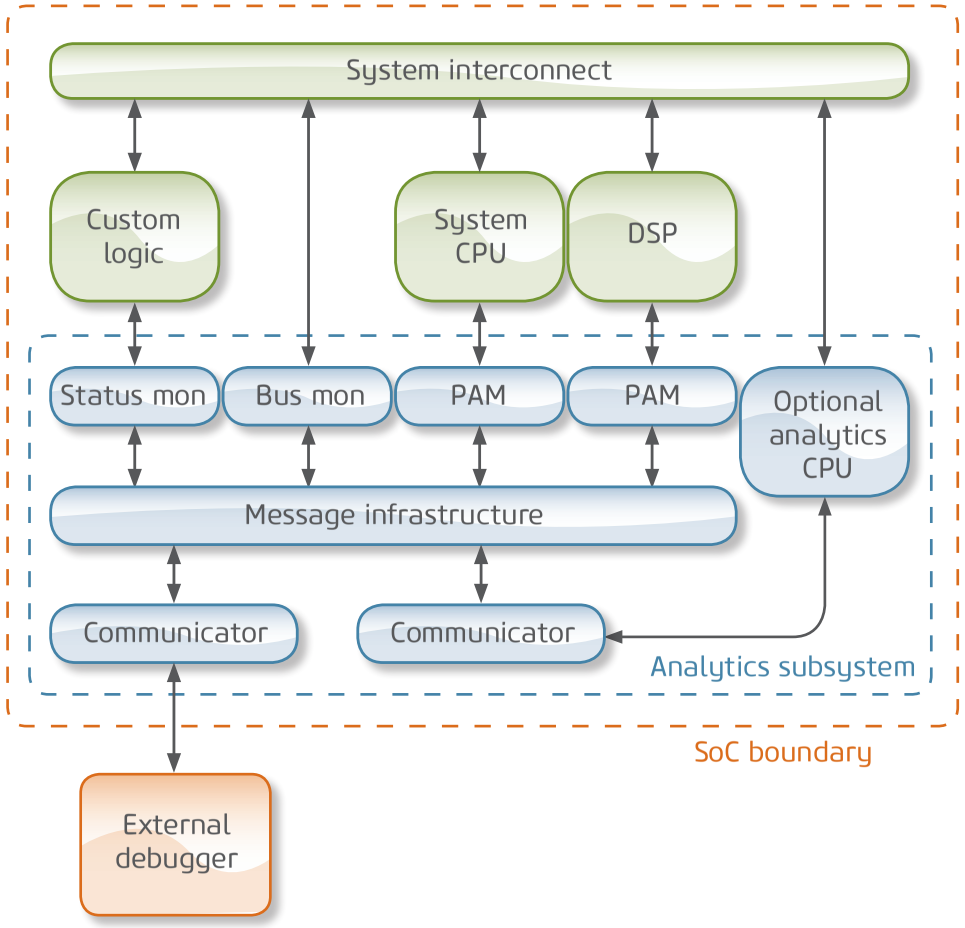
Analytics for security & functional safety

UltraSoC's embedded analytics technology provides a powerful platform for developers who need to ensure the security and functional safety of their products - particularly in the automotive industry. Our semiconductor IP can improve verification and validation during product development; and it can be used in deployed products to spot both systemic and random errors, providing a new level of safety functionality, and allowing in-field system health monitoring and advanced forensics.



UltraSoC offers a suite of semiconductor IP that non-intrusively monitors and analyzes the behavior and interactions of hardware and software at the system level. We allow system and SoC developers to gain a holistic, system-level view of complex behaviors across the SoC.

Because our solution is IP-vendor independent, it enables intelligent monitoring and understanding of the activity of any on-chip structure – including custom logic, buses, and CPU cores. This significantly improves verification and validation in development, and then operates as a monitor or safety mechanism during operation in-field.

Information and analysis gained from the UltraSoC infrastructure means that designers can more easily satisfy the functional safety, risk assessment, testing, reporting and traceability requirements of standards such as ISO 26262, IEC 61508, EN50126/8/9 and CE 402/2013; in the same way, we also facilitate the move to security standards such as SAE J3061.

