Preventing unwanted attention

A reference design to protect fpga based systems uses a simple challenge and response system. By Graham Pitcher.

The fpga has been embraced with enthusiasm by embedded systems designers. Through its programmability, the device lends itself to a number of roles. At one end of the scale, it can act as a level translator, providing an interface between otherwise incompatible devices. It can act as a companion chip to a central processor or microcontroller and it can be the heart of the system in its own right. Meanwhile, fpgas can act as prototyping platforms for devices such as asics.

As developers look to integrate more functionality into their products, fpgas are displacing dsp's and microcontrollers, particularly in the consumer and automotive sectors. Low cost fpgas are thought to be used in 25% of these applications.

While fpgas have grown in popularity, their security hasn’t always kept up. Not all fpgas use the same approach and that means some are inherently safer than other versions because security is included in their approach. Nevertheless, all engineers should be paying attention to the security of their design in order to prevent it from being pirated by a number of approaches, including reverse engineering.

Perhaps the fpga which is most open to abuse is the sram based devices. With this fpga, the configuration bitstream needs to be loaded from an external memory each time the device is switched on. Because the bitstream essentially travels across an unprotected pcb trace it is possible to intercept and interpret the information, allowing another person to access the IP.

Companies can also be affected by ‘over manufacturing’, where contract manufacturers, for example, might program more fpgas than are needed and then sell them on to competitors.

It is possible to protect the data being seen by unauthorised eyes. One approach is to use some form of encryption algorithm and security keys. But there is a view that, even though such an approach will protect the design against copyright theft, it’s often too expensive for consumer applications.

Here’s a feeling for the extent of the problem. Maxim says device manufacturers lose ‘billions of dollars’ a year to piracy and quotes a 2010 report from the Brand Protection Alliance. In the report, the Alliance cites customs and Interpol estimates the global trade in counterfeit goods of all types is now worth more than $500 billion a year and represents more than 5% of all world trade.

According to Maxim, electronics companies will have invested too much in product development costs to leave their fpga based design unprotected. Using a reference design based on its 1-Wire secure memories, Maxim says fpga IP can be protected from the unwanted attention of counterfeiters for less than $1.

The reference design, which is intended for use with Xilinx’ Spartan-6 fpgas, comprises free software – available from Maxim or Xilinx – and the DS28E01-100 from Maxim’s 1-Wire secure memory portfolio.

Operating over a single pin, the built in challenge and response SHA-1 authentication scheme in the DS28E01-100 prevents unauthorised product builds and safeguards fpga IP. The reference design also allows manufacturers to turn on fee based software controlled feature upgrades remotely without physically altering the installed hardware.

“Maxim’s security system provides best in class protection for licensing control and feature set upgrades, said Prem Nayar, the company’s business manager for secure information and authentication products. “If the DS28E01-100 and the fpga do not ‘recognise’ each other, the fpga design is effectively disabled.”

In order for the security system to work correctly, the designer must select an 8 byte secret key and load this into the fpga’s firmware.

---

**Fig 1: 1-Wire security reference design**

<table>
<thead>
<tr>
<th>DS28E01 – 100 secure memory</th>
<th>User design</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Wire</td>
<td>Bitt secure core</td>
</tr>
<tr>
<td>GND</td>
<td>Test Pass</td>
</tr>
<tr>
<td>SIO</td>
<td>IFF test Enable</td>
</tr>
</tbody>
</table>

configuration memory

---

www.newelectronics.co.uk
An 8-byte key must also be programmed into the 1-Wire memory. When power is applied, the FPGA configures and will perform a challenge and response authentication — identification friend or foe (IFF) process.

Firstly, the FPGA generates a random number and sends it to the 1-Wire memory as a challenge. The secure memory then computes a message authorisation code, or MAC, based on a combination of its secret key, the challenge, its unique identification number and other fixed data. Meanwhile, the FPGA will compute the expected response, based on the same data used in the first process. The two MAC values are then compared and if they match, the FPGA will proceed into normal operation. If they don’t, the FPGA will then take whatever actions have been decided by the designer. Maxim’s reference core seamlessly overlays on the Spartan-6 device; uses less than 5% of the logic cell resources and eases the loading of secret keys into the FPGA.

The algorithm used by the 1-Wire memory and by the host FPGA is SHA-1, which has been developed by the US National Institute of Standards and Technology (NIST). According to Maxim, distinctive characteristics of the SHA-1 algorithm include its irreversibility, its collision resistance and its high avalanche effect. The company says it is ‘computationally infeasible’ to determine the input corresponding to a MAC and that is is ‘impractical’ to find more than one input message that produces a given MAC. Meanwhile, the high avalanche effect means that any change in input will produce a ‘significant change’ in the MAC computed.

“With the use of a Maxim 1-Wire secure memory device, Xilinx customers can easily add a level of design security to their products,” said Jim Burnham, a platform marketing manager for Xilinx’ Zynq, Virtex, Spartan and CPLD development boards and kits. “While targeting the Xilinx Spartan-6 families today, this could also be used with Artix-7, Kintex-7, Virtex-7 and the Zynq-7000 families,” he added.

But it’s not just Xilinx which has tested this method, Altera has also investigated the approach. In a white paper, Altera says ‘This FPGA design security IFF solution protects Altera FPGA designs from being cloned, even if the configuration data bit stream is captured. The user design remains disabled until the hash algorithm computation in both the FPGA and the secure memory match. This design security solution protects FPGA designer’s IP.’

Xilinx adds ‘The system’s security is fundamentally based on the secrecy of the secret key and loading of the key in a secure environment. The simple interface to programming and authentication provided makes this copy protection scheme very easy to implement.’

The reference design requires free security software from Avnet, a DS28E01-100 memory device and one of three evaluation platforms: the Spartan-6 LX75T development kit; the Spartan-6 LX9 MicroBoard or the Spartan-6 LX16 evaluation kit. With the latter two boards, users will need the DS28E10-100 plug in module.