SOLUTION BRIEF

Arria® 10 SoC

Arria® 10 SoC for Secure Communications Systems

Intel (formerly Altera) provides a complete portfolio of high-bandwidth and low-power silicon solutions, software tools, and market-focused intellectual property to meet the needs of modern military secure communications systems. Sensitivity to size, weight, and power (SWaP) constraints, as well strategies to help designers deal with migrating security rules and standards, provide you a flexible approach to design for today's requirements as well as tomorrow's changing environment.

Intel's product portfolio of low-power devices with high-assurance capabilities and security features includes the Cyclone® III LS FPGA family, the Cyclone V FPGA and SoC family, and now the Arria® 10 FPGA and SoC family. The Arria 10 FPGA features a broad range of product densities and power-saving features and techniques to enable your secure communication or network system to perform more of the functions of a secure communication system in a single device. Enhanced digital signal processing (DSP) blocks and integrated ARM* processors enable single-chip functionality of both waveform and high-speed packet data processing.

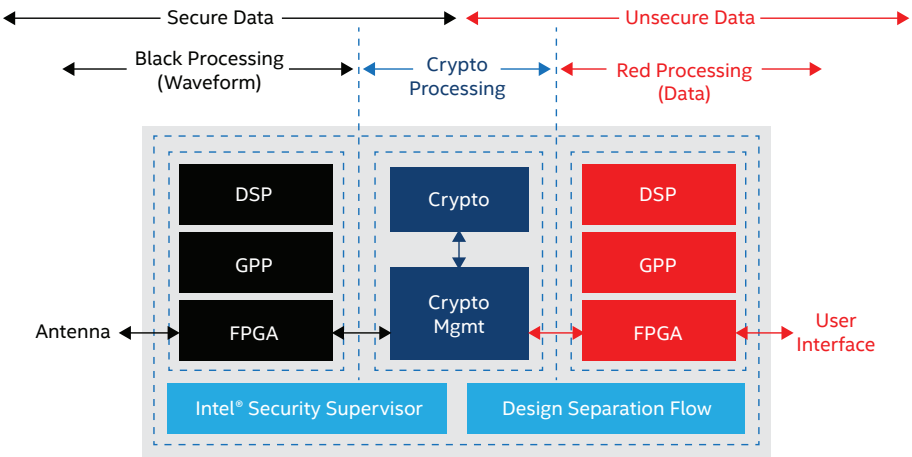
Arria 10 FPGA and SoC

Arria 10 GX: High data rate and low-power FPGAs with up to 96 transceivers up to 17.4 Gbps data rates and advanced security features.

Arria 10 SX: High data rate and low-power SoCs with up to 48 transceivers to 17.4 Gbps data rates, hardened ARM* Cortex*-A9 processors, and advanced security features.

Arria 10 GT: Very high data rate and lower power FPGAs with up to 96 transceivers up to 28.05 Gbps and advanced security features.

Figure 1. Single-Chip Waveform, Data, or System Solution Using the Arria 10 SoC



Additional Features of Intel® FPGAs Suitable for Secure Communications Systems:

- Single event upset (SEU) detection and mitigation automatically and continually monitors FPGA configuration RAM for SEU or other errors
- Extended life cycles: Intel historically provides the longest life cycles of all major FPGA providers, reducing costly end-of-life (EOL) risks to program
- Leaded packages: Intel provides leaded package options across nearly all product families
- Reliable supply chain: Intel maintains a reputation for robust and reliable supply chains
- AQEC compliance: Intel is part of the Aerospace Qualified Electronics Components (AQEC) working group and previous families hold GEIASTD- 0002-01 certifications
- DO-254 compliance solutions: Combined with certified Nios® II soft embedded processors and third party assessment partners, Intel has a long history of use in DO-254 applications
- Advanced security features: Intel has a legacy of security features in all FPGA product families to include bitstream encryption and authentication, antitamper and anti-cloning features, and now secure boot and code authentication for Arria 10 SoC ARM Cortex-A9 processors

Silicon Convergence in Military Secure Communications

The migration of military communications from point-to-point to multipoint and 'ad-hoc' networking is a challenge to interoperability design and test. Common waveform and data delivery elements are needed across a diverse set of individual user and data center endpoints. This makes FPGA and software-based designs a necessity for force interoperability.

