The Importance of Zero Trust in Microelectronics

Dr. Lisa J. Porter
LogiQ, Inc. Arlington, VA Lisa.Porter@LogiQ-inc.com (703)627-5671

Keywords: Zero-Trust, supply chain, security, resiliency

Recently, supply chain fragility as well as massive cybersecurity breaches have raised legitimate concerns about the need to rethink the entire global microelectronics value chain. However, there has been significant confusion regarding how to address the challenge, and unfortunately the recent availability of large government subsidies has incentivized the promotion of inferior solutions.

Resiliency must be the focus, not perfectly secure systems. While the concepts are often conflated, they are in fact distinct. The latter goal is not only impossible, but also leads to deeply flawed solutions, where the pursuit of trust (e.g., trusted suppliers, trusted networks) becomes the proxy for the development of secure systems. For example, the US DoD's focus on "secure and trusted" microelectronics has resulted in a reliance on trusted foundries, which ironically has degraded its security posture, not only because of the inherent flaw in perimeter defense approaches upon which trusted foundries rely, but also because they have forced the DoD to rely on older technology, making the DoD less competitive on the global stage, and more vulnerable to counterfeit products.

By contrast, resiliency is defined by the International Council on Systems Engineering (INCOSE) as "the ability to provide required capability in the face of adversity" [1]. The pursuit of resiliency in complex systems acknowledges the reality that failures (whether of malicious origin or not) will happen, and that the goal should be to minimize their impact on operations.

Today's globally distributed and intertwined microelectronics value chain has evolved to be optimized for efficiency and innovation, not resiliency, and current events have highlighted the need to address this shortcoming. The Zero-Trust (ZT) philosophy enables the design and implementation of resilient systems without incurring the negative consequences of pursuing "secure and trusted" systems. It assumes that any complex system (e.g., a network, a foundry, a supply chain) either has been or will be compromised, and that the pursuit of trust in any part of the system introduces a vulnerability that can be exploited. Therefore, it eliminates trust as a goal and instead focuses on data-driven quantitative risk assessment and management, where risks can include not only those related to adversarial attacks (e.g., cyber-attacks, malicious insertion, theft of IP), but also those associated with unintended human errors, natural disasters, and geopolitical dynamics (e.g., trade policies, pandemics). Such risk assessment should be conducted on a continual basis, enabling dynamic decision-making that adapts to updated information and enables the continual mitigation of the assessed risk. The amount of mitigation can be tailored so that the estimated residual risk meets the risk tolerance (and associated cost tolerance) of the customer/application. *It is important to emphasize that a ZT approach does not imply the elimination of risk – it is about risk management, not risk avoidance.* The latter is not possible, and the pursuit of "perfectly secure", "trusted", or "zero-risk" systems is antithetical to what ZT is all about.

Effectively implementing ZT in microelectronics will ideally entail instrumenting the entire lifecycle – from specification to design to fabrication to packaging and test to integration into subsystems and systems to fielding/operations – providing fine-grained measurements that enable continual risk assessment and subsequent mitigation should that risk exceed a pre-determined threshold. More specifically, quantitative assessments would be calculated at multiple stages along the lifecycle, with each assessment taking into account the particular risks (malicious and benign) associated with that stage.

The practical implementation of such an approach cannot introduce significant throughput impact or prohibitive cost penalties. Fortunately, modern foundries are highly automated and collect large amounts of process data, test data, access data, etc., with a focus on improving quality, yield, and reliability. And a significant amount of data is collected at package assembly facilities for quality assessment as well. Thus, an obvious first step would be to begin with the data that is already collected and determine whether and how it can be used to provide additional

information that can reduce risk. It is possible, even likely, that experts could develop multiple analytic functions that would translate this data into quantitative estimates of risk; such development should be collaborative and transparent across the industry. Keeping such algorithms proprietary will not provide a competitive advantage, as everyone in the ecosystem will want to know what is being calculated as the underpinning of a risk assessment.

