



The Low Power Programmable Leader

# Lattice Security Solutions

# MARKET SEGMENT REQUIREMENTS

## Advanced Security Features

- Hardware Root-of-Trust (RoT)
- Platform Firmware Resilience (PFR)
- Instant-on
- Integrated dual boot
- Post Quantum Cryptography (PQC)

**Compliant Security Solutions for  
Every Market Segment**

## Flexible I/Os & High Programmability

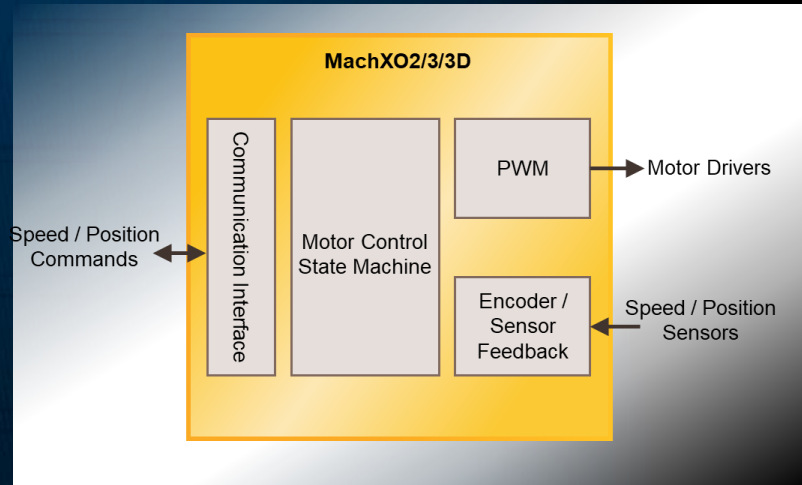
- High I/O count
- Various I/O voltage support
- Hot-socketing support

## Low Power & Small Form Factor

- Simplify thermal design
- Long lasting performance
- As small as 3 x 3mm in size

# Industrial & Automotive Applications

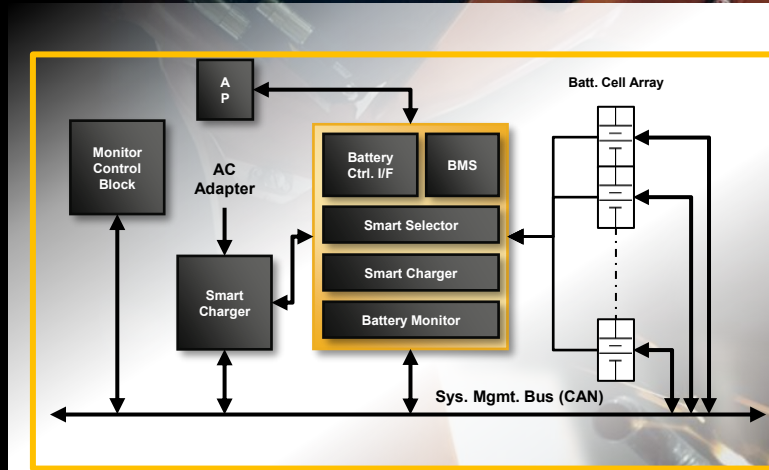
## MOTOR CONTROL



### Key Features

- Easy to use package
- Single-Chip FPGA

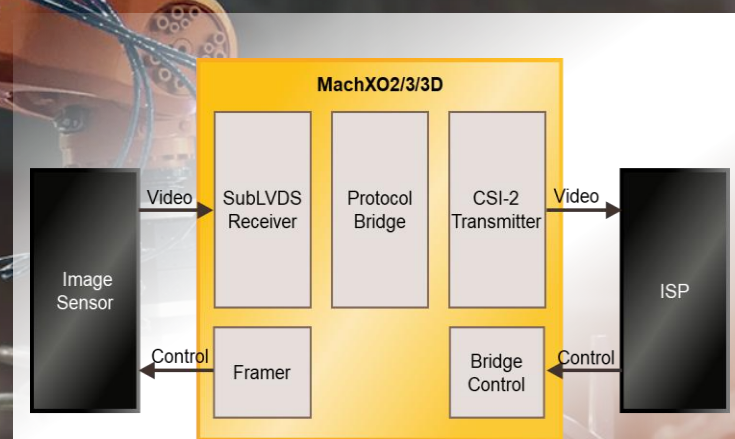
## BATTERY MANAGEMENT CONTROL



### Key Features

- Intelligent cell balancing for charge equalization per battery cell
- Control charge/ discharge process and real-time battery information

