Architecture Brief

Shared Memory Protection in Altera SoCs

Introduction

Memory protection is often associated with more advanced processors. The feature prevents errant or illegal processor transactions from reading or corrupting other memory regions. To protect shared resources in SoC FPGAs, Altera extends memory protection to elements in the FPGA that generate memory traffic.

This Architecture Brief outlines the protection of shared memory systems and the benefits of incorporating ARM TrustZone® protection technology.

Key aspects of this paper are highlighted in an on-line video, "System Reliability: Memory Protection", which can be found at www.altera.com/socarchitecture under the "Reliability and Flexibility" tab.

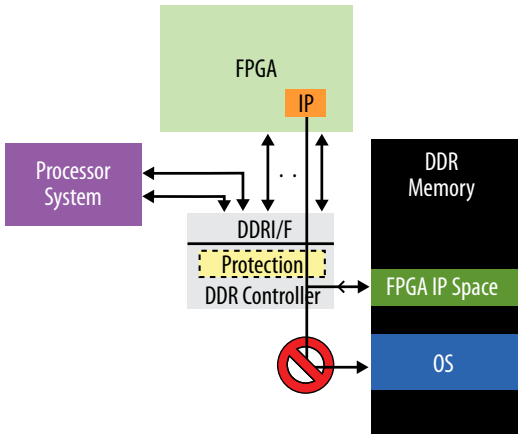
Memory Protection for Shared Memory

Memory protection is a feature often associated with more advanced processors. Whether it is called a memory management unit (MMU) or memory protection unit (MPU), it prevents errant or illegal processor transactions from reading or corrupting other memory regions. In the Cortex-A9 processor, ARM extends this protection concept with TrustZone® technology, which provides a system-wide approach for security-sensitive systems.

Some SoC FPGAs extend memory protection to the FPGA. This is needed as the processor and FPGA can share a single external DDR memory interface in order to save cost, reduce board space, or save power. What if the custom FPGA logic accidentally overwrites a section of memory belonging to the processor's data, application code, or operating system (OS) kernel? This may cause a system fault or vector the processor in the wrong direction.

To prevent this from happening, specific memory regions may be dedicated to an OS or embedded software applications while other memory regions may be dedicated to FPGA-based functions, as shown in ***Figure 1*** (below). Via memory protection, the FPGA-based functions are prevented from corrupting the OS or embedded software regions.

Figure 1: Example DDR Memory Protection Where Processors and FPGA Share a Common Memory



TrustZone provides one level of memory protection, essentially one secure boundary that shelters one memory region from all other non-secure memory access. Both the Altera SoC FPGAs and those from Vendor B support ARM's TrustZone® security features. However, TrustZone alone cannot solve the problems that arise with multiple operating systems or multiple memory masters, each of which needs unique protection or specific access to shared regions of the memory map. ***Table 1*** summarizes the memory protection for FPGA accesses to external memory.

Table 1: Memory Protection for FPGA Accesses to External Memory

Function/Feature	Altera SoC FPGA	Vendor B
TrustZone Security	Yes	Yes
TrustZone Region Size Granularity	1 MB boundary	64 MB boundary
Memory Protection	20 user-definable protection rules. Each rule defines • TrustZone® • Address range • Master ID range • Port range (mask) • Inclusive/exclusive	1 protected memory region • TrustZone®

The Altera SoC FPGA protects regions with much finer granularity, down to 1 MB. Furthermore, the Altera SoC FPGA supports 20 user-definable protection rules for a specific region. This allows finer tuning and more precise control, making it possible, for example, to prevent FPGA masters from accessing undesired regions

Conclusion

Dedicating specific regions of a memory to the OS and embedded software applications ensures that sections cannot be over-written in error, adversely affecting the processor OS, data or application code. Altera SoCs also have fine granularity TrustZone® security to define the range of memory protection.

Want to Dig Deeper?

For more details on the memory protection settings in Altera SoC FPGAs, see Chapter 11 of the Cyclone V SoC HPS Handbook or Chapter 11 of the Arria V SoC HPS Handbook.

Altera Corporation
101 Innovation Drive
San Jose, CA 95134
USA
www.altera.com

Altera European Headquarters
Holmers Farm Way
High Wycombe
Buckinghamshire
HP12 4XF
United Kingdom
Telephone: (44) 1494 602000

Altera Japan Ltd.
Shinjuku i-Land Tower 32F
6-5-1, Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-1332
Japan
Telephone: (81) 3 3340 9480
www.altera.co.jp

Altera International Ltd.
Unit 11- 18, 9/F
Millennium City 1, Tower 1
388 Kwun Tong Road
Kwun Tong
Kowloon, Hong Kong
Telephone: (852) 2 945 7000
www.altera.com.cn

SS-01240