S&P Global
Mobility

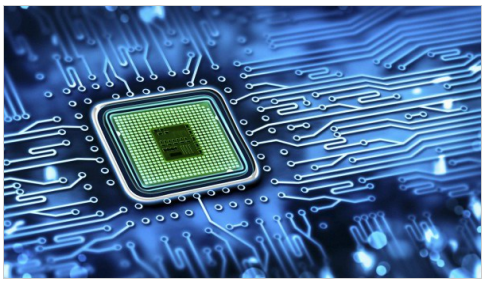
AutoTechInsight Insights
E/E and Semiconductor
June 2026

The blind spots in the chip supply chain: Q&A with Loftware

24-Jun-2026 12:13 GMT

Matthew Beecham
S&P Global
Supply Chain and Technology, Automotive

How automakers have improved chip supply resilience, but poor supply-chain visibility remains a major risk.



Source: Getty Images/crstrbrt

The automotive industry has spent the years since the semiconductor shortage pursuing a familiar set of remedies: expanding fabrication capacity, diversifying sourcing, reshoring production and securing long-term supply agreements. Governments have poured subsidies into domestic chip manufacturing; automakers have forged closer relationships with semiconductor producers; suppliers have invested heavily in resilience planning. Yet, amid the race to secure more capacity, a subtler vulnerability persists. Carmakers still struggle to see deeply enough into the sprawling supplier ecosystems on which modern vehicle production depends.

That visibility gap sits at the heart of this discussion with Tim Vessel, Senior Account Executive at Loftware. While much of the industry's attention remains fixed on advanced chips and AI-driven demand, the more immediate operational risk for many manufacturers may lie further down the supply chain: among mature-node semiconductors, packaging operations, materials suppliers and logistics networks that remain difficult to monitor in real time. Automotive supply chains are deeply interconnected, but the data systems supporting them are often anything but. Information remains fragmented across suppliers, regions and incompatible platforms, leaving manufacturers with only partial visibility into key dependencies and emerging points of failure.

Tim Vessel

[Source: Loftware]

The following is an edited transcript of the conversation.

S&P Global Mobility: AI infrastructure demand is absorbing semiconductor capacity and investment attention. Where do you see the most acute collision points between AI-driven chip demand and automotive semiconductor requirements?

Tim Vessel: What we are hearing from our customers, many of whom are global manufacturers that depend on semiconductor availability to keep production moving, is growing concern about understanding where potential bottlenecks may emerge as AI-driven demand reshapes parts of the semiconductor ecosystem. Vehicles still depend heavily on mature-node semiconductors for power management, sensors, microcontrollers, advanced driver assistance system, battery systems and safety functions. Those components may not always receive the same level of investment as advanced-node chips used in AI infrastructure, but they remain critical to keeping automotive production moving.

While AI investment is driving expansion in advanced-node production, it can also influence how resources, supplier attention and production priorities are allocated throughout the supply chain.

For automotive manufacturers, the issue is less about predicting the exact point of constraint and more about ensuring enough visibility across supplier networks to identify and respond to risks before they impact production.

The collision point is visibility and response time. Automakers need to understand not only which suppliers provide critical components, but also where those components originate, how they move through the network and which upstream dependencies could create production risk. When that information sits across disconnected supplier systems, companies end up reacting after a constraint has already affected the line.

The stronger position is readiness. That means having connected supplier networks, consistent product identification and traceability data that help manufacturers spot emerging risks earlier and respond before disruption becomes a production issue.

Much of the industry discussion focuses on advanced-node chips, but vehicles still depend heavily on mature-node semiconductors. What makes mature-node supply particularly difficult to monitor and protect from a traceability perspective?

Mature-node semiconductors often move through complex supplier networks involving multiple manufacturing sites, testing facilities, packaging operations, distributors and logistics partners. The challenge is that visibility often fades as you move beyond direct supplier relationships.