It is reasonable as a next step to determine whether (and what) additional measurements could further reduce risk. Presumably, such additional measurements will introduce additional cost, so a tiered level of residual risk (or equivalently, a tiered level of assurance), will enable cost-risk trades. For example, the use of additional measurements that enable authentication and provenance within a certain probability might result in a "Tier 2" assurance level, while measurements that also enable inference of the probability of malign insertion remaining below a threshold might result in a "Tier 3" assurance level. The analytics that calculate assurance levels at each step of the lifecycle may be a function of data collected at that step as well as of the results from prior steps. As noted above, the development of the algorithms that would translate the data into levels of assurance, as well as the definitions of those levels, will need to be developed collaboratively across the industry.

There are clearly some challenges to implementing this approach, but they are not insurmountable. For example, every step along the lifecycle involves multiple vendors/suppliers, none of whom are likely to be willing to share data with each other. Modern data collection systems used for product quality/yield monitoring already encrypt data to protect it from IP theft [2]. It should be possible to apply encryption techniques to risk calculations as well, even if these calculations must include data from multiple vendors. In recent years, the field of secure computation has significantly improved the performance (reduced computational expense) of many multi-party encryption protocols (e.g., electronic voting, private information retrieval, etc.), and this expertise can be applied to this problem. [See Figure 1.] So, while what is measured and how probabilities of various risks are calculated based on those measurements should be openly defined and agreed upon, the measurements themselves can remain encrypted.

A second challenge will be to ensure that the industry can quickly share lessons learned so that risk assessment can be continually improved across the lifecycle. Risk matrices will be calculated based on known risks; as new risks materialize, they will need to be quickly added, and the appropriate

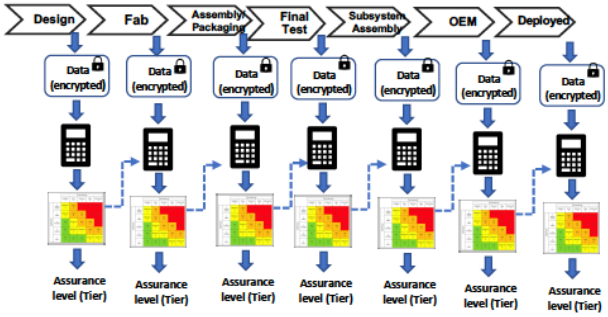

Fig.1: Implementing Quantitative Risk Assessment along the entire lifecycle

measurements will need to be identified to mitigate them. The need for an open and transparent approach to enabling a dynamic risk assessment capability at each stage of the lifecycle cannot be overstated. While this will be challenging for such a diverse community of vendors and customers, the microelectronics industry already participates in several successful standards bodies (e.g., IPC, IEC, JEDEC, IDEA, IEEE, SAE, SEMI) to accomplish similar objectives. Furthermore, maintaining open standards will help to foster innovation in the development of measurement tools and techniques – such a result has been observed in other open-standards activities (e.g., the explosion of new companies and technologies supporting the Open RAN architecture being driven by the O-RAN alliance [3]).

Finally, the economic hurdles of implementing a multi-tiered quantitative risk assurance approach across the lifecycle must be acknowledged, particularly for those vendors with low margin businesses. Fortunately, the return on investment from making measurements that will lay the foundation for implementing ZT should be demonstrable through the positive impact that such measurements will also have on quality, yield, and reliability. For example, the demand for quality and reliability improvement will continue to escalate from the automotive industry. Modern cars contain around 8000 chips [4], a number that will only increase, particularly as autonomous driving gains popularity. This means that acceptable failure rates will become increasingly challenging to meet, which should drive demand for more measurements particularly to the "left" of the lifecycle (e.g., in the fab).

