Tessent Embedded Analytics provides a complete suite of silicon IP and software for hardware-based security and functional safety; in-field and in-lab performance monitoring and optimization; and silicon bring-up and debug.

Our portfolio includes configurable blocks for hardware-based cybersecurity and safety; modules that non-intrusively monitor all major CPUs and custom logic; transaction-aware probes for common buses and interconnects; highspeed communications IP that allows the rich data we generate to be captured and recorded; and software to process and display that data.

Embedded Analytics provides a holistic, system-level view of the complex behaviors within today’s SoCs. Our IP and software helps engineers to implement safety and cybersecurity functions in hardware; and to more quickly and cost effectively debug and optimize hardware and software in the lab and in the field.

By incorporating Embedded Analytics IP into a device, designers can intelligently monitor, understand and control the activity of any on-chip structure – including custom logic, buses, and CPU cores.

With low overhead of silicon area and power, the architecture scales from low-cost embedded chips to the largest SoC project, easing the development of AI / ML chips and heterogeneous multicore designs with hundreds of hardware blocks and substantial amounts of software.

Tessent Embedded Analytics turns on-chip data into actionable information, spotting cyber threats at hardware speed; optimizing real-life product performance in the field; accelerating SoC time-to-revenue; revealing hard-to-find bugs; increasing quality; de-risking development; and reducing potential liability costs. It fits gracefully into any SoC development flow and is fully compatible with a variety of third-party development tools.

At-a-glance
- Scalable SoC monitoring / analytics
- In-life system monitoring
- Hardware-based cybersecurity threat detection, response and forensics
- Functional safety
- Performance monitoring, optimization, profiling
- Powerful in-lab development capabilities
- Bring-up and debug
- Reveals hard-to-find bugs, deadlocks
- Sophisticated software (IDE) support
- Unified view of hardware and software
- CPU vendor independent
- Hardware-based, wire speed
**Functional Overview**

The modular, hierarchical Embedded Analytics architecture consists of four classes of IP block:

- **Safety and security modules**: including our Bus Sentry and CAN Sentry products
- **Analytic modules**: monitor and control system components
- **Message infrastructure**: dedicated fabric to connect Embedded Analytics components
- **Communicators**: interface the Embedded Analytics system to on-chip or external systems

Analytic modules can probe system hardware or software. Some monitor system buses; others offer a memory-mapped peripheral device API for access by software; others are optimized to interface with CPUs; and some are "embedded logic analyzers" for monitoring custom logic. All are parameterized at design time and configurable at run time.

**Communicator modules** connect the Embedded Analytics environment to external systems either on or off-chip. They include lightweight peripheral interfaces; high-performance trace interconnects; versatile blocks such as the Universal Streaming Communicator; and industry-standard interfaces such as JTAG, USB, Ethernet and Aurora.

**Active managers** form an inherent part of the SoC’s in-life functionality

Cybersecurity is a particular focus for this class of module, since they enable mitigation and prevention responses at wire speed, and add an extra layer of defense in depth to any cybersecurity solution. The Bus Sentry, for example, monitors transactions on the bus or NoC, and instantaneously blocks suspicious activity.

---

**Product Features**

- On-chip monitoring and analytics IP
- Delivered as parameterized soft cores
- Hardware-based cybersecurity
- Instantaneously detect abnormal behaviors
- Mitigate threats, prevent propagation
- Forensic recording, threat landscape profiling
- Functional safety
- Verification and validation for standards compliance
- Continuous in-field performance optimization
- Data centers, storage etc
- Preventive maintenance / field failure analysis
- Powerful IDE & analytic software
- Breakpoints, trace, cross triggering, matching, filtering, sequencing, trace and event generation
- Optimized support for multiple CPU vendors
- Visualization and data science capabilities
- Protocol-aware monitors for bus and NoC structures
- AXI, ACE, ACElite, OCP, CHI and others
- Rich message-based infrastructure
- On and off-chip interfaces
- Vendors’ debug systems (CoreSight, PDTrace)
- IEEE1149, SWD-style, Aurora, SerDes, USB2
- Ethernet, PCIe, USB3

---

© 2021 Siemens. A list of relevant Siemens trademarks can be found here. Other trademarks belong to their respective owners.

Siemens Digital Industries Software
siemens.com/eda

Americas  +1 314 264 8499
Europe    +44 (0) 1276 413200
Asia-Pacific  +852 2230 3333