We are not semiconductor manufacturing experts, but we do work with global manufacturers seeking to improve how they manage product identity, supplier data and traceability across complex networks. What we see is that risk often exists several layers below where most companies are looking.

For automakers, that creates a practical problem. A component may be low-cost relative to the vehicle, but if it supports a safety system, power function or electronic control unit (ECU), the operational impact of disruption can be significant. Traceability helps connect the component, supplier, location and movement data needed to understand where risk sits.

This is where product identification becomes more strategic. It provides manufacturers with a common way to connect parts, packaging, supplier activities and operational data across multiple organizations. Without that consistency, mature-node supply becomes difficult to monitor because the data is fragmented before it reaches the original equipment manufacturer.

During the last semiconductor shortage, where did visibility break down most severely — between OEMs and tier 1 suppliers, between tier 1 suppliers and semiconductor suppliers or deeper in tier 2, tier 3 and materials networks?

Based on customer conversations, the largest visibility gaps often existed beyond direct supplier relationships.

Many OEMs had relatively strong communication with tier 1 suppliers. The harder question was what sat behind those suppliers: shared component sources, manufacturing locations, packaging operations, material dependencies, and logistics constraints that could affect multiple programs at once.

That is where automotive supply chains are most exposed. The industry is structured as a network, but too many processes still operate through one-to-one handoffs. When a disruption hits several layers upstream, companies may not have enough connected data to understand which plants,

programs or vehicle lines could be affected.

The lesson is that visibility cannot stop at the first tier. OEMs do not need access to every commercial detail in the network, but they do need a trusted way to capture and share the risk signals that matter. That includes manufacturing location, product identity, country of origin, lead-time changes, supplier status and disruption alerts tied to critical components.

If an automaker wants visibility beyond tier 1 suppliers, what data should it actually require?

The data requirements will vary by organization and risk profile, but the starting point should be information that helps the automaker understand the origin, movement, dependency and impact.

That can include manufacturing location, country of origin, component identifiers, lot or batch information where relevant, packaging and shipment data, supplier status, lead-time changes, quality events and other traceability data tied to production risk.

The important point is that visibility has to be usable. Asking suppliers for broad disclosure can create resistance and slow adoption. Asking for specific, standardized data points tied to operational risk is more realistic.

This is where common product identification standards and connected supplier processes matter. They allow OEMs and suppliers to share the right information in a consistent format, without forcing every supplier to expose commercially sensitive details. The goal is not to know everything about every supplier. The goal is to know enough to make faster, better decisions when conditions change.

How should OEMs balance deeper supplier transparency with the commercial reality that many tier 2 and tier 3 suppliers may be reluctant to disclose sensitive sourcing, capacity or customer-allocation information?

OEMs should think in terms of collaboration, not full disclosure. In our experience, most suppliers are not unwilling to share information. They are cautious about sharing information that could expose customer allocations, proprietary sourcing strategies or commercial relationships. That is understandable.

The practical answer is to define which information is necessary for risk management and which is not. An OEM may not need to know a supplier's full customer allocation or contract terms. It may need to know whether a critical component is tied to a specific manufacturing region, whether lead times are changing, or whether a supplier event could affect production.

Successful networks establish trusted mechanisms for quickly sharing relevant information. That means common standards for product identification, clear governance for access and workflows that allow suppliers to provide risk signals without giving up sensitive commercial control. Resilience comes from building trust into the way data is shared.

What role can labeling, product identification and packaging intelligence play in semiconductor risk management that traditional Enterprise Resource Planning (ERP), Electronic Data Interchange (EDI) or supplier portals cannot?

ERP, EDI, and supplier portals are important systems. They are very effective at managing transactions, orders, shipments and supplier communications.

The gap is that these systems do not always connect product identity across multiple suppliers, sites, regions and business systems. In a complex automotive supply chain, that matters. A semiconductor component may move through several points before reaching final assembly. At each handoff, the manufacturer needs accurate information about what the component is, where it came from, how it was handled, and whether it meets the right requirements.

