INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 3, Issue 1 OCT 2014

HIGH PERFORMANCE REALIZATION OF MULTI-THREAD PROCESSING USING RTOS FOR COMMUNICATION SYSTEM

[1]K.Ramya,
PG Scholar in VLSI System design,
[2]K.Hymavathi,
M.Tech, Assoc. Professor, ECE Department,
[1]ramya474@gmail.com,
[2]hymasreeja@gmail.com,
[1, 2]Swami RamanandaTirtha Institute of Science and Technology, Nalgonda.

ABSTRACT:

The present day FPGA (Field Programmable GateArray) technology is capable to design high performance embedded systems based on its soft core (MicroBlaze) and hardcore (PowerPC) processors, embedded memories and other IPcores. Embedded system design demands use of limited hardwareresources with as minimum power as possible while providing
higher throughput. One way to decrease the complexity ofapplication is to use a thread-oriented design where a process isdivided into a number of manageable pieces known as threads.Each thread is responsible for some part of the application, thusproviding multitasking. Further, for real-time task execution weneed to have an efficient RTOS (Real Time Operating System)infrastructure on FPGA. Deciding a particular scheduling algorithm for thread execution requires the knowledge of resourceutilization for the specific scheduling policy. Hence, a properexploration of the various threads scheduling algorithms in termsof resource utilization, for a given embedded platform is of muchimportance.The incorporation of XILKERNEL RTOS in FPGA is a latestfacility. Though there exists a few research work on analyzingthe resource requirement in multitasking scenario for a givenembedded RTOS environment, our work on resource estimationfor the various task scheduling policies using XILKERNEL is
first of its kind. Implementation of real-time scheduling algorithmlike RMS on XILKERNEL has also been endeavored, using OSvirtualization, since it is not directly supported by the kernel ofXILKERNEL.

*Key words:*FPGA; Micro Blaze; RTOS; XILKERNEL; Thread

I. INTRODUCTION

Reconfigurable System like FPGA platform has the potential to provide the performance benefits of ASICs and the flexibility of processors. An FPGA is a collection of programmable gates embedded in a flexible interconnect network that can contain hard or soft microprocessors. FPGAs combine the programmability of processors with the performance of custom hardware. As FPGAs can provide a useful balance between performance and flexibility, they become the primary source of computation in many critical embedded systems.

FPGA based embedded system have

become a platform for the implementation of cryptographic algorithms, which needs large number of bit-level operations, and that can be done efficiently on FPGA. The merit of our paper lies in the implementation of cryptographic algorithm utilizing threads, run by an RTOS on FPGA systems, which is quite challenging in this reconfigurable architecture domain. The usage of RTOS is advantageous in many respects, as RTOS is an efficient tool to optimize the software runtime as the code complexity grows, by distributing the tasks into multiple threads. Better and safer synchronization and resource management are also major advantages of an RTOS. As an RTOS, we have chosen Xilkernel and TEA as our cryptographic algorithm to be implemented, which is quite popular.

Our contribution in this paper can be briefed as follows

- Establishing reliable communication between multiple FPGA devices is an essential component for developing complex real time systems used for applications like real time data acquisition and processing.
- Our paper proposes the major issue that two threads running separately on each board can communicate with each other via RS232 communication link.
- The algorithm is implemented in hardware by introducing the concept of thread execution by an RTOS and its hardware utilization proves that our implementation is efficient.

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

II. Literature Survey:

A. Embedded system &RTOS

Technologies that are used for implementing embedded systems are general-purpose microprocessors, micro-controllers,custom ASIC (Application-Specific Integrated Circuit) processor and FPGA. In FPGA based embedded system design, somedefinite process steps are performed for achieving the designgoal. Those steps include hardware synthesis, necessary library generation for software application and initializing ofinstruction memory for processor.It's not necessary that every embedded system or FPGAbased embedded design has to have an OS. The system withless complex architecture and with simple application doesnot require any OS/RTOS Without an RTOS, one can makea system to perform following Background/Foreground model. RTOS is an operating system that supports real-timeapplications by providing logically correct result within a stipulated deadline. RTOS environments are broadly classified intothree types namely, Hard, Firm and Soft . The architectureof an RTOS as shown in Fig. 1 is dependent on the complexityof its deployment. The core of an RTOS is known as the kernel.The kernel also contains a scheduler for executing threads inaccordance with a scheduling mechanism. A thread is like afunction that has its own stack, and a Thread Control Block(TCB) . An API is provided to allow access to the kernelfor the creation of threads. In FPGA based embedded

systemthere are many third party RTOSes such as Vxworks, Nucleus,eCOS, Threadx.