## CAMERA/DISPLAY BRIDGING

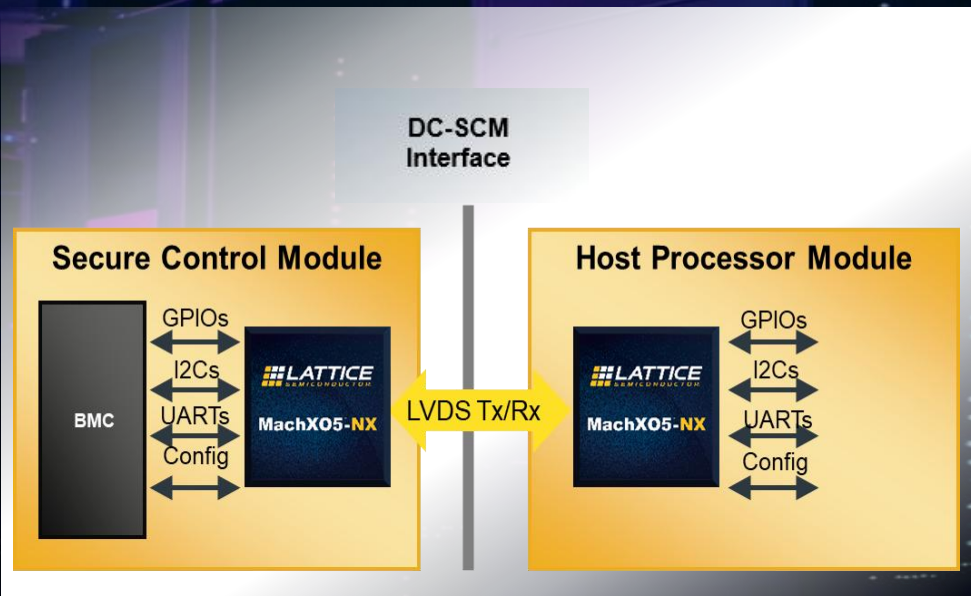


### Key Features

- Fast I/O (900 Mbps in XO3)
- Small Footprint Packages

# Server Compute and Communications Applications

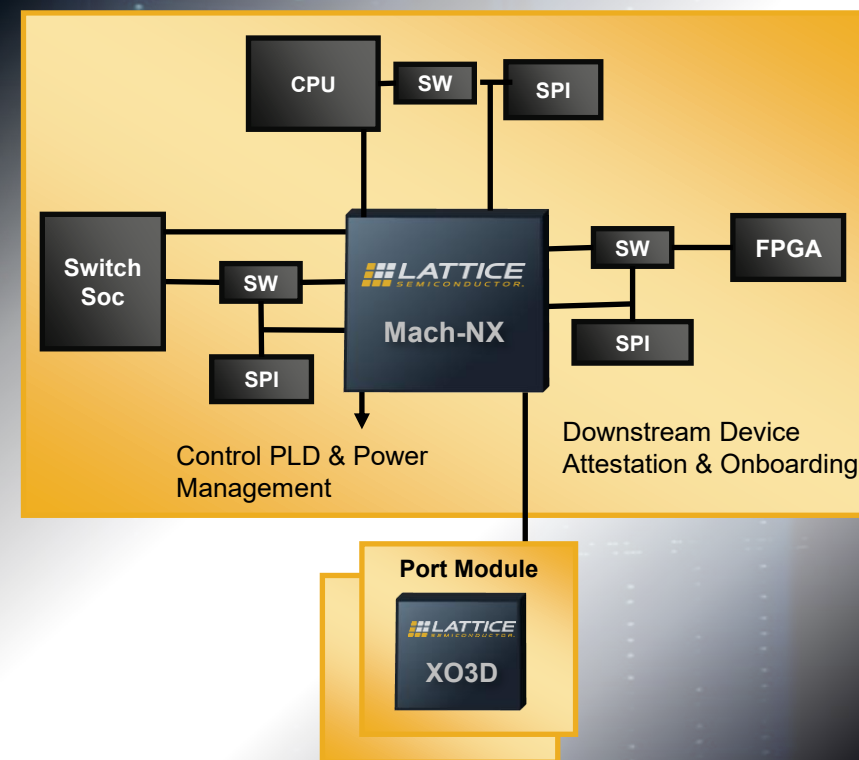
## SECURE CONTROL MODULE



### Key Features

- Modular design for dis-aggregated control logic
- Supports LVDS Tunneling Protocol & Interface (LTPI) to aggregate low-speed serial interfaces