Product identification, labeling and packaging intelligence provide a common execution layer. They help connect physical products to digital information across the supplier network. That is especially important when sourcing changes, trade requirements shift, or a quality issue requires fast analysis.

The goal is not tracking for its own sake. It is giving manufacturers access to accurate product and supplier information quickly enough to act. That is where product identification becomes part of semiconductor risk management, not just a downstream operational task.

What early-warning indicators should automotive manufacturers monitor to detect semiconductor disruption before it becomes a line-stoppage event?

The specific indicators will vary, but many manufacturers are paying closer attention to lead-time changes, supplier communications, delivery performance, quality events, disruption notices and activity in key manufacturing or logistics regions.

The stronger approach is to connect those signals to product and supplier data. A lead-time change is useful, but it becomes much more actionable when the manufacturer can quickly identify which components, plants, production programs and vehicles may be affected.

This is where connected supplier networks can help. If product identification, packaging data, shipment status and supplier updates are aligned, manufacturers can detect exceptions earlier and understand the operational impact faster.

The warning signs are often there before the line stops. The problem is that they are frequently scattered across emails, portals, spreadsheets, ERP systems and supplier updates. The companies that respond best are the ones that can bring those signals together and turn them into coordinated action.

As vehicles become more software-defined and electronics-intensive, how does the traceability challenge change?

Traceability becomes much more important as vehicles become more electronics-intensive. Modern vehicles include thousands of electronic components supporting safety systems, connectivity, battery management, infotainment, ADAS and other software-driven functions. When a quality issue, recall or supply disruption occurs, manufacturers need to understand exactly which components were used, where they originated, and which vehicles may be affected.

That is difficult if component data, supplier information and product identification records are disconnected. A software-defined vehicle still depends on a physical supply chain. Every sensor, module, chip, connector and packaging unit has to be accurately identified and connected to the right production and vehicle data.

As vehicle complexity increases, traceability becomes a control point for operational efficiency, customer safety and recall readiness. The more electronic content in the vehicle, the more important it becomes to maintain accurate and connected product data across the full lifecycle.

Where does AI help most in improving automotive semiconductor supply visibility?

AI's greatest value is not necessarily predicting the next disruption. It is helping manufacturers make sense of large volumes of supply chain data that are too complex to analyze manually.

The most useful applications include identifying anomalies across supplier networks, detecting risk signals earlier, normalizing data from different trading partners and helping teams prioritize the exceptions that require action.

However, AI is only as useful as the data foundation behind it. If product identification is inconsistent, supplier data is incomplete, or traceability records are fragmented, AI will amplify confusion rather than solve it.

The manufacturers that will get the most value from AI are the ones that first strengthen data quality, supplier connectivity, and traceability. AI can help teams move faster, but it needs reliable product and supplier information to work from. In automotive, intelligence has to be built on connected execution.

If you were advising an automaker on a 12- to 24-month roadmap for semiconductor supply resilience, what are the first three capabilities it should build?

The first priority is improving visibility across the supplier ecosystem. Automakers need a clearer view of where critical components originate, how they move and which dependencies could affect production.

The second is strengthening traceability. That means connecting product identity, supplier data, packaging information, shipment activity and manufacturing records in a way that supports faster decisions during disruption or quality events.

The third is building more collaborative information-sharing processes across suppliers and trading partners. OEMs should focus on trusted, standardized mechanisms for sharing the data that matters, without requiring suppliers to disclose unnecessary commercial information.

Success should be measured by how quickly a company can identify a disruption, understand its impact and act across the network. The most resilient automotive companies over the next decade will not necessarily be those with the largest inventories, but those with the most connected, visible and collaborative supplier networks.

CONTACTS

The Americas
+1 877 863 1306

Europe, Middle East & Africa
+44 20 7176 1234

Asia-Pacific
+852 2533 3565

www.spglobal.com/mobility