicles — hit a record $49,507 in December 2022.

/ A

Today's vehicles are more impressive than those of the previous generation, and it's safe to assume the next generation will continue the pattern.

Once a collection of simple wiring harnesses supplying power to electronics like turn signals and radios, the electric/electronic architectures of modern vehicles is complex collection of hardware, network communications, software, wiring, sensors and more.

They not only allow the driver to indicate what direction they plan to turn or get the latest traffic report, now users can ask for directions to their favorite restaurant, get live traffic updates to avoid backups and even let the vehicle drive semi-autonomously for stretches of roads.

As the demands on E/E architectures have grown, there's been a shift from a decentralized or distributive network of individual microprocessors for each individual sensor or control — and then adding new systems for each additional sensor or control — to a more centralized system allowing for a more efficient use of resources and computing power. Deploying zonal architectures addresses the increasing complexity and computational demands of E/E systems, enabling car manufacturers to meet the demands of software-defined vehicles.

The key to the success of zonal architectures is the development of hardware and software that can meet the demands put upon the new centralized network. New technologies using zonal architectures include advanced driver assistance systems, semi-autonomous driving, and infotainment systems.

The latest generation of sensors and system-on-chips (SoCs) are allowing for even more integration. It's this level of incorporation accelerating the improvement of fully autonomous driving systems and other AI-related functions.

Tesla's hard push into those areas has forced other automakers and suppliers to work hard to ensure they're ready to compete with the new generation of software-defined vehicles. Synopsys is working with auto suppliers to ensure they are hitting the target when it comes to these systems.

Synopsys expertise includes E/E architectural consulting and modeling and automotive-grade IP. The company also offers comprehensive design and verification services, EDA suite with automotive flows, emulation, and prototyping. Synopsys assists automotive software developers in complying with global safety standards and to build security and quality into all stages of their lifecycle, helping to initiate development months sooner.

&

There's no question the vehicle of the future is going to be more complex, require more computing power and essentially be cutting-edge technology on four wheels. However, the unknown is how this

will unfold. Will automakers take the lead? Will suppliers provide the know-how to handle the car of tomorrow?

Many thought automakers would begin to move development of complex, software-defined vehicles in-house as, ultimately, they'll be held accountable for it. Additionally, they've been developing many of their own technologies for years now, ranging from GM's OnStar to Ford's BlueCruise and Tesla's Full Self-Driving.

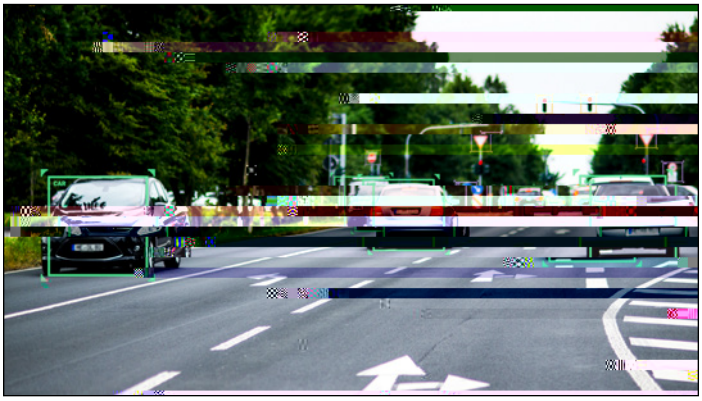
However, suppliers are often the catalyst that ensure the new technologies take off. Perhaps nowhere is that more evident in the moves by Apple, which is upgrading its CarPlay technology to provide more services and a better experience for users. The updated version of CarPlay reportedly will offer directions that are more easily understood by users, as well as new features. One example is direct access to downloaded podcasts from the cloud rather than forcing users to have the podcasts downloaded prior to coming into the vehicle.

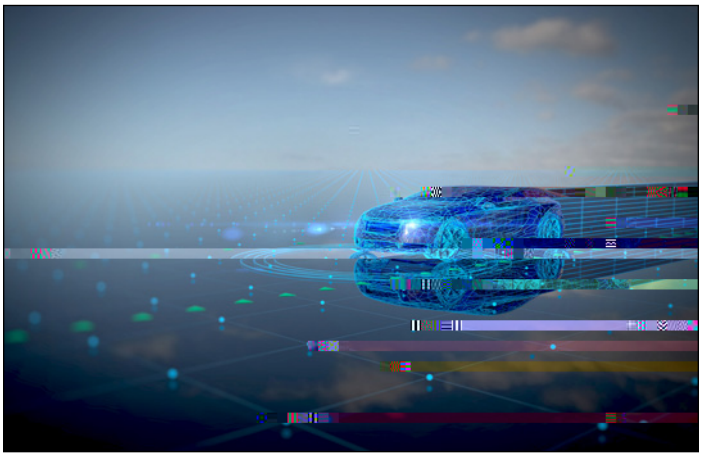
The push to produce connected cars is accelerating and seemingly all the players are being invited to sit at the table and may the best technology win. As is often the case, Synopsys is already involved.

&

Milliseconds count — and improving the speed and efficiency of semiconductor chips responsible for brake lights, automatic door locks and engine controls is basic, but crucial, to safety improvements. Synopsys helps designers virtualize the process, shifting software development from on-road prototypes, test rigs and hardware-in-the-loop to the computer of the function developer. This focus speeds up and ensures the accuracy of testing and validation — and lowers cost all in the same instant.

Today's cars, trucks and crossovers have become computers on wheels. It's not unusual to find more than 100 separate microprocessors onboard the latest luxury vehicles, and even entry-level models are loaded up with digital displays, smart





safety systems and other digital features. But while research shows consumers continue to demand ever more onboard technologies, the trend poses some distinct challenges — notably cybersecurity.

Researchers have already shown it's possible to take control of high-tech vehicles, such as the Tesla Model Y or even as long ago as 2015, a Jeep Cherokee. So, far, such attacks have been limited to the lab, but experts warn it's only a matter of time before cyberattacks occur in the real world — especially as more and more manufacturers add over-the-air update capabilities to their vehicles. This technology allows a manufacturer to download software updates — but also provides a potential vector for the bad guys.

Experts warn of a variety of threats hackers could pose. As with home computers, some will be seeking personal information, such as credit card or social security numbers, that can be used to steal your identity. An even bigger concern is what hackers might be able to do as autonomous vehicle technology begins coming to market. Tesla, General Motors with Super Cruise, Ford with BlueCruise and Mercedes-Benz are among the growing list of manufacturers offering partially automated or even what is claimed to be fully automated vehicle technologies for retail buyers. Advanced robocabs and driverless trucks are now being tested on public highways.

The potential benefits are substantial — among them safer highways and reduced shipping costs, according to proponents. But the risks could be equally significant. That was underscored when a half-dozen Cruise robocabs suddenly ceased operation at a busy intersection in San Francisco, causing an hours-long traffic tie-up. Experts worry that hackers could cause crashes, even hijack vehicles.

That's driving the industry to take aggressive steps to lock out hackers. New standards, such as ISO/SAE 21434, are meant to address automotive cybersecurity.

It's one thing to lay out new standards, but it's another to implement them. Effective solutions need to be holistic, touching every possible vector where hackers could gain access to a vehicle, corrupt software, even take remote control of a vehicle, stresses Synopsys expert Dr. Dennis Kengo Oka. He is part of a team that can help automakers and suppliers address mobile cybersecurity, from the chip level up through the implementation of safe and secure over-the-air technology.

A

One of the biggest challenges for an automotive manufacturer is bringing a new concept to its customers. In a fast-changing world,