Furthermore, there are lessons to be drawn upon from the cybersecurity arena. For many years, information security officers had the near-impossible task of convincing their C-suite colleagues to meaningfully invest in cybersecurity – the benefits were very difficult to quantify in terms of the bottom-line, especially because traditional cybersecurity methods relied heavily upon perimeter defense strategies that were not very effective. However, as data breaches and ransomware attacks have become more prevalent and costly (e.g., the 2020 SolarWinds attack and the 2021 Colonial Pipeline ransomware attack), the demand for a cybersecurity methodology that enables resiliency against such threats has resulted in a pivot away from perimeter defense and toward ZT. In 2020, the NSA issued a public endorsement of a ZT security model [5] and NIST published a conceptual framework for implementing a Zero-Trust architecture (ZTA) for enterprise networks [6]. And on 26 January 2022, the White House issued a memorandum that sets forth a ZTA strategy for all federal departments and agencies, stating, "In the current threat environment, the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data." [7].

It is not difficult to imagine a devastating ransomware-like attack on an OEM based on an exploitation of the microelectronics lifecycle. Hence, there should be growing interest and support from OEMs to invest in a complete ZT approach such as the one outlined above.

Such attacks are also of great concern to the national security community and have been a key driver of the flawed focus on "trusted foundries". Rather than continuing to pursue a strategy in microelectronics manufacturing that it has recognized is fundamentally flawed for cybersecurity, the USG, especially the DoD, should take a leadership role in accelerating the adoption of the ZT approach across the microelectronics lifecycle. Specifically, the DoD should work closely with the commercial sector, particularly the OEMs, to define quantifiable assurance standards for commercial microelectronics. This will enable the national security community to confidently access state-of-the-art commercial microelectronics that are critical for next-generation systems – access that "trusted foundries" simply cannot provide. In recent years, the DoD has begun to transition toward a ZT approach, publicly advocating for the development of quantitative assurance standards in design [8], fabrication [9], and advanced packaging [10]. However, these initiatives have also placed an emphasis on "onshoring" these capabilities. While onshoring advanced fabrication and packaging manufacturing should bolster the US microelectronics industrial base, this goal should not be conflated with that of developing a resilient supply chain through ZT. Onshoring is no different than a perimeter defense approach unless it is accompanied by the development and use of quantitative assurance standards. But more importantly, onshoring the entire global semiconductor manufacturing lifecycle, for all types of semiconductors, is simply infeasible. Thus, the DoD must not limit its development of assurance standards solely to onshore facilities – such standards should be defined and implemented throughout the global ecosystem. Only by applying a ZT methodology to the entire ecosystem will we be able to elevate the resilience of microelectronics for all customers, to include the DoD.

REFERENCES

[1]https://www.incose.org/incose-member-resources/working-groups/analytic/resilient-systems

[2] See, for example, the Optimal+ solution by NI, https://www.ni.com/content/dam/web/pdfs/oplus_data_encryption_solution.pdf

[3] https://www.o-ran.org/

[4] https://electroiq.com/files/2018/01/process-watch-the-automotive-problem-with-semiconductors/

[5]https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/

[6]https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[7] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[8] https://nstxl.org/opportunity/ramp-phase-ii/; https://www.eetimes.com/dod-ramps-secure-chip-design-effort/#

[9] https://nstxl.org/dod-and-s2marts-impacting-the-microelectronics-ecosystem-through-the-rapid-assured-microelectronics-prototypes-commercial-ramp-c-project/

[10] https://nstxl.org/opportunity/state-of-the-art-heterogeneous-integrated-packaging-ship-prototype-project/;https://www.defense.gov/News/Releases/Release/A

rticle/2384039/department-of-defense-announces-1972-million-for-microelectronics/

ACRONYMS

DoD: Department of Defense
IDEA: Independent Distributors of Electronics Association
IEC: International Electrotechnical Commission
IEEE: Institute of Electrical and Electronics Engineers
INCOSE: International Council on Systems Engineering
NIST: National Institute of Standards and Technology
NSA: National Security Agency
OEM: Original Equipment Manufacturer
RAN: Radio Access Network
USG: United States Government
ZT: Zero-Trust
ZTA: Zero-Trust Architecture