SHA3 CoProcessors IP Core Reference Manual

SHA3 IP Core architecture, interfaces, internal formatting, and performance

Contents

Document Overview 4
System Overview 4
Modes supported 6
Example System Use 7
Hardware Interface Control Documentation 7
AXI4-Lite Configuration Interface 7
Medium-Performance Iterative Interface 8
Configurable-Round Wide Interface 8
Performance 8
AXI4-32 iterative data path 9
AXI4-128 iterative data path 9
AXI4-128 configurable-round RPC=2 data path 9
Reference Architecture 10
Portability and Integration 10
Fail Safe//High Assurance versions 10
Simulation Environment 11
Implementation 11
Synthesis and Place-and-Route 11
Clocking and Clock-Domain Crossing 12
Top-Level Register Map 12
Verification Results 13
Current OOC Implementation Results 14
Resource Requirements 14
Verification, Warranty Disclaimer, Limitation of Liability, and Exclusive Remedy 15
Customer Verification Responsibility 15
Warranty Disclaimer 15

Limitation of Liability 15

Liability Cap 16

Exclusive Remedy 16

High-Risk Applications 16

Figure 1 Summary 4

Figure 2 Capabilities 5

Figure 3 Iterative Coprocessor IP Core 5

Figure 4 Configurable-Round Coprocessor IP Core 6

Figure 5 Control & Status 8

IP Core	SHA3 hardware accelerator supporting SHA3-224, SHA3-256, SHA3-384, and SHA3-512
Primary Interface	AXI4-Lite x32 control plus AXI4-32/128/256/512 raw-message data
Implementation Forms	Iterative RTL core and optional configurable Rounds Per Cycle (RPC) pipelined high-throughput RTL core
Deliverables	Unencrypted synthesizable RTL, software drivers, wrappers for RAMs/FIFOs, and a full self-checking testbench

Figure 1 Summary

Document Overview

This manual provides a high-level reference for the SHA Solutions SHA3 CoProcessors IP Core. It describes the supported digest modes, integration interfaces, implementation options, deliverables, simulation environment, and implementation expectations for FPGA or ASIC targets.

The IP core computes SHA3-224, SHA3-256, SHA3-384, and SHA3-512. Both the iterative and configurable-round cores accept arbitrary byte-length raw messages and perform the final FIPS 202 SHA-3 formatting internally.

System Overview

The SHA3 CoProcessors IP Core is an unencrypted RTL implementation of the SHA3 hash functions. It is delivered in fully synthesizable form and is suitable for targeting mainstream FPGA devices, high-end FPGA devices, or ASIC flows.

- Supported digest modes: SHA3-224, SHA3-256, SHA3-384, and SHA3-512.
- Iterative version: runtime-selectable SHA3 mode, one Keccak-f[1600] round per clock, and internal final-block formatting.
- Configurable-round version: selectable 1/2/4/8/12/24-round combinational unroll with internal final-block formatting.
- Memory and FIFO wrappers isolate soft RAMs and FIFOs so target-specific libraries can be ported cleanly.

- Software drivers and a full self-checking testbench are provided with the IP deliverables.

Capability	Reference Behavior
Hash algorithms	SHA3-224, SHA3-256, SHA3-384, and SHA3-512
Iterative latency	24 clocks per permutation; exact-rate final blocks require an internal second permutation
Performance	Measured 256 MiB DMA and completed-hash results are provided in the Performance section
RTL delivery	Unencrypted, fully synthesizable source RTL
Target support	FPGA and ASIC flows, with portable wrappers for RAMs and FIFOs

