OmniTrust

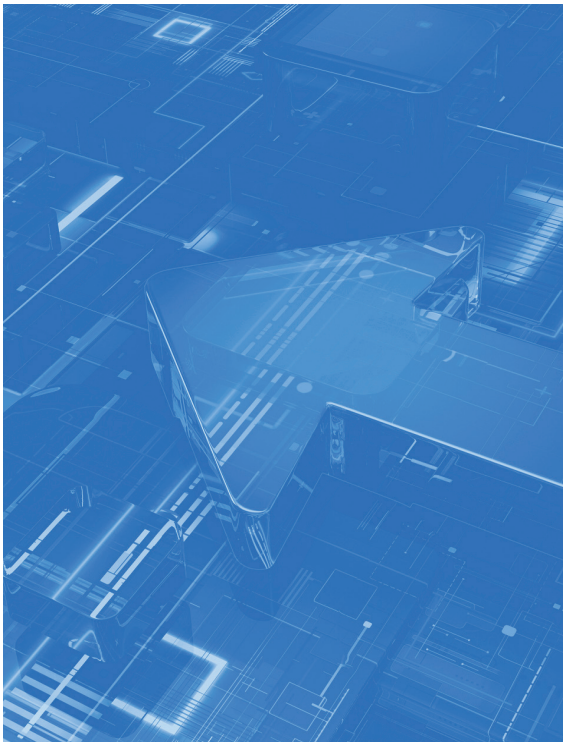
SYNOPSYS®

Infineon

WHITE PAPER

Shift-Left Trust

Extending Virtual Development to Embedded Trust Validation



The Gap

Virtual platforms changed the way embedded software is developed. Architecture exploration, middleware integration, regression testing, and CI/CD workflows increasingly begin before hardware exists. Virtual ECUs and electronics digital twins have moved functional validation into virtual environments where software can be integrated, exercised, and debugged before the first prototypes arrive.

Shift-Left Trust extends virtual development by integrating embedded trust validation into the same workflow used for software development and functional validation.

Functional validation has broadly moved into virtual development, with trust validation now making the same transition, albeit unevenly. In many programs, secure boot, firmware integrity, root-of-trust enforcement, HSM configuration, SHE interfaces, protected memory, and provisioning flows still reach full validation late in the development cycle. Embedded trust often reaches full maturity during hardware integration. Modern embedded systems depend on trusted software as much as functional software, yet only one is routinely validated before hardware exists. The consequences include limited visibility, late defect discovery, and security integration becoming part of the critical path.

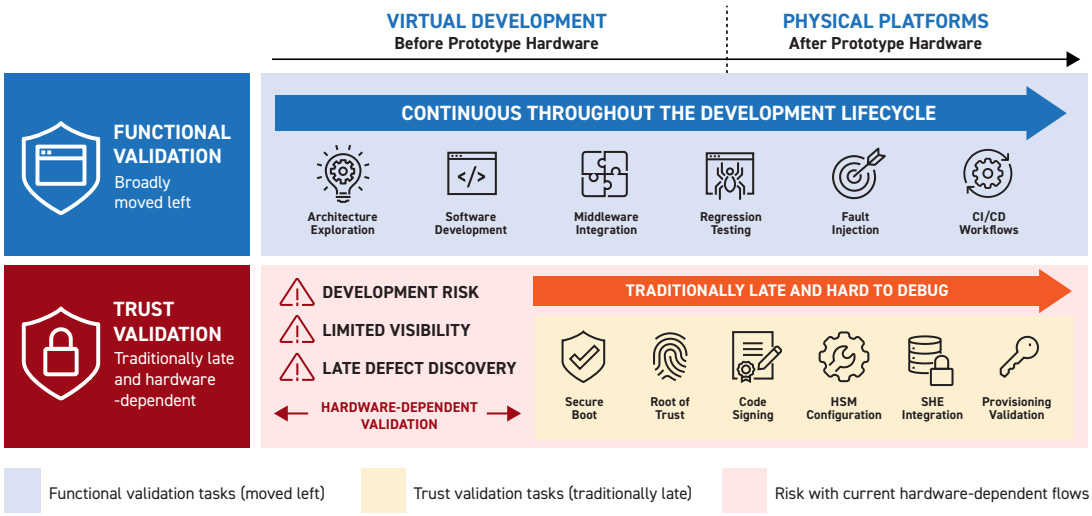


Figure 1: The Trust Validation Gap
Functional validation has moved left. Trust validation remains late.

The issue is not cryptography. The challenge is that the most security-critical functions depend on hardware-backed services that are difficult to observe during bring-up. HSMs, SHE interfaces, cryptographic accelerators, protected memory regions, and provisioning mechanisms are designed to protect system integrity. During integration, they often become the most challenging aspects of system integration.