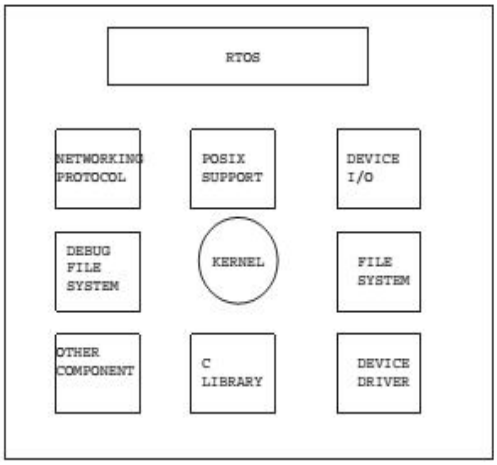


Fig. 1. Architecture of an RTOS

B. Xilkernel

XILKERNEL is a small, robust, and modular kernel,with the features of an operating system. It is modular inthe sense that only the functions needed in the target systemneeds to be included, which helps keeping the size of theoperating system small. It also provides synchronization andcommunication primitives for implementing co-operative taskexecution for solving a problem. XILKERNEL supports twotypes of scheduling one is round robin with predefined timeslice, and strict priority scheduling, where each thread canbe assigned with a particular priority value.

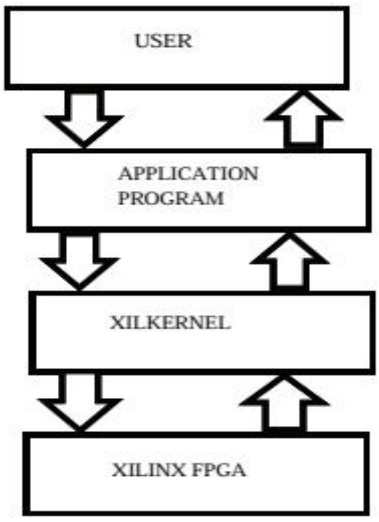


Fig. 2. Architecture of FPGA based embedded system with XILKERNEL

Modern cryptography:

The modern field of cryptography can be divided into several areas of study.

Symmetric-key cryptography:

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher. Block ciphers can be used as stream ciphers.

Public-key cryptography:

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well.

Public-key cryptography can also be used for implementing digital signature schemes. A

digital signature is reminiscent of an ordinary signature; they both have the characteristic of being easy for a user to produce, but difficult for anyone else to forge.

TinyEncryptionAlgorithm:

In cryptography, the Tiny Encryption Algorithm (TEA) is a block cipher notable for its simplicity of description and implementation, typically a few lines of code. It was designed by David Wheeler and Roger Needham of the Cambridge Computer Laboratory; it was first presented at the Fast Software Encryption workshop in Leuven in 1994, and first published in the proceedings of that workshop. The cipher is not subject to any patents.

III. Real Time Threads Processing Usingfpga

In this work, few experiments on real-time multi-threadprocessing in FPGA have been carried out. Usually threadshave limited built-in memory. In the event, a particular threadrequires more memory for data processing, it can be assignedlocally. Fig. 3 shows a summary of the experiments that havebeen carried out.Five experiments are performed on single processor architecture, based on Spartan3e starter board with XILKERNELas RTOS and Micro Blaze as processor. The XILKERNELhas built-in access control mechanisms of Semaphore andMutexin its core-kernel for thread synchronization. The accesscontrol mechanisms i.e. enable-disable ofSemaphoreand lockunlock ofMutexare available as built-in functions within theXILKERNEL and also available externally with POSIX APIs.

In section III-A two experiments on thread synchronizationsupported by POSIX APIs are presented where each thread undertakes data processing based on locally available memories.In section III-B two experiments on thread communicationhave been described where the synchronization is supported bybuilt-in XILKERNEL functions and the threads have limitedmemory handling capability. It is necessary to appropriately