Figure 2 Capabilities

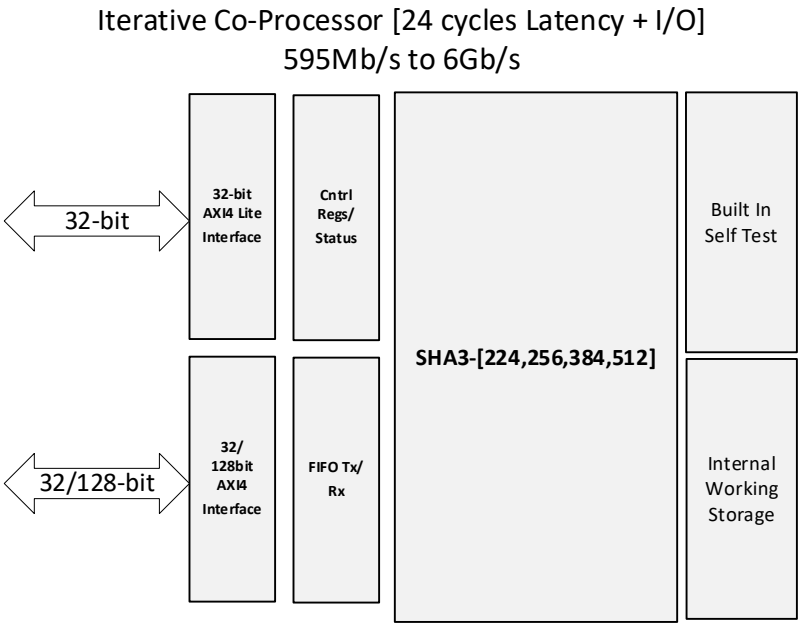


Figure 3 Iterative Coprocessor IP Core

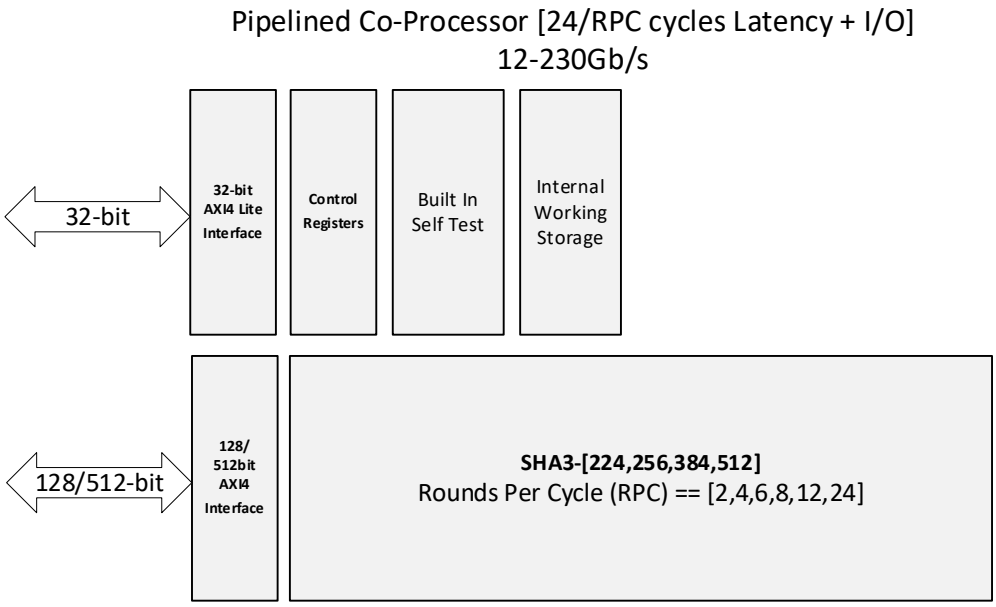


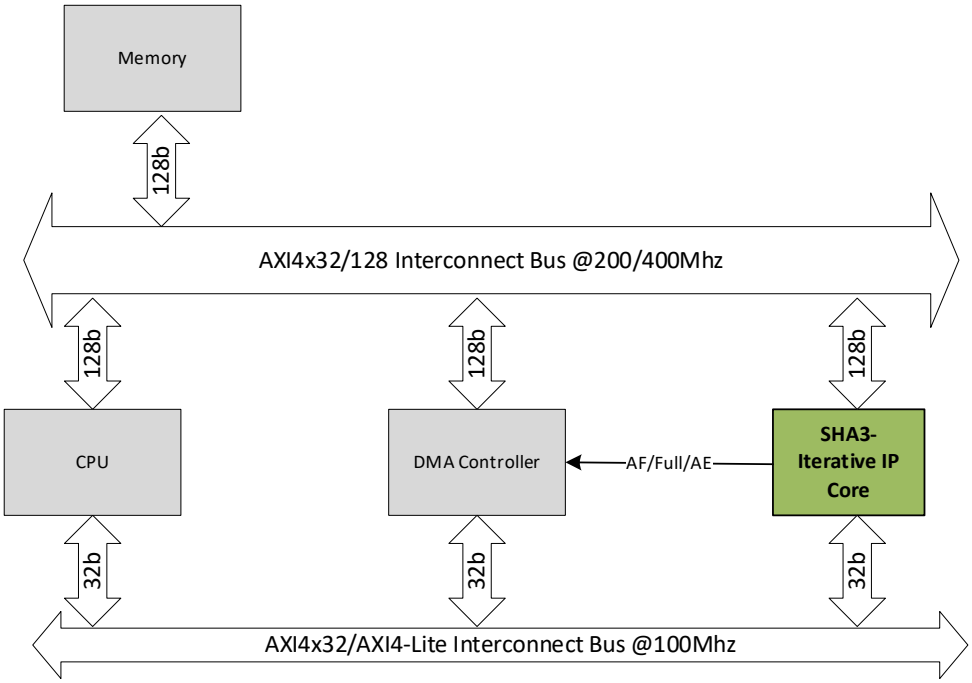
Figure 4 Configurable-Round Coprocessor IP Core