Virtual Platforms Changed the Schedule

Virtual development has changed how embedded systems are engineered. Rather than waiting for hardware, software teams now execute production binaries inside virtual platforms that accurately model target devices and system behavior. Functional validation begins earlier, integration becomes continuous, and development is no longer paced by prototype availability. This model is becoming standard practice across semiconductor suppliers, automotive

OEMs, and Tier 1 suppliers because it improves software readiness independent of physical hardware. The next step is to make embedded trust validation part of the same virtual workflow, rather than a separate activity that reaches maturity during hardware bring-up.

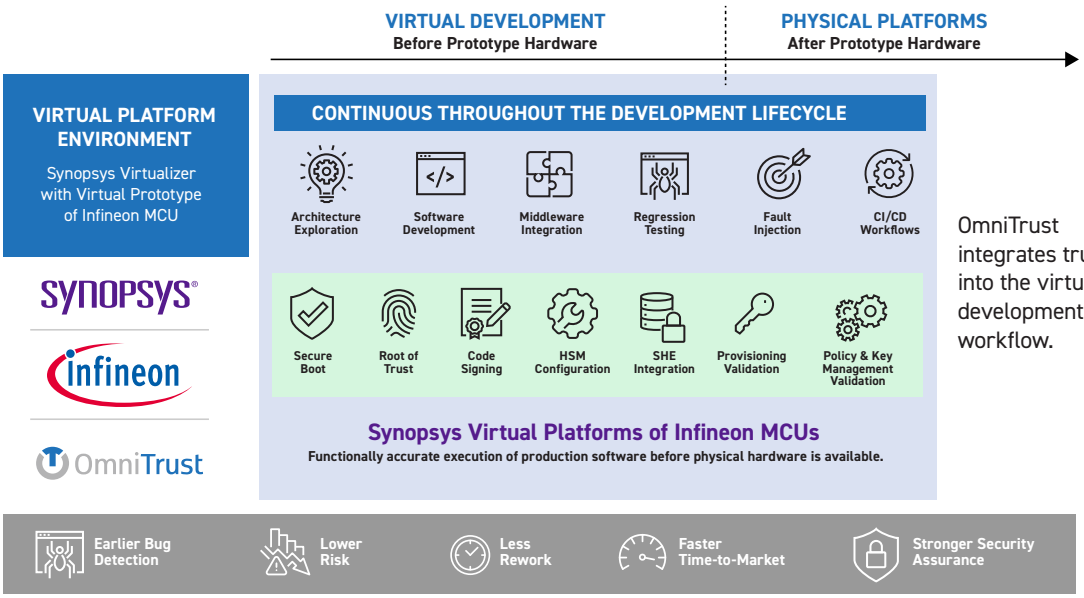


Figure 2: Shift-Left Trust: Closing the Gap
Bring trust validation left. Validate trust early, continuously and with full visibility.

Figure 2 shows how extends virtual development workflows into embedded trust validation. Through the collaboration between Synopsys, Infineon and OmniTrust, Synopsys Virtualizer™ provides virtual platforms of the Infineon MCUs for AURIX™ TC3x and TC4x, Traveo and RISC-V. This enables the eco-system as well as Tier1 and OEM customers with a development environment allowing functionally accurate execution of production software before physical hardware is available. OmniTrust extends the environment with embedded trust validation, allowing secure boot, firmware integrity, root-of-trust enforcement, HSM and SHE services, protected memory, and controlled provisioning flows to be exercised alongside the software they protect. Together, these solutions allow software, functional, and trust validation to progress on a shared virtual development schedule.

Shift-Left Trust extends existing virtual development workflows rather than introducing new ones.

What Becomes Testable

Moving trust validation into the virtual environment changes what becomes observable. Firmware signatures can be verified before deployment. Boot policy decisions can be inspected as they occur. Root-of-trust behavior can be traced through execution rather than inferred from failure. HSM services, cryptographic accelerators, protected memory access, and provisioning sequences can be exercised repeatedly using unmodified production binaries under deterministic conditions. Hardware-backed security functions intentionally limit access and visibility in production systems. Virtual development allows teams to inspect integration behavior without weakening the production security model. Failures that once appeared only during prototype bring-up become reproducible software events. They can be debugged, regression-tested, and resolved before physical hardware becomes the limiting resource.

Why It Matters

Shift-Left Trust extends existing virtual development workflows rather than introducing new ones. Software development, functional validation, and trust validation progress within the same virtual environment and on the same development schedule. Engineering effort shifts from hardware integration to software verification. Security validation no longer competes with prototype availability.

Conclusion

Virtual platforms have changed how embedded software is developed. Synopsys Virtualizer and the virtual platforms for Infineon MCU enable electronics digital twins that allow production software to be developed, integrated, debugged, and validated before physical hardware is available. Shift-Left Trust from OmniTrust brings that same workflow to embedded security and trust validation. The virtual platform is becoming the place where software and trust are engineered together.

OmniTrust SYNOPSYS® Infineon