Security Partner

Partner Use Case

Securing FPGA-based industrial platforms

NovTech uses OPTIGA™ TRUST P SLJ 52ACA, a programmable security chip, in their Field Programmable Gate Array (FPGA)-based industrial platform, NetLeap™. By using a hardware solution, robust security measures were easily implemented to fight a variety of software based and physical attacks against the system.

Products

OPTIGA™ TRUST P

Security Partner

Use case

Application context and security requirement

Implementing adequate security measures in industrial applications is critical. Exploited vulnerabilities can bring down control systems, put lives at risk and cause financial or reputational damages. Proactive approaches should be taken to lock down functionality of the system and protect against unintended use.

Challenge

Industrial systems that are built on State of Charge (SoC) FPGA based systems (i.e. FPGAs that have both the FPGA fabric and an embedded Central Process Unit (CPU)) can be vulnerable to a number of attacks including:

1. Reverse engineering the configuration bitstream – Transforming an encoded bitstream to a readable/editable format (FPGA side), reverse engineering the boot code (CPU side)
2. Tampering with the bitstream and fault injection – Injecting unauthorized code into the FPGA bitstream during programming (FPGA side) or tampering with the boot code (CPU side)
3. Read back – Capturing a snapshot of the FPGA configuration including look-up tables and memory state when the FPGA is in operation (FPGA side)
4. Cloning and counterfeits – Reading the bitstream by recording them during the transmission process and use the bitstream to create cheaper clones (FGPA side), cloning and counterfeits the boot code (CPU side)
5. Invasive and semi-invasive attacks – Includes techniques like physically probing the device to extract secret information by de-packaging it (both FPGA and CPU)

Implementation

To fill the security gaps discussed above, the embedded experts at NovTech chose the Infineon's OPTIGA™ Trust P SLJ 52ACA device in NetLeap™, - a multi-protocol six-port Ethernet aggregator platform. The dedicated security chip provides several layers of security including authentication, protected storage, secure updates, secure boot, memory integrity, and protection against tampering and physical attacks.

User benefits

Benefits of a programmable external hardware security solution include

› 1. Robust security that is not easily implementable with a software solution in the FPGA
› 2. Shorter design time for security related features and capabilities
› 3. Flexible and programmable solution to meet end-application requirements

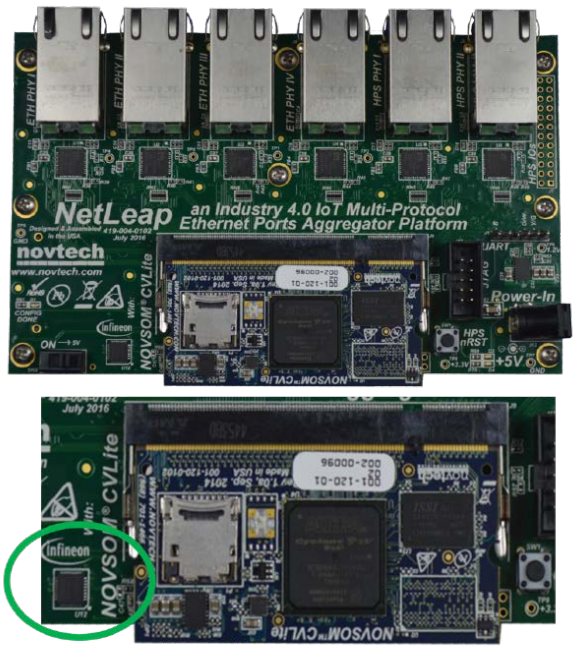
Security Partner

Solution

NovTech in partnership with Altera®, now part of Intel®, designed NetLeapTM - a multi-protocol six-port Ethernet aggregator platform. NetLeap simplifies the development of industrial platforms that require connectivity to various industrial protocols such as TSN, PROFINET®, EtherCAT®, EtherNet/IP, Ethernet Powerlink, Modbus TCP, SERCOS III and others. With six ports, NetLeap allows different protocols to reside on the same platform and can be used as a protocol bridge, a switch, or a router. This pre-production ready solution is based on Altera®, Cyclone V SoC, and FPGA with ARM® Cortex A9 cores.

Cyclone V SoC includes security features to protect designs against unauthorized copying, reverse engineering, and tampering of user configuration files. Configuration bitstreams are encrypted with 256-bit Advanced Encryption Standard (AES) and users have the option to set up volatile or non-volatile key storage. In addition, Cyclone V SoC offers tamper protection mode to prevent FPGA from being loaded with an unencrypted configuration file and the devices does not support a configuration read-back feature. By implementing encryption via the hardware-based OPTIGA™ Trust P solution, the system is more robust and free from vulnerabilities such as infected code. Another benefit is that it does not require any additional software as it is a self-contained solution.

However, all these features target the FPGA portion of the SoC. In order to protect the ARM® cores, a complex pseudo security solution can be created by forcing the ARM core to be booted by the FPGA. This requires significant engineering efforts in designing and developing HDL embedded security blocks on the FPGA side and firmware/software Intellectual Property (IP) on the boot/Operating System (OS) side. Typically, such a method would be highly inefficient and resource intensive. An efficient and robust option is to use an external chip next to the FPGA. This will offer several layers of security without adding design complexity.