Modes supported

The following SHA3 modes are supported at run time by setting the control register to select the mode [224,256,384,512].

SHA-3 Mode	Input Width (Rate)	Input Width (Bytes)	Keccak-f[1600] Rounds per Block	Digest Width
SHA3-224	1152 bits	144 bytes	24	224 bits (28 bytes)
SHA3-256	1088 bits	136 bytes	24	256 bits (32 bytes)
SHA3-384	832 bits	104 bytes	24	384 bits (48 bytes)
SHA3-512	576 bits	72 bytes	24	512 bits (64 bytes)

Example System Use



1. CPU Sets up SHA3 Mode & Msg Byte Length in SHA3 Regs via AXI4L
2. CPU Sets up DMA to transfer 256MB message from Memory to SHA3 FIFO via AXI4-128/32 bursts
3. CPU polls for SHA3 Digest complete.
4. CPU reads computed SHA3 Digest from AXI4L Regs

The example system use case is targeted around a non-cacheable AXI4L interface for register configuration and status, and a separate higher bandwidth DMA capable transfer interface for the message data.

Hardware Interface Control Documentation

AXI4-Lite Configuration Interface

The supported wrappers use AXI4-Lite x32 for configuration and status plus a separate AXI4-32, AXI4-128, AXI4-256, or AXI4-512 full data interface for raw message DMA and digest readback. The AXI data aperture decodes 4 KiB and accepts incrementing bursts of up to 256 beats. The application-facing FIFO, message assembler, SHA3 input, and digest path use the selected data width end to end.

Software selects the SHA3 mode in REG9, writes the complete message byte length to REG11, and then DMAs exactly that many raw user message bytes to the FIFO input. REG11 starts the autonomous operation. AXI WSTRB selects the valid bytes in each accepted beat. REG2 Tx_EOF_Mod4 is retained only for compatible readback and is not used.

DMA of messages longer than 4KB require the software to monitor the FIFO status via AXI4l registers or a autonomous DMA may use the DMA_*status signals to regulate flow control.

Interface Area	Purpose	Notes
Configuration	Select SHA3 mode in REG9	SHA3-224/256/384/512; core type is a wrapper parameter.
Message length	Write total bytes to REG11 and start	REG11 is authoritative; REG2 Tx_EOF_Mod4 is unused.
Raw input DMA	Load exactly REG11 bytes	User message data to hash. No preformatting required.
Status / digest	Throttle DMA and return the result	TX level plus Full/AF/AE flags; width-matched digest beats.

Figure 5 Control & Status

Medium-Performance Iterative Interface

The iterative core supports all four modes at runtime in the AXI4-32 and AXI4-128 systems. The pipelined wrapper supports AXI4-128, AXI4-256, and AXI4-512 data; the released OOC configuration uses AXI4-512. DMA_TxFIFO_Full, DMA_TxFIFO_AF (three-quarters full), and DMA_TxFIFO_AE are also exported as discrete flow-control status signals.

Configurable-Round Wide Interface

The AXI4-128/256/512 fully pipelined system uses ready/valid flow control internally. Independent single-block messages can enter the core on consecutive clocks. Blocks in one long message retain the required sponge-state dependency. The wrapper derives internal FIRST/LAST and valid-byte metadata from REG11 and the accepted raw byte count; an exact-rate final block automatically adds a padding-only block.

