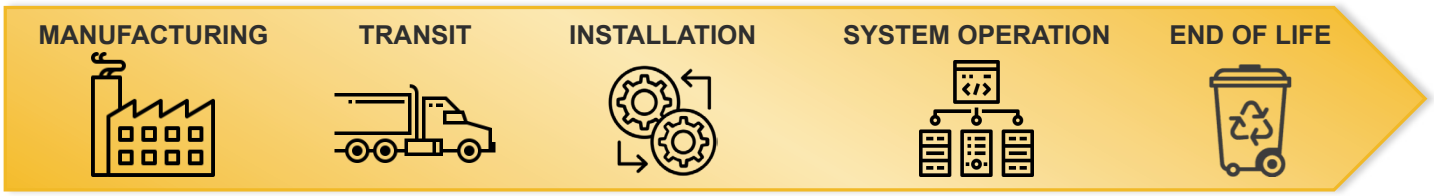
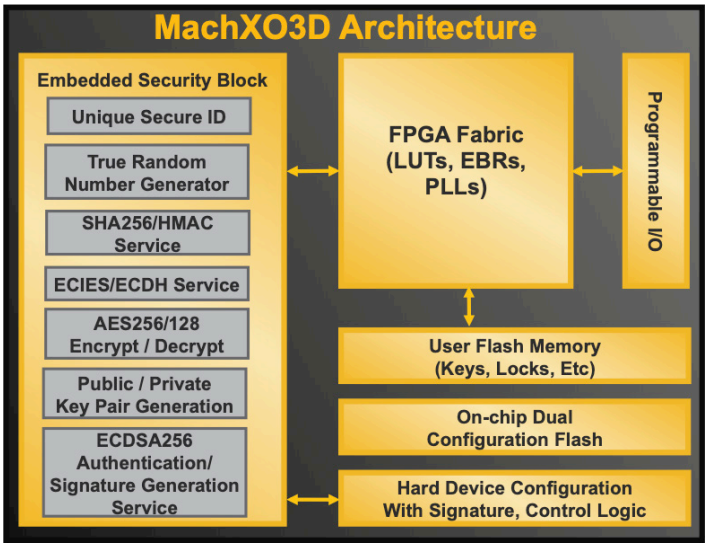
MachXO3D™

Enhance Secure Control Applications with **Hardware Root-of-Trust** and **Dual Boot** capabilities to **simplify** implementation of **comprehensive**, **flexible** and **robust** hardware security throughout the product lifecycle.



Secure Control

- Built on proven MachXO3LF architecture.
- Adds on Embedded Security Block that enables Hardware Root-of-Trust and pre-verified cryptographic functions
- On Device Configuration Flash enables dual boot eliminating the need for external memory
- Hardened Device Configuration Engine ensures only FPGA configurations from a trusted source can be installed



Features

	MachXO3D-4300	MachXO3D-9400
LUTs	4300	9400
User Flash (kbits)	367 / 1122[1]	1088 / 2693[1]
Hardened Security	Yes	
On-device Dual-boot	Yes	
I3C compatible I/O[2]	Yes	
Temperature Grades	Com / Ind / Auto	

1. When dual-boot is disabled, image space can be repurposed as extra UFM

Available Packages

	I/O Count	
0.5 mm Spacing	**MachXO3D-4300**	**MachXO3D-9400**
72 QFN (10 mm x 10 mm)	58 (HC / ZC)	58 (HC / ZC)
0.8 mm Spacing		
256-ball caBGA (14 mm x 14 mm)	206 (HC[1] / ZC)	206 (HC / ZC[1] / HE[2])
400-ball caBGA (17 mm x 17 mm)		335 (HC / ZC)
484-ball caBGA (19 mm x 19 mm)		383 (ZC[1] / HE[2])

1. Available in automotive grade
2. Available in automotive grade only
HC = Performance (VCC = 3.3 / 2.5 V)
ZC = Low Power (VCC= 3.3 / 2.5 V)
HE = Performance (VCC = 1.2 V)

Robust Security

- MachXO3D complies with NIST SP 800 193 Platform Firmware Resiliency (PFR) Guidelines
  - **Protects** non-volatile memory through access control
  - Cryptographically **detects** and prevents boot from malicious code
  - **Recovers** to latest trusted firmware in case of corruption
- Industry's first control-oriented FPGA compliant with NIST PFR guidelines
- Programmable logic minimizes attack surface dynamically configuring access control throughout product lifecycle

Comprehensive Security

MachXO3D Enables	Security Features
Data Security	Data Encryption
Equipment Security	Firmware Authentication
Data Integrity	Data Authentication
Design Security	Code Encryption
Brand Protection	Device Authentication

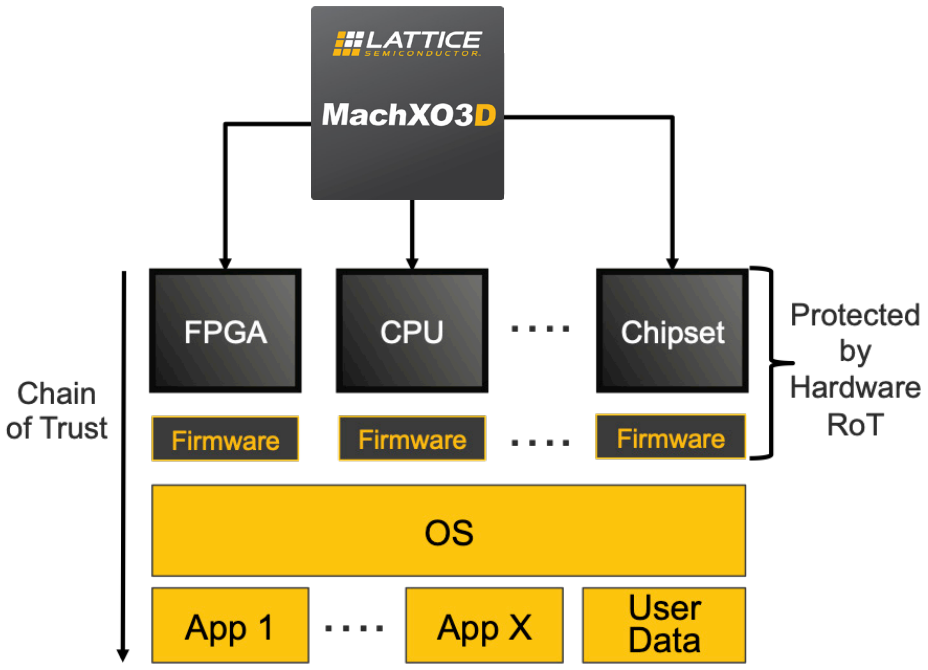
Flexible

- Wide range of temperature grade options including: Commercial, Industrial and AEC-Q100 qualified Automotive
- Provides secure and reliable in system updates
  - Dual Boot enables Fail Safe Reprogramming
  - Hardened Device Configuration Engine prevents unauthorized access to configuration memory

Simple

- Simplifies chain of trust implementation by integrating Root-of-Trust with platform's first on, last off device
- Protects platform processor firmware with no code changes
- MachXO3D is pin compatible with MachXO3

Chain of Trust with MachXO3D



Applications Support
www.latticesemi.com/support

September 2020
Order #: I0268 Rev. 2