August 30, 2023

Microchip's PolarFire® FPGA's Single-Chip Crypto Design Flow "Successfully Reviewed" By the United Kingdom Government's National Cyber Security Centre

The Review confirms strength of PolarFire FPGA's security solution

CHANDLER, Ariz., Aug. 30, 2023 (GLOBE NEWSWIRE) -- Security is now an imperative for all designs in every vertical market. Today, system architects and designers received further evidence of the security of their communications, industrial, aerospace, defense, nuclear and other systems relying on Microchip Technology's **(Nasdaq: MCHP)** PolarFire FPGAs. The United Kingdom Government's National Cyber Security Centre (NCSC) has reviewed the devices when used with the Single-Chip Crypto Design Flow against stringent device-level resiliency requirements.

"The NCSC conducts a very rigorous analysis, and the work done with Microchip on the Design Separation Methodology in the PolarFire FPGA enables the user to take advantage of improved resilience and functional isolation within the device. This reinforces Microchip's commitment to our comprehensive approach to security," said Tim Morin, technical fellow at Microchip's FPGA business unit. "This analysis provides the option for single-chip cryptography in addition to what already exists within the devices for protecting IP, securing data and protection against physical tampering—an often overlooked and very powerful threat to every electronic system, especially those at the intelligent edge."

PolarFire FPGAs implement Microchip's industry-leading security architecture to protect intellectual property, secure data and secure supply chains.

- PolarFire FPGA IP protection includes:
  - AES 256-encrypted configuration files with SHA 256-based HMAC authentication
  - Processing is protected against Differential Power Analysis (DPA) with technology licensed from Cryptography Research Incorporated (CRI)
  - Public key cryptographic cores: Elliptic Curve Cryptography (ECC) for secure distribution of keys
  - True random number generators

- PolarFire FPGA data security features include:
  - Hardened cryptographic accelerators for use in the end application
  - Pass-through CRI license enables royalty-free development of DPA-protected algorithms using techniques patented by CRI

- PolarFire FPGA supply chain security features reduce the risk of counterfeiting, re-marking and overbuilding and include:
    - Silicon biometrics, including Physically Unclonable Functions (PUFs), that allow each device to be uniquely identified and cryptographically validated

The devices are supported by Microchip's Libero® SoC Design Suite available to license, including no-charge versions, from Microchip's Purchasing and Client Services website at **www.microchipdirect.com.** PolarFire FPGA and SoC development kits and hardware are also available on the purchasing and client services website.

About the PolarFire Family

Microchip's **PolarFire** devices lead their product category in delivering twice the power efficiency, military-grade security and the industry's highest reliability, which the company will extend with the PolarFire 2 FPGA roadmap as Microchip continues to increase compute capability in ever-smaller and less costly industrial, IoT and other edge-compute products. With their real-time, Linux®-capable RISC-V-based microprocessor subsystem, **PolarFire SoC** devices are the only SoCs on the market that create new configurable processing capabilities through hardened RISC-V core complexes in a fast FPGA fabric. Ideally positioned to create custom compute inside an FPGA fabric, this family of FPGAs and SoCs has played a major role in fueling the fast-growing market for systems that move computer workloads to the power-sensitive intelligent edge. Developers can begin designing with Microchip's PolarFire family using the **software tools**, which are available on the company's website. All first-generation PolarFire devices are in full production.

Resources

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

- Application image: **www.flickr.com/photos/microchiptechnology/53137375615/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 125,000 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, the Microchip logo and PolarFire are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries. Libero is a registered trademark of Microchip Technology Incorporated in the U.S.A. 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 Inc.