Performance

These are simulated-cycle measurements for the same 256 MiB pseudo-random image at a modeled 200 MHz on the existing Linux/WSL instance with Verilator 5.051. DMA includes each raw burst, its response, the software-style REG1 FIFO-level check, and any almost-full pause; it ends after the final burst is accepted. DMA+hash ends at the exact core digest-valid edge and excludes digest FIFO reads.

Every result matched an independent OpenSSL digest. These are current-source results after the registered compaction, assembly, and full-AXI address handshakes. MiB/s uses 1 MiB = 1,048,576 bytes.

AXI4-32 iterative data path

Mode	Core	DMA (ms)	DMA (MiB/s)	DMA+hash (ms)	Message Throughput
SHA3-224	Iterative	363.505	704.255	363.507	5.9Gb/s
SHA3-384	Iterative	374.259	684.017	374.261	5.7Gb/s
SHA3-512	Iterative	503.314	508.629	503.317	4.2Gb/s

AXI4-128 iterative data path

Mode	Core	DMA (ms)	DMA (MiB/s)	DMA+hash (ms)	Message Throughput
SHA3-224	Iterative	251.652	1,017.276	251.658	8.5Gb/s
SHA3-384	Iterative	348.442	734.700	348.450	6.1Gb/s
SHA3-512	Iterative	503.305	508.638	503.317	4.2Gb/s

AXI4-128 configurable-round RPC=2 data path

Mode	Core	DMA (ms)	DMA (MiB/s)	DMA+hash (ms)	Message Throughput
SHA3-224	Configurable RPC=2	130.477	1,962.025	130.490	16.5Gb/s
SHA3-384	Configurable RPC=2	180.661	1,417.018	180.678	11.8Gb/s

Mode	Core	DMA (ms)	DMA (MiB/s)	DMA+hash (ms)	Message Throughput
SHA3-512	Configurable RPC=2	260.955	981.013	260.979	8.2Gb/s

The released configurations are AXI4-32 iterative, AXI4-128 iterative, and AXI4-128 configurable-round RPC=2. For one long message, the block-to-block sponge-state dependency controls hashing cadence. The configurable-round core reduces each permutation to 24 / RPC processing clocks.

Reference Architecture

The reference architecture separates software-visible control, the SHA3 permutation datapath, local buffering, and target-dependent memory/FIFO bindings. This separation keeps the algorithmic RTL portable while allowing the integration wrapper to be optimized for a selected FPGA family or ASIC library.

1. AXI4-Lite control and status logic receives software commands and exposes completion state.
2. Built in Self Test logic verifies the core is functioning correctly.
3. Input buffering queues raw message data and AXI byte strobes. The autonomous assembler counts accepted bytes against REG11 and creates rate-sized SHA3 blocks without software intervention.
4. The SHA3 datapath formats the final block internally and performs the selected SHA3-224/256/384/512 computation.
5. Output digest handling returns the selected-width result to software or downstream logic.
6. RAM and FIFO wrapper layers isolate inferred or library-specific storage resources.

Portability and Integration

The IP is supplied in RTL form and is not encrypted. All included design units are fully synthesizable. Wrappers are provided for soft RAMs and FIFOs so optimized implementations can be ported to specific target libraries, including ASIC memory macros or FPGA-native resources such as Xilinx built-in FIFOs.

Fail Safe//High Assurance versions

The IP is also available with Error Correction Coding (ECC) on all memories and storage, as well as optionally with a High Assurance Fail Safe or Tripple Modular Redundant versions for use in systems where computations must be safe [e.g. IEC 61508, ISO 26262, DO-254 etc]. These techniques also make the core suitable for use in Radiation Environments [LEO, GEO orbits etc].

Simulation Environment

The IP package includes a full self-checking testbench. The simulation environment is intended to validate the SHA3 modes, control sequencing, data movement, and digest comparison without relying on manual waveform review.

- Module-level tests exercise raw empty and randomized short messages, control, and datapath behavior.
- Top-level AXI tests cover empty, short, rate-minus-one, exact-rate, and multi-block raw messages in every mode.
- Self-checking scoreboards compare produced digests against expected values.
- File-backed DMA regressions compare 256 MiB results with OpenSSL on Linux/WSL using Verilator.

Implementation

Synthesis and Place-and-Route

The SHA3 IP core is intended for standard synthesis and implementation flows. The unencrypted RTL delivery allows integrators to run lint, simulation, synthesis, timing analysis, and implementation using their normal FPGA or ASIC toolchain.

