The Importance of Secure Data Sharing

By: Mike McIntyre,
Onto Innovation

Content as published on
Semiconductor Engineering blog post, May 2024.

When it comes to data accessibility, the terms "secure" and "share" seem like two diametrically opposed words. Conventional wisdom would suggest that any effort to secure data would involve limiting access to that data, while sharing data would involve opening up access to that data for others to view and use.

As it turns out, semiconductor operations need to do both.

On the one hand, semiconductor companies often need to share data so others can leverage data for problem solving and improve their overall manufacturing processes. On the other, these companies need to know their data is secure and free from data leaks resulting in lost IP or negating a competitive advantage. The solution: secured data sharing.

Secured data sharing

Why do semiconductor companies need secured data sharing? It's best to answer this question by thinking back to when factories were building parts for their own use.

Previously, these facilities — what we refer to as original equipment manufacturers (OEMs) — had access to the complete manufacturing history of a device, as well as the electrical test and quality results from their customers. When issues arose, the OEM had the ability to dredge up all the process and operational histories for the questionable devices, draw correlations to potential issues and, ultimately, implement operational fixes to resolve problems and eliminate recurrences. Additionally, these OEMs were able to leverage the differences, in designs and process flows, between multiple devices as of part of their problem-solving tool kit. During this era, the biggest challenge for an OEM was a lack of access to a consolidated data repository.

Today, we have a considerably better understanding of the importance of effectively accessing data and how to do it. Unfortunately, with the proliferation of fabless design houses, foundry manufacturing and outsourced assembly and test (OSAT) facilities, the supply chain of data has become fractured and isolated (Figure 1). In other words, data is generally not shared. In this situation, device providers and design houses are at a distinct disadvantage compared to OEMs.

The Importance of Secure Data Sharing

By: Mike McIntyre,
Onto Innovation

Content as published on
Semiconductor Engineering blog post, May 2024.

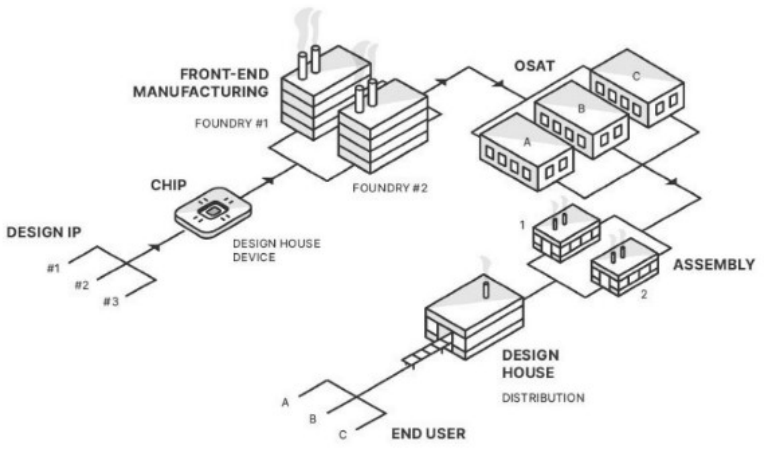

Figure 1: With three different designs, two foundries, three OSATs, two assembly houses, a separate design house and three end users, sharing data securely is challenging.

Design houses are held accountable for the quality of a shipped device, and yet they do not have the ability to match inline metrology and inline process characteristics to the electrical test results needed to solve product quality questions. They also do not have the capability to look at electrical test results across multiple components and understand how these results impact the full-blown system they are selling to end customers. Each of these data sources are isolated and inaccessible to the individuals who need access to this data to solve their everyday problems and improve the overall position of their products in the marketplace.

At Onto Innovation, we've addressed this conundrum by restricting sensitive data to authorized users, while opening up areas of data to broader user groups, including, ultimately, users who are outside of a factory's wall. Fundamentally, this allows IT managers to identify users who need to view and work with sensitive data as part of their normal duties. Because of the breadth of sensitive data — including information about yields, electrical performance, financial data or factory planning — information system administrators can customize who sees what, down to the specific user. Leveraging this capability, several Onto customers have extended this functionality to their downstream customers, giving device makers the ability to look into the factory and extract information normally unavailable to them. The end result is the ability to produce better products.

Having access to previously unavailable upstream manufacturing histories allows device designers to gain a greater understanding of why

their products are performing the way they are. Additionally, if quality concerns are drivers for the parts being manufactured, the additional insights a factory provides can now be passed on to device makers. These insights can include regional information regarding existing defects, inline metrology patterns as they appear across wafers, and specific correlations between wafer acceptance tests and device electrical performances in a package.

Over the last couple of years, manufacturing fab customers have adapted this functionality by providing their customers with access to normally restricted data. This access has been beneficial for manufacturing customers and design houses. More specifically, this functionality has taken what might be an adversarial relationship between the wafer manufacturer and the device maker as to who owns specific problems and has turned this conflict into an opportunity between the two to develop a cooperative solution where both parties work with the same data and come to the same conclusion as to the source of the problem and what corrections are needed to improve the device.

Conclusion

With secure data sharing, device makers can access manufacturing details and fundamentally recover some of the advantages that were lost when they shifted away from an OEM business model. Device makers also can retain manufacturing history, along with detailed quality test and returns history, to create a greater ability to isolate issues, if and when, they occur, and foundries have the ability to provide a service to their customers. Together, they are able to move forward as partners and create a more transparent working relationship.

The Importance of Secure Data Sharing

By: Mike McIntyre,
Onto Innovation

Content as published on
Semiconductor Engineering blog post, May 2024.

About the author
Mike McIntyre is director of product management for enterprise software at Onto Innovation.