June 1, 2021

Microchip Further Protects FPGA-based Designs with First Tool that Combats Major Industry Threat to System Security in the Field

Builds on its FPGA family's best-in-class security to block the theft of data, intellectual property and other private information from deployed systems

CHANDLER, Ariz., June 01, 2021 (GLOBE NEWSWIRE) -- Mission-critical and other high-assurance systems deployed worldwide are under rapidly evolving threats from cybercriminals who attempt to extract Critical Program Information (CPI) via the FPGAs that power them. Microchip Technology Inc. **(Nasdaq: MCHP)** today announced it has extended its FPGA family's security with the DesignShield development tool that further helps prevent this information from being extracted for malicious purposes.

"As a leader in the security space, Microchip offers a portfolio featuring the latest countermeasures for reducing the risk of cloning, intellectual property theft, reverse engineering, or the insertion of malicious Trojan Horses," said Bruce Weyer, vice president of Microchip's FPGA business unit. "Protecting CPI in deployed systems with our DesignShield tool is essential for national security and economic vibrancy. The tool advances the state of bitstream protection mechanisms and provides another defensive layer in ensuring that deployed systems behave as intended and are safe from counterfeiters and their threat to a developer's design investments and brand reputation."

The DesignShield tool was created to protect developers of aerospace, defense and other high-assurance systems from cybercriminals trying to acquire an FPGA's bitstream from the fielded system. It deters reverse-engineering of the bitstream, which can often include CPI, by obscuring its logical equivalent using a combination of logic and routing-based encryption techniques. This improves design security and integrity while reducing system corruption risks, and reduces the possibility that custom code, intellectual property, or information critical to national security is used by non-authorized agents.

Availability

The DesignShield tool is available under license as part of Microchip's Early Access Program, which enables customers to begin designing with FPGA devices and design tools ahead of broader commercial availability. The DesignShield tool is part of Microchip's Libero Development Tool Suite. For more information, contact DesignShield@microchip.com.

Microchip's FPGA Security

Based on non-volatile flash memory, Microchip's FPGAs offer inherently better security than SRAM-based alternatives that expose sensitive bitstream data on every power cycle. Microchip FPGAs also include unique integrated security features that prevent overbuilding

and cloning, protect design IP, and provide a root of trust, secure data communications and anti-tamper capabilities. The company's layered approach to security includes licensed, patented differential power analysis (DPA) protection, built-in certified security functions, built-in tamper detectors, and supply chain assurance that the FPGA is authentic. Security requires layers and not having a single wall to break through. DesignShield adds another layer that protects the authenticity, integrity, and confidentiality of a design.

Resources
High-res images available through Flickr or editorial contact (feel free to publish):

- Press image: **www.flickr.com/photos/microchiptechnology/51161706791/sizes/l/**

About Microchip Technology
Microchip Technology Inc. is a leading provider of smart, connected and secure embedded control solutions. Its easy-to-use development tools and comprehensive product portfolio enable customers to create optimal designs which reduce risk while lowering total system cost and time to market. The company's solutions serve more than 120,000 customers across the industrial, automotive, consumer, aerospace and defense, communications and computing markets. Headquartered in Chandler, Arizona, Microchip offers outstanding technical support along with dependable delivery and quality. For more information, visit the Microchip website at **www.microchip.com**.

Note: The Microchip name and logo and Microchip logo are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries. All other trademarks mentioned herein are the property of their respective companies.

Editorial Contact:
Brian Thorsen
480-792-7182
brian.thorsen@microchip.com

Reader Inquiries:
1-888-624-7435

Source: Microchip Technology Incorporated