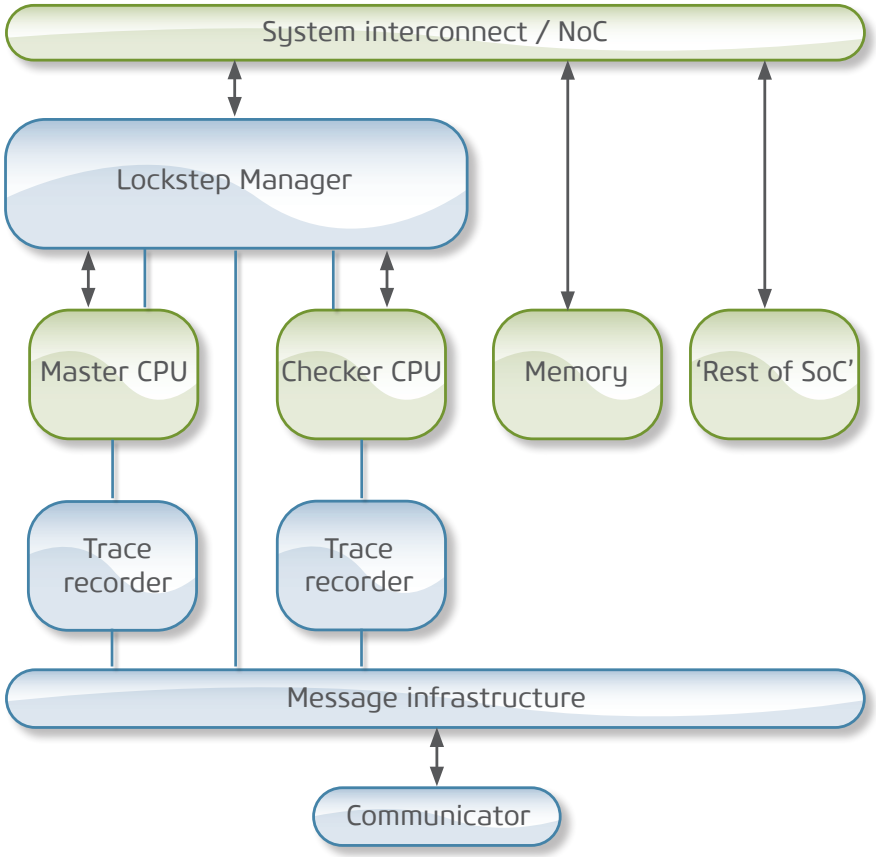
Security & functional safety in hardware

UltraSoC's embedded analytics technology provides a powerful platform for developers who need to ensure the security and functional safety of all kinds of products – from vehicles and factory robots to consumer devices. It allows designers of systems-on-chip (SoCs) to build an independent internal monitoring system into their devices. Being hardware-based, this responds in real-time and is extremely difficult for an attacker to circumvent: ensuring that the end product operates safely and securely, exactly as the designer intended.



The UltraSoC architecture places a system of intelligent monitors and actuators within the SoC. These continuously check the operation of the device, reliably and instantaneously detecting anomalous behavior.

The architecture can be used to implement common functional safety design strategies such as lockstep operation (see left). In security applications it facilitates real-time threat mitigation; prevents propagation; and can provide a detailed forensic record of system behavior in the event of an attack.

The UltraSoC on-chip infrastructure can be configured at run-time to deal with known cyber-attack vectors; and because it protects the underlying hardware, it is also robust against "zero day" attacks that designers cannot anticipate. The infrastructure is also a rich source of data, allowing the use of cloud- or edge-based analytics to build a system signature. This in turn allows the system to adapt as the threat landscape evolves.

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 ISO26262, 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 and ISO21434.

At-a-glance

- **Hardware-based security and functional safety**
- **Operates in real-time: microseconds not milliseconds**
- **Extra layer of security 'below the OS': extremely difficult to circumvent**
- **Standards support**
  - ISO26262, IEC 61508, EN50126/8/9 CE402/2013
  - SAE J3061, ISO21434
- **Supports the full product cycle**
  - Debug, validation, verification
  - Safety and security in-life
  - Risk assessment, traceability
  - Visibility after software updates
- **Delivered as silicon IP and software**

©2019 UltraSoC | **info@ultrasoc.com** | **www.ultrasoc.com**

Functional overview

The modular, hierarchical UltraSoC architecture consists of three classes of IP block: analytic modules; a message infrastructure; and communicators.

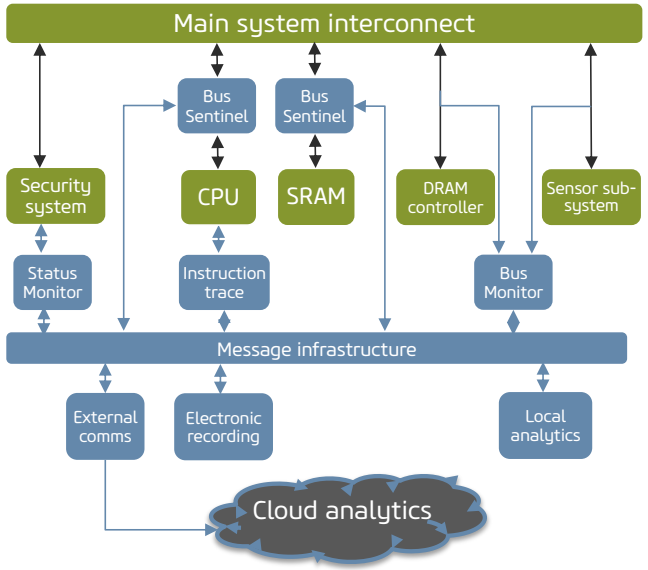
UltraSoC analytic modules work at wire speed, making them ideal for implementing security and safety functions independently of the main system. Many are designed to be non-intrusive, allowing their use in safety-critical systems without changing the operation of the main system. Others include mechanisms that provide instantaneous response to anomalous behavior.

UltraSoC monitors are a rich source of data, which can be processed at the edge or remotely in the cloud, allowing system profiling and an evolving response to changes in the cybersecurity threat landscape.

Safety- and security-specific features include:

The Lockstep Manager checks consistency between redundant subsystems of any type - CPUs, DSPs and even custom logic. It is applicable to any CPU architecture (no native support required), extendible to any number of redundant subsystems, and can be configured to verify operation at any level of granularity: at register level within the CPU, at instruction level, and at bus transaction level.

Bus Sentinel provides a hardware-based level of security working "below the operating system". It monitors transactions on the SoC's internal bus or NoC, instantaneously blocks suspicious transactions, and allows the construction of a long-term profile of system operation to secure against current and future cyber threats.



Product features

- **On-chip monitoring, analytics & forensics IP**
  - Delivered as parameterized soft (Verilog) IP
- **Wire speed monitoring & analysis**
- **In-life**
  - Safety: non-intrusive monitoring
  - Security: threat detection & mitigation, propagation prevention
- **In-lab**
  - Debug, integration, validation
  - Optimization, performance tuning
- **Bus Sentinel**
  - Additional hardware-based security layer
  - Monitors SoC bus / NoC transactions
  - Detects, blocks and records cyber-attacks
  - Enables sophisticated system profiling
- **Lockstep Manager**
  - Dual-redundancy, split / lock, master / checker, voting with any number of CPUs/subsystems
  - Register, instruction or transaction-level checking
  - 'Native' CPU support not required
- **Recording and forensics**
  - Detailed log of internal system behavior
  - Edge- or cloud-based processing / profiling