For FPGA targets, the portable RAM/FIFO wrappers can map to inferred resources or device-optimized primitives. For ASIC targets, the same wrapper boundary allows library-specific RAM macros and FIFO implementations to be substituted without changing the algorithmic SHA3 RTL.

Deliverable	Included Content
RTL source	Unencrypted, synthesizable SHA3 IP core RTL
Wrappers	Portable wrappers for soft RAMs and FIFOs
Drivers	Software drivers for core configuration and operation
Verification	Full self-checking testbench for functional validation
Integration support	Guidance for FPGA/ASIC resource binding and target-specific optimization

Clocking and Clock-Domain Crossing

The 32-bit AXI4-Lite interface is clocked by s_axil_clk; the full AXI4 data interface, both FIFOs, the message assembler, and the SHA-3 core are clocked independently by s_aclk. The reference OOC constraints use 100 MHz for s_axil_clk and 200 MHz for s_aclk and declare the clocks asynchronous.

Every AXI4-Lite register read and write uses a coherent NRZ request/acknowledge mailbox. The source holds its address and payload stable while the request state crosses a two-flop synchronizer. The datapath domain commits a write or snapshots read data before returning the acknowledge state. The AXI4-Lite response is issued only after that acknowledge returns, so software sees committed state without sampling a changing multibit bus. The common active-low s_aresetn asynchronously resets both domains.

Top-Level Register Map

All addresses are byte offsets in the 32-bit AXI4-Lite aperture. Reserved bits read zero unless explicitly described as readback. Application registers and status are owned by the s_aclk domain and are reached through the NRZ mailbox.

Reg	Offset	Access	Reset / fields / behavior
REG0	0x00	RO	RX status: [0] empty, [1] almost empty, [2] almost full, [8] digest available/IRQ, [31:16] unread digest bytes.
REG1	0x04	RO	TX status: [0] full, [1] at least 3/4 full, [2] almost empty, [15:3] beat occupancy, [28:16] bytes in last completed burst.
REG2	0x08	RW	TX control, reset 0x80000000: [31] TX FIFO reset; [5:4] legacy Tx_EOF_Mod4 readback is unused; all other bits reserved readback.
REG3	0x0C	RW	RX control, reset 0x80000000: [31] RX FIFO reset; [30:0] reserved readback.
REG4	0x10	RW	General-purpose output GPO[31:0].
REG5	0x14	RW	General-purpose output GPO[63:32].
REG6	0x18	RO	General-purpose input GPI[31:0]; tied to zero by the SHA-3 wrappers.

Reg	Offset	Access	Reset / fields / behavior
REG7	0x1C	RO	General-purpose input GPI[63:32]; tied to zero by the SHA-3 wrappers.
REG8	0x20	RW	Reserved 32-bit application access-control readback register.
REG9	0x24	RW	SHA control, reset 0x00000003: [1:0] mode 0/1/2/3 = SHA3-224/256/384/512; write-one [8] clears sticky complete/error.
REG10	0x28	RO	SHA status: [0] KAT done, [1] KAT pass, [2] KAT fail, [3] user complete, [4] busy, [5] digest writer busy, [6] error, [7] digest available, [9:8] active mode, [15:10] error code.
REG11	0x2C	RW	TxMessageByteLen[31:0]. A full-word write starts one autonomous raw-message operation; zero starts the empty message.
REG12	0x30	RO	User-message permutation count since reset.
REG13	0x34	RO	Capabilities: [3:0] mode mask 0xF, [15:8] maximum rate 144 bytes, [23:16] AXI beat bytes 4/16/32/64, [31:24] protocol version 3.
REG14	0x38	RO	Total core permutation count, including reset-time KATs.
REG15	0x3C	RO	SHA subsystem identifier/version 0x53483303.

REG10 last-error codes are: 1 = REG11 written while unavailable, 2 = startup KAT failed, 3 = DMA byte count exceeded REG11, 4 = accepted beat contained no valid bytes, and 5 = SHA core sequence error. REG11 is the only message-length authority; REG2 Tx_EOF_Mod4 is unused.

Verification Results

The dual-clock directed Verilator regression passed 120 cases: 24 cases each for AXI4-32 iterative, AXI4-128 iterative, and AXI4-128/256/512 configurable-round wrappers. Every build exercises all four SHA-3 modes over empty, short, rate-boundary, exact-rate, and multiblock messages. Reset-time KAT now contains both the empty message and the one-block message "abc" for SHA3-224/256/384/512.