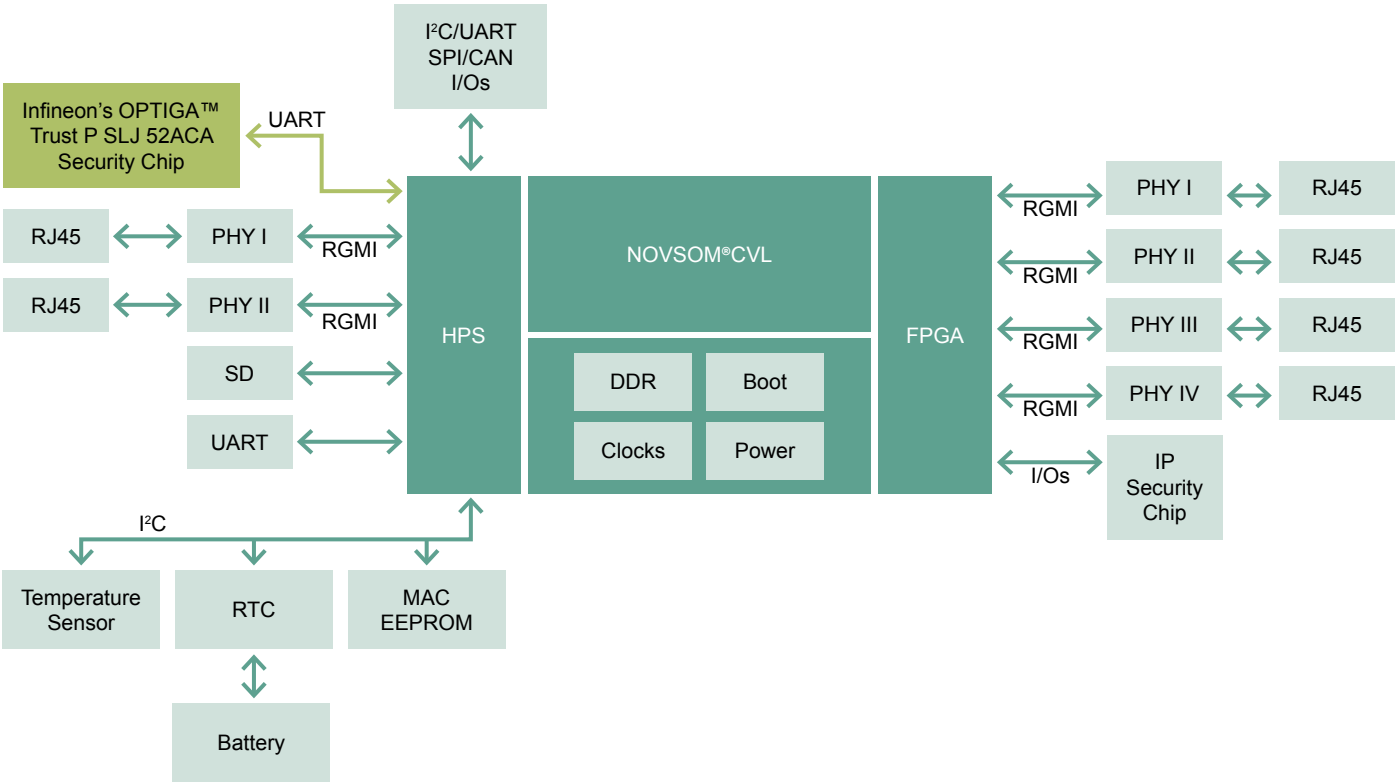


Security Partner

Solution

For a robust and feature-rich security solution, NovTech integrated Infineon's OPTIGA™ Trust P SLJ 52ACA within the NetLeap™ design. This security controller offers following benefits:

- Protected storage of credentials and device configuration information
- Secure boot of the system
- Device authentication to the network
- Secure update of device firmware and configuration
- Secure communication channel for data exchanges over the network
- Operational mode usage of crypto functions for running the secure Applications
- Protection against side channel attacks
- Logical & physical anti-tamper
- Device asymmetrical key diversification through PKI (public key infrastructure)



Security Partner

Partner

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

NovTech Inc

NovTech, Inc. was founded in 1998 by a group of engineers to enable OEMs to shorten design time by providing off-the-shelf board solutions and services. NovTech has designed and produced over 300 turn-key solutions for the aerospace, automotive, consumer industrial, medical and home automation industries. is a design services company as designed and produced over 300 turn-key solutions for a variety of market segments. Areas of expertise include:

1. Designing embedded systems based on 8-bit microcontrollers to 32-bit ARM and x86 processors
2. Implementing end-device security in SoC platforms
3. High-speed memory interfaces
4. PCB design and optimizing power consumption
5. Designing-production ready systems including all aspects of electrical and mechanical design

NovTech Inc's contribution to the Infineon Security Partner Network

NovTech can play a pivotal role in the ISPN through

1. Supplier of off-the-shelf boards and reference designs that incorporate Infineon security solutions for designs based on SoC FPGAs or ARM Cortex™ A microprocessors. If needed, boards can be customized for specific requirements.
2. Participant in Infineon events to promote awareness on security and play an "expert" role in a variety of customer settings including seminars, trainings, panel discussions, etc. Topics can range from "fundamentals of security" to "how to build robust security for end devices".

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 10 / 2016

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).