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

<table>
<thead>
<tr>
<th></th>
<th>MachXO3D-4300</th>
<th>MachXO3D-9400</th>
</tr>
</thead>
<tbody>
<tr>
<td>LUTs</td>
<td>4300</td>
<td>9400</td>
</tr>
<tr>
<td>User Flash (kbits)</td>
<td>367 / 1122¹</td>
<td>1088 / 2693¹</td>
</tr>
<tr>
<td>Hardened Security</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>On-device Dual-boot</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>I3C compatible I/O²</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Temperature Grades</td>
<td>Com / Ind / Auto</td>
<td></td>
</tr>
</tbody>
</table>

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

### Available Packages

<table>
<thead>
<tr>
<th>I/O Count</th>
<th>MachXO3D-4300</th>
<th>MachXO3D-9400</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5 mm Spacing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>72 QFN (10 mm x 10 mm)</td>
<td>58 (HC / ZC)</td>
<td>58 (HC / ZC)</td>
</tr>
<tr>
<td>0.8 mm Spacing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>256-ball caBGA (14 mm x 14 mm)</td>
<td>206 (HC¹ / ZC)</td>
<td>206 (HC / ZC / HE²)</td>
</tr>
<tr>
<td>400-ball caBGA (17 mm x 17 mm)</td>
<td>335 (HC / ZC)</td>
<td></td>
</tr>
<tr>
<td>484-ball caBGA (19 mm x 19 mm)</td>
<td>383 (ZC¹ / HE²)</td>
<td></td>
</tr>
</tbody>
</table>

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

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

Comprehensive Security

**MachXO3D Enables**

- Data Security
- Equipment Security
- Data Integrity
- Design Security
- Brand Protection

**Security Features**

- Data Encryption
- Firmware Authentication
- Data Authentication
- Code Encryption
- Device Authentication

Applications Support

www.latticesemi.com/support