## NETWORK SWITCH



### Key Features

- Scalable PFR (Programmable Fabric Resource)
- End-to-End Security

# FPGAs With Hardware Root Of Trust



## MachXO2

### Key value

- More Voltage Options
- Low power
- Instant On

### Application

- Microprocessor Interface Expansion
- Hardware Acceleration



## MachXO3

### Key value

- Extended Temperature Range
- Instant on
- Small Package

### Application

- Motor Control Interface
- Platform Management & Control



## MachXO3D

### Key value

- Security
- Dual Boot Flash
- Platform Firmware Resilience (PFR)

### Application

- Secure Server
- Platform Management & Control



## MachXO4™

### Key value

- Flexible & Robust I/O
- Instant on
- Low Power & Small Package
- Support in Radiant

### Application

- Motor Control Interface
- Camera & Display Bridging
- Platform Management & Control



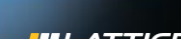
## Mach™ -NX

### Key value

- Security
- High I/O Count
- Platform Firmware Resiliency (PFR)

### Application

- NIST Compliant PFR
- Tektagon XFR Platform RoT



## MachXO5™ -NX

### Key value

- Security
- PCIe Gen2
- Large User Flash Memory

### Application

- Network Switch
- LVDS Tunneling Protocol

# FPGAs With Hardware Root Of Trust

**LATTICE**  
SEMICONDUCTOR

**Mach™ - NX**

## Key value

- Security
- High I/O Count
- Platform Firmware Resiliency (PFR)

## Application

- NIST Compliant PFR
- Tektagon XFR Platform RoT

| Features                                                                             |                                            | Mach-NX        | Other FPGAs       | MCUs & BMC        |
|--------------------------------------------------------------------------------------|--------------------------------------------|----------------|-------------------|-------------------|
|   | <b>DETECT</b><br>Firmware Authentication*  | < 5 seconds    | 15-30 seconds     | 10-20 seconds     |
|   | <b>PROTECT</b><br>Real-time SPI Monitoring | Nanoseconds    | Nanoseconds       | Not Supported     |
|  | <b>RECOVER</b><br>Firmware Recovery        | 5 Microseconds | 100s ms – minutes | 100s ms – minutes |

\*Authenticating 64MB flash image @ 33MHz

# Lattice Sentry™ Solution Stack – Cyber Resilience Pioneer



## CUSTOM DESIGN SERVICES

Server/Compute

Communications

Industrial/Embedded

Automotive



## DEMONSTRATIONS

Detection

Recovery

Protection

Attacking Firmware/  
I2C Peripherals

Fault Log



## REFERENCE DESIGNS

PFR Project  
Example Code

Quick Switch  
Schematics for SPI/QSPI

Manifest  
Generator

Processor  
Command Emulator



## SOFTWARE TOOLS



Lattice Propel™ Builder



Lattice Propel™ SDK



## IP CORES

QSPI Monitor

QSPI Streamer

Secure Enclave

I2C Monitor

ESP Mux

PLD Interface



## HARDWARE PLATFORMS

Lattice Sentry™ Demo Board for MachXO3D and Mach-NX



## Complete Solution Toolkit – CPU Agnostics

**LATTICE**  
**SupplyGuard**

# LEADING SUPPLY CHAIN PROTECTIONS

MANUFACTURING



TRANSIT



INSTALLATION



SYSTEM OPERATION



END OF LIFE



# Lattice Security Solution Value Proposition



## PRODUCT LINE



- Advanced Security Features
- Flexible I/Os and Highly Programmable
- Low Power & High Reliability

## SOLUTION STACKS



- CPU Agnostic PFR/Cyber Resilience
- Complete Solution Toolkit
- Strong Ecosystem Partner Network

## SECURITY SERVICE



- Locked Parts from Lattice to Manufacturers
- Enable Device Tracking through Supply Chain

# More Resources Available

## [Sales Resources](#)

- Sales Toolbox – Presentations by marketing team for customers
- Channel Partners – Resources for Distribution Channel

## [Lattice Insights On-demand Trainings](#)

- Control & Security Product Line Overview (1 Hr 13 Min)
- Developing with Lattice FPGA: Advanced Security Features for Configuration (25 Min)
- Security Overview: Introduction to Lattice Sentry Solution & SupplyGuard (52 Min)
- Developing with Lattice Sentry Solution (25 Mins)



## [MachXO5-NX](#)

- Reference Design
- Example Use Cases
- Documentation

## [Mach-NX](#)

- Reference Design
- Example Use Cases
- Documentation

## [MachXO4](#)

- Reference Design
- Example Use Cases
- Documentation

## [MachXO3D](#)

- Reference Design
- Example Use Cases
- Documentation



The Low Power Programmable Leader