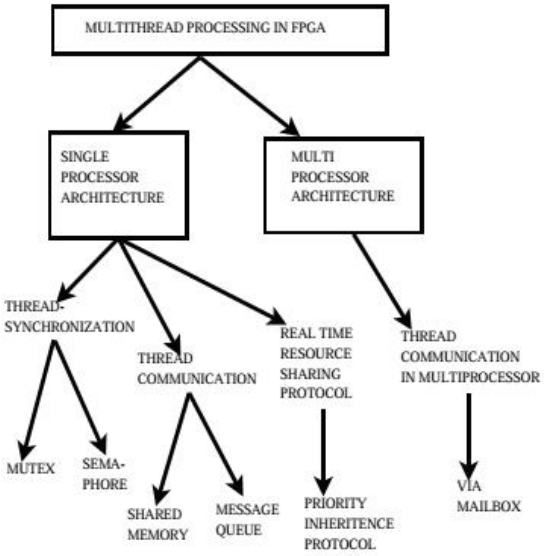


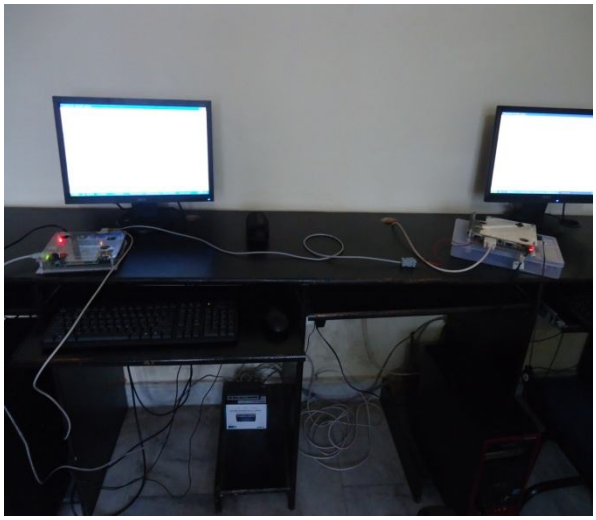
Fig. 3. Total experiments performed

IV. RESULTS:

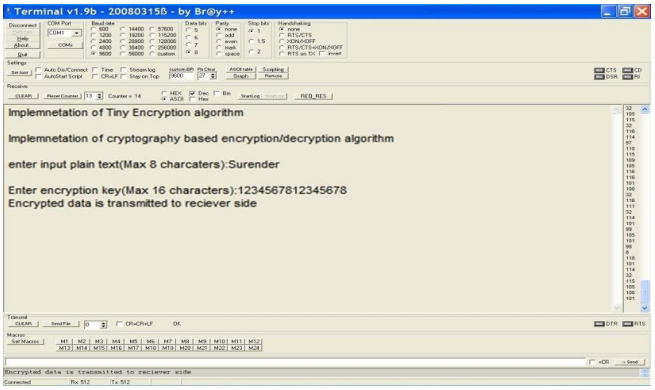
In the previous section various real-time thread processingexperiments have been described. In this section we discuss
the FPGA resources utilized by the different thread processingprocedure and the corresponding memory consumption. InEDK environment, we have.mrp&.par file which give thedetails of resource utilization of the design.

The below figures show the hardware configuration for communication between two fpgas. In this communication we require two pc's two fpgas and three rs-232 cables. RS232 (DTE to DCE cable) is used for communication between fpga and pc. RS232 (DTE to DTE cable) is used for communication between two fpga's. It is used to transfer data from one fpga to another fpga.

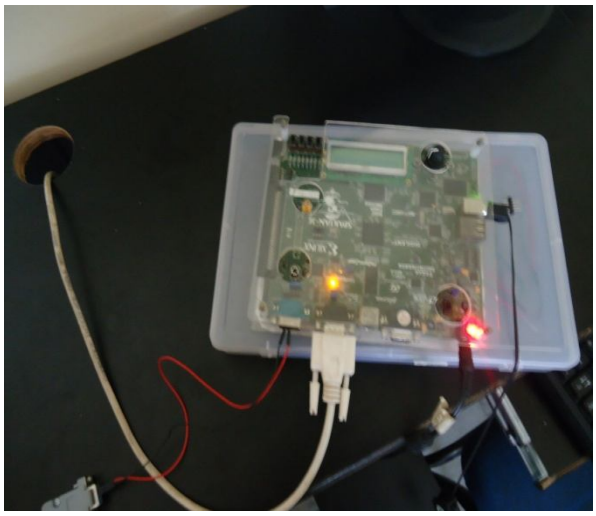
The two different cables and its connections with fpga are shown in the below figures.