UltraSoC fits gracefully into any SoC development flow and is fully compatible with industry standard development tools. It requires very little overhead in terms of silicon area and power, scaling from low-cost embedded chips to the largest SoC project.

At-a-glance

- **Scalable system-level monitoring / analytics**
- **Silicon IP + software tools**
- **IP vendor independent**
- **Non-intrusive, wire speed**
- **Security and functional safety**
- **Standards support**
  - ISO 26262, IEC 61508, EN50126/8/9 CE402/2013
  - SAE J3061
- **Supports the full product cycle**
  - Debug, validation, verification
  - Safety and security alarms
  - Risk assessment, traceability
  - Visibility after firmware updates

Functional overview

The modular, hierarchical UltraSoC architecture consists of three classes of IP block:

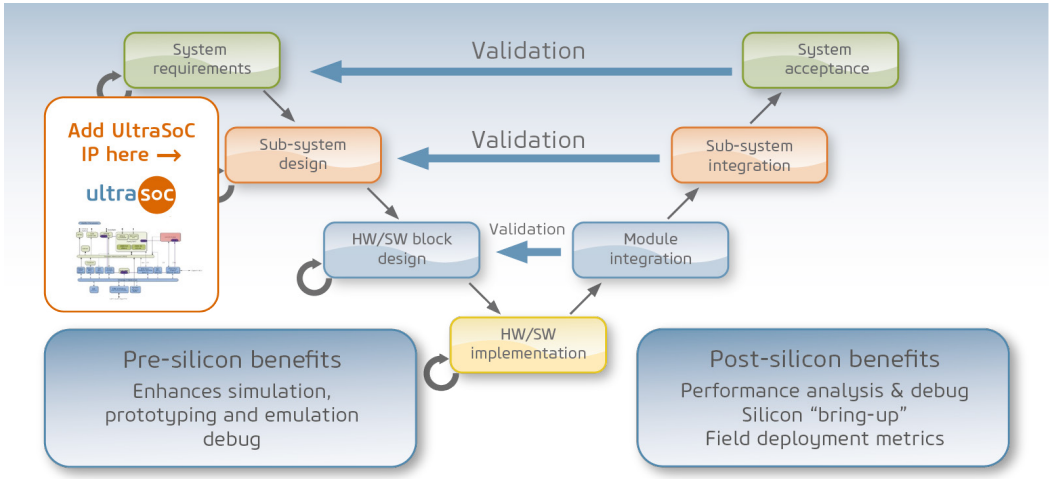
- **Analytic modules:** enable monitoring and control of system components
- **Message infrastructure:** dedicated fabric to connect UltraSoC components
- **Communicators:** interface the UltraSoC system to on-chip or external systems

UltraSoC monitors are non-intrusive and work at wire speed, making them ideal for implementing security and safety functions independently of the main system. In ISO 26262 terms, UltraSoC monitors function as a Safety Element out of Context (SEooC).

The architecture includes features specifically optimized for safety and security.

The lock-step monitor checks consistency between redundant modules. Applicable to any CPU (no native support required) and extendible to other error tests, voting systems, etc, this provides powerful, flexible options should a mismatch be detected.

Bare Metal Security® provides a hardware-based level of security "below the operating system" making it extremely difficult for an attacker to detect or subvert. It supports the requirements of SAE 3601 cybersecurity for automotive.



- **On-chip monitoring, analytics & forensics IP**
  - Delivered as parameterized soft cores
- **Non-intrusive, wire speed monitoring and analysis**
- **Development support**
  - Debug, integration, validation
- **In-life**
  - Safety: non-intrusive monitoring
  - Security
- **Independent**
  - Supports any combination of custom and vendor-supplied IP
- **Safety- and security-specific features**
  - Bare Metal Security
  - Highly granular traceability / forensics
  - Lock-step monitoring
- **Extensive partner-based support**
  - PVT monitors (Moortec)
  - NoC integration (NetSpeed)
  - Resilience (Resiltech)