Current OOC Implementation Results

Vivado 2026.1 evaluated the complete integrated wrappers out of context on xcvu9p-flga2104-2-e. AXI4-Lite is constrained to 100 MHz, the data/FIFO/SHA domain to 200 MHz, and the clock groups are asynchronous. Maximum input/output delays are one-half of the associated clock period. WNS is the worst setup slack against those constraints. The x32 and x128 FIFO36E2 and RTL/BRAM variants routed with positive slack. AXI4-128 configurable RPC>2 designs requires a 22nm or faster ASIC implementation to meet timing at 200Mhz so these are not routed in the FPGA emulation target.

Configuration	CLB LUTs	CLB registers	BRAM tiles	DSPs	WNS (ns)
AXI4-32 iterative, FIFO36E2	10,446	8,781	2	0	+0.648 routed
AXI4-32 iterative, RTL BRAM	10,589	8,890	1	0	+0.587 routed
AXI4-128 iterative, FIFO36E2	13,703	9,603	4	0	+0.434 routed
AXI4-128 iterative, RTL BRAM	13,015	9,909	4	0	+0.174 routed
AXI4-128 configurable RPC=2 (synth only)	33,982	19,391	4	0	+0.235 routed

Resource Requirements

Current-source utilization, implementation status, and WNS are reported in Current OOC Implementation Results above.

Verification, Warranty Disclaimer, Limitation of Liability, and Exclusive Remedy

Customer Verification Responsibility

The IP Core has undergone internal verification and testing by the Vendor; however, such verification is performed for the Vendor's internal purposes only and does not constitute a representation, warranty, or guarantee that the IP Core is error-free, defect-free, suitable for any particular application, or capable of meeting the Customer's specific functional, performance, timing, reliability, safety, security, regulatory, environmental, or operational requirements.

The Customer acknowledges and agrees that it is solely responsible for the verification, validation, integration, implementation, qualification, and testing of the IP Core within the Customer's design and for determining the suitability of the IP Core for the Customer's intended application. The Customer assumes all risks associated with the use of the IP Core in any FPGA, ASIC, SoC, or other hardware or software implementation.

Warranty Disclaimer

THE IP CORE IS PROVIDED "AS IS" AND "WITH ALL FAULTS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE VENDOR DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, ACCURACY, COMPLETENESS, PERFORMANCE, RELIABILITY, OR ERROR-FREE OPERATION.

The Vendor does not warrant that the IP Core will operate without interruption, meet the Customer's requirements, or be free from defects, vulnerabilities, design errors, implementation errors, documentation errors, or other deficiencies.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE VENDOR SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF ANY KIND, INCLUDING, WITHOUT LIMITATION:

* Silicon re-spin costs;
* Mask costs;
* Manufacturing costs;
* Assembly or test costs;
* Product recall costs;

* Qualification or certification costs;
* Field failures;
* Warranty claims;
* Loss of profits;
* Loss of revenue;
* Loss of business opportunity;
* Loss of data;
* Business interruption; or
* Failure of the Customer's product or system to satisfy its intended functional or operational requirements,

whether arising in contract, tort (including negligence), strict liability, warranty, or otherwise, even if the Vendor has been advised of the possibility of such damages.

Liability Cap

Notwithstanding any provision of this Agreement to the contrary, the Vendor's aggregate cumulative liability arising out of or relating to the IP Core, this Agreement, or the use of the IP Core shall not exceed the total license fees actually paid by the Customer for the specific IP Core giving rise to the claim.

Exclusive Remedy

The Customer's sole and exclusive remedy for any defect, nonconformity, or other claim relating to the IP Core shall be, at the Vendor's sole discretion:

(a) correction of the defect;
(b) provision of a corrected or updated version of the IP Core, if available; or
(c) refund of the license fees actually paid for the affected IP Core upon termination of the applicable license.

The remedies set forth in this Section are exclusive and are in lieu of all other rights or remedies available at law or in equity.

High-Risk Applications

Unless expressly agreed to in writing by the Vendor, the IP Core is not designed, intended, or warranted for use in life-support systems, nuclear facilities, aviation safety systems, weapons systems, or other applications where failure of the IP Core could reasonably be expected to result in death, personal injury, or severe property or environmental damage. The Customer assumes all risks associated with any such use.