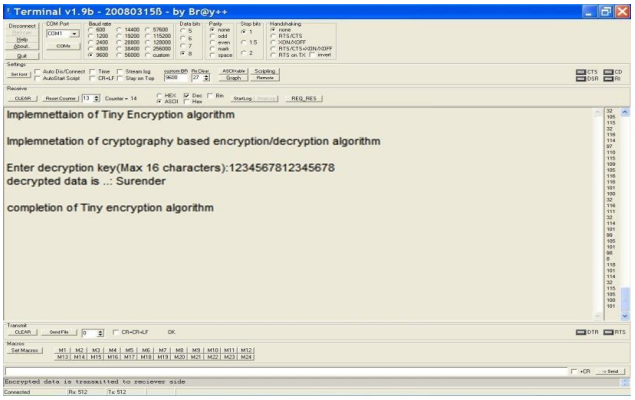


WITHOUT RTOS :
Result in Transmitter System



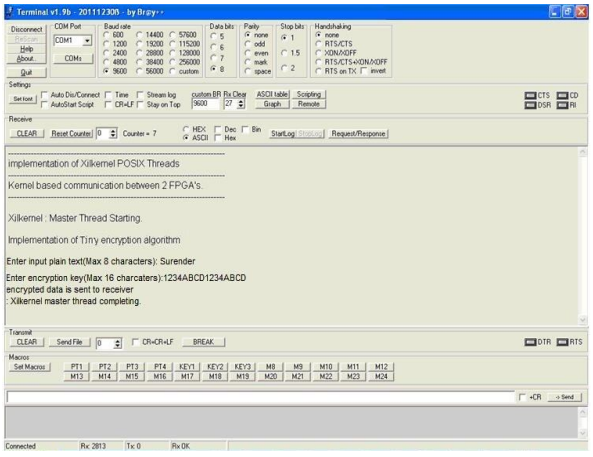
Result inReceiver System



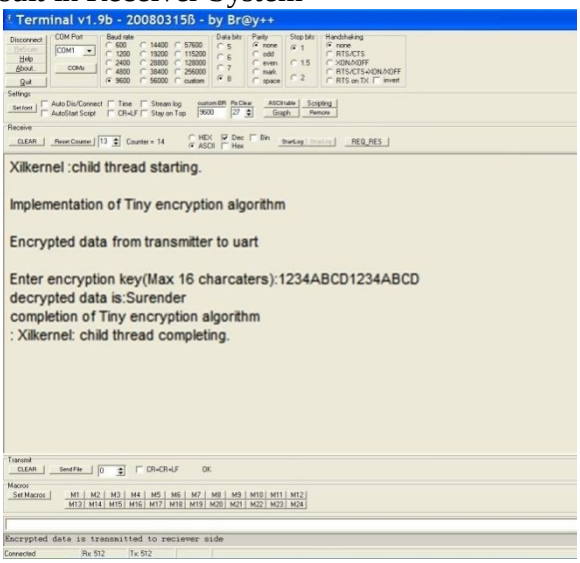


WITH RTOS:

Result in Transmitter System



Result in Receiver System



CONCLUSION:

Implementing a microblaze soft core processor on the FPGA.The verification of l communication between two FPGA's(chip to chip communication).And here the communication is done in secured manner by applying tiny encryption algorithm. This is all done on RTOS(real time operating system) environment. We can implement the same algorithm in high end FPGA boards which is having high speed as well as for more speed applications we can implement this application by using power pc type of processor. For more security for communication we can go for other encryption algorithms. Or If we increased the key bit length then it would be critical to decode the information for the third party member other than transmitter and receiver.

REFERENCES

[1] S. Sau , C. Pal and A Chakrabarti "Design and Implementation of Real Time Secured RS232 Link for Multiple FPGA Communication, Proc. Of International Conference on Communication, Computing & Security,201 I, ISBN - 978-1-4503-0464-1.

[2] C. D. Walter. August 1999. Montgomery's Multiplication Technique: How to Make It Smaller and Faster. Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, Springer. No. 1717. pp. 80-93.

[3] AMazzeo, L. Romano, G. P. Saggese and N. Mazzocca. 2003. FPGABased Implementation ofa Serial RSA Processor.Design. Proceedings of the conference on Design, Automation and Test in Europe - Volume I. ISBN:O-7695-1870-2.

[4] xilkernel_v3.00.pdf on www.xilinx.com.

[5] R.L. Rivest et al. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.Communications of the ACM.Vol. 21. pp. 120-126.

[6] Cryptography & Network Security ByBehrouzAForouzan.

[7] Montgomery Algorithm for Modular Multiplication Professor Dr. D. J. Guan ,August 25, 2003.

[8]RSA & Public Key Cryptography in FPGAs, John Fry, Martin Langhammer Altera Corporation -Europe

[9] A. Tenca, C. Koc. 1999. A Scalable Architecture for Montgomery Multiplication. Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, No. 1717, pp. 94-108.