Just as the needs of military and government users converge in joint interoperability requirements and authorities, the capabilities of integrated circuits to support these requirements is converging in Intel SoC products. Software-defined radios leverage the agility of processor-based software as well as the low power and performance advantages of dedicated and specialized function ASICs. FPGAs and SoCs are uniquely capable of bringing general purpose processors, flexible logic, and streamlined hard logic blocks for protocol, DSP, and peripheral support, enabling an optimized platform for secure communications development.

The Importance of Design Separation in High-Density Designs

One of the primary design capabilities in a secure communication system is the ability to assure data separation between black and red data processing functions, to include signal processing and memory access. This necessity only increases with high density Arria 10 SoCs. Historically, very strict data separation guidelines have been required for voice and data communications systems at the highest levels of required security.

The Intel design flow has supported a set of design separation guidelines, and tools for design separation support, since the Cyclone III LS family of FPGAs. This design separation flow will be supported for the Arria 10 FPGAs and SoCs, providing both a design and verification methodology to meet internal and external standards for data integrity and failsafe operation. Despite rapid changes in design separation verification methodologies in several industries, design separation will become more important and more difficult because of the convergence of many different data and traffic management functions into single devices.

ARRIA 10 DEVICE CAPABILITIES, SUPPORT, AND BENEFITS

CAPABILITY	BENEFITS TO SECURE COMMUNICATIONS SYSTEMS
High-Density Systemon-Chip with ARM Hardened Processors	• High-speed fabric for data plane operation, and dedicated hard processor for control plane functions • Ability to separate software-defined radio waveforms and services into hardware and software components on a single chip • New power savings features like SmartVoltage ID, low Vcc supply device options, in addition to the legacy power-saving features carried over from previous FPGA families • ARM Cortex-A9 processor has dedicated memory controller and pin connections that do not need to go through FPGA fabric
Intel SoC FPGA Embedded Design Suite Adaptive Debug Environment	• Intel SoC FPGA Embedded Design Suite includes the exclusive ARM Development Studio™ 5 (DS-5™) Intel FPGA edition that integrates SignalTap™ design interfaces • Intel's unique ability to set software and hardware triggers for integrated software/hardware testing • The ARM Cortex-A9 adds substantial capability to run test scripts and routines on-chip for enhanced debug capability • Test and debug interfaces
System Security Supervisor IP	• Integrated System Security Supervisor IP (SSIP) provides single logic block to configure, monitor, and report on all security related features in the FPGA • Fixed and productized block provides simple framework for scheduling and executing device zeroization from the SSIP in case of security compromise
Robust Multi-Key Agile Partial Reconfiguration	• Agile Partial Reconfiguration provides the capability to separately encrypt PR regions with different keys, and indicate in a header which key to use for decryption • Provides multi-stage secure boot capability to FPGA bitstream configuration • Powerful tool for multi user environments to enhance system trust and protect intellectual property (IP)

ARRIA 10 FPGA/SOC PRODUCT FAMILY HIGHLIGHTS

LOGIC ELEMENTS	TRANSCEIVERS	VERSIONS	MEM	PACKAGES	APPLICATION
160K	6-12	GX, SX	9 Mb	19 mm, 27 mm, 29 mm	Battery Power, Soldier Radio
220K	6-12	GX, SX	11 Mb	19 mm, 27 mm, 29 mm	Module, Soldier Radio
270K	12-24	GX, SX	15 Mb	27 mm, 29 mm, 35 mm	SDR Waveform and Security
320K	12-24	GX, SX	17 Mb	27 mm, 29 mm, 35 mm	SDR Waveform and Security
480K	12-36	GX, SX	28 Mb	29 mm, 35 mm	Multi-Channel SDR
570K	24-48	GX, SX	35 Mb	35 mm, 40 mm	Multi-Channel SDR
660K	24-48	GX, SX	42 Mb	35 mm, 40 mm	Multi-Channel SDR, High-Rate Data Encryption
900K	24-96	GX, GT	47 Mb	35 mm, 40 mm, 45 mm	High-Rate Data Encryption
1,150K	24-96	GX, GT	53 Mb	35 mm, 40 mm, 45 mm	High-Rate Data Encryption

Want to Dig Deeper?

To learn more about designing secure communications systems using the Arria 10 FPGA and SoC, visit www.altera.com/products/fpga/arria-series/arria-10/overview.html

To learn more about other solutions for Military secure communications systems visit www.altera.com/solutions/industry/military/applications/secure-communication/mil-secure.html

or contact your local Intel representative.