بسم الله الرحمن الرحيم

∞∞∞

تم رفع هذه الرسالة بواسطة / سامية زكى يوسف

بقسم التوثيق الإلكتروني بمركز الشبكات وتكنولوجيا المعلومات دون أدنى مسئولية عن محتوى هذه الرسالة.

ملاحظات: لا يوجد

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer and Systems Engineering Department

Designing of a Secure AUTOSAR-based Communication Gateway

A Thesis submitted in partial fulfillment of the requirements of
Doctor of Philosophy in Electrical Engineering
(Computer and Systems Engineering)

By
Ahmed Mohamed Moro Ahmed Hamed
Master of Science in Electrical Engineering
(Computer and Systems Engineering)
Faculty of Engineering, Ain Shams University, 2016

Supervised by
Prof. Dr. Ashraf Mohamed Mohamed Elfarghly Salem
Prof. Dr. Mohamed Watheq Ali Kamel El-Kharashi
Dr. Mona Mohamed Hassan Safar

Cairo, 2022

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer and Systems Engineering Department

Designing of a Secure AUTOSAR-based Communication Gateway

by

Ahmed Mohamed Moro Ahmed Hamed

Master of Science in Electrical Engineering
(Computer and Systems Engineering)
Faculty of Engineering, Ain Shams University, 2016

Examiners' Committee

Name and affiliation	**Signature**
Prof. Dr. Amr Galaleldin Ahmed Wassal Prof. at Computer Engineering Department Faculty of Engineering, Cairo University.	.....
Prof. Dr. Ayman Mohamed Mohamed Hassan Wahba Prof. at Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University.	.....
Prof. Dr. Ashraf Mohamed Mohamed Elfarghly Salem Prof. at Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University.	.....
Prof. Dr. Mohamed Watheq Ali Kamel El-Kharashi Prof. at Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University.	.....

Date: 3 July 2022

Statement

This thesis is submitted as a partial fulfillment of Doctor of Philosophy in Electrical Engineering, Faculty of Engineering, Ain shams University. The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Ahmed Mohamed Moro Ahmed Hamed

Signature

.....

Date: 3 July 2022

Researcher Data

Name: Ahmed Mohamed Moro Ahmed Hamed
Date of Birth: 13/08/1989
Place of Birth: Cairo, Egypt
Last academic degree: Master of Science
Field of specialization: Electrical Engineering
University issued the degree: Ain Shams University
Date of issued degree: 2016
Current job: Engineering Manager at Siemens Digital Industries Software, Integrated Electrical Systems Segment

Abstract

Today's automotive Software (SW) applications exhibit high communication within Electronic Control Units (ECUs) and between networked vehicle nodes. Here comes the role of the AUTomotive Open System ARchitecture (AUTOSAR) Communication (COM) module that defines a standard for the common SW communication interfaces and behaviour for internal communication (i.e., communication within an ECU) and external communication (i.e., communication between networked vehicle nodes), which is independent of the communication protocol used.

Due to the improvement of exchanged information between ECUs, the need to deal with other types of protocols, which are able to transfer long Protocol Data Units (PDUs) and signals, has been aroused and it became possible to transfer other types of information (e.g., images and maps).

The idea of this research is to design a secure AUTOSAR-based COM Application-Specific Instruction Set Processor (ASIP) for handling long PDUs and signals by packing long transmitted signals into their corresponding PDUs and unpacking long received signals from their corresponding PDUs. This circuitry will be designed directly on Hardware (HW) instead of SW to accelerate the process of packing/unpacking long signals into/from their corresponding long PDUs. Then integrating the accelerated part on HW with the core SW of the AUTOSAR COM module and measuring the performance improvement. The exchange of the PDUs between ECUs has to be done in a secure manner by using the appropriate cryptographic algorithms to prevent hackers from gaining access to the information inside these PDUs and altering it.

The research presents the design and implementation details of four versions of AUTOSAR COM ASIP. The first version is a non-pipelined version. This version introduced two new instructions that are used to handle long signals and PDUs. It can handle (i.e., send or receive) 4 bytes of any signal in only one instruction so it can handle signals and PDUs of any arbitrary length. The second version is a non-pipelined version as well. This version supports all functionalities available in the previous version. In addition, it introduced six new instructions that are used to secure exchanging PDUs between ECUs by applying a hashing algorithm on signals contained in these PDUs.

The third version is a pipelined version. This version supports all functionalities available in the previous versions. It increases throughput of instructions supported by the previous versions using a pipelined technique. Throughput of this third version is 169x more than throughput of Controller Area Network Flexible Data-rate (CAN FD) protocol, and 100x more than throughout of FlexRay protocol. The fourth version is a pipelined

version as well. This version supports all functionalities available in the previous version in an enhanced fashion. Throughput of this third fourth version is 245x to 338x more than throughput of CAN FD protocol, and 156x to 229x more than throughout of FlexRay protocol.

Summary

Today's automotive Software (SW) applications exhibit high communication within Electronic Control Units (ECUs) and between networked vehicle nodes. Here comes the role of the AUTomotive Open System ARchitecture (AUTOSAR) Communication (COM) module that defines a standard for the common SW communication interfaces and behaviour for internal communication (i.e., communication within an ECU) and external communication (i.e., communication between networked vehicle nodes), which is independent of the communication protocol used.

Due to the improvement of exchanged information between ECUs, the need to deal with other types of protocols, which are able to transfer long Protocol Data Units (PDUs) and signals, has been aroused and it became possible to transfer other types of information (e.g., images and maps).

The idea of this research is to design a secure AUTOSAR-based COM Application-Specific Instruction Set Processor (ASIP) for handling long PDUs and signals by packing long transmitted signals into their corresponding PDUs and unpacking long received signals from their corresponding PDUs. This circuitry will be designed directly on Hardware (HW) instead of SW to accelerate the process of packing/unpacking long signals into/from their corresponding long PDUs. Then integrating the accelerated part on HW with the core SW of the AUTOSAR COM module and measuring the performance improvement. The exchange of the PDUs between ECUs has to be done in a secure manner by using the appropriate cryptographic algorithms to prevent hackers from gaining access to the information inside these PDUs and altering it.

We implemented four versions of AUTOSAR COM ASIP. The first version is a non-pipelined version. This version supports long signals and PDUs. Throughput of this version, in transmitting and receiving frames with different lengths, is 99x more than throughput of Controller Area Network Flexible Data-rate (CAN FD) protocol, and 55x more than throughout of FlexRay protocol.

The second version is a non-pipelined version as well. This version supports all functionalities available in the previous version. In addition, it supports securing exchanging PDUs between ECUs by applying a hashing algorithm on signals contained in these PDUs. Throughput of this second version is 75x more than throughput of CAN FD protocol, and 42x more than throughout of FlexRay protocol.

The third version is a pipelined version. This version supports all functionalities available in the previous versions. It increases throughput of instructions supported by the previous versions using a pipelined technique. Throughput of this third version is 169x

more than throughput of CAN FD protocol, and 100x more than throughout of FlexRay protocol.

The fourth version is a pipelined version as well. This version supports all functionalities available in the previous version in an enhanced fashion. Throughput of this third fourth version is 245x to 338x more than throughput of CAN FD protocol, and 156x to 229x more than throughout of FlexRay protocol.

This speedup gained by the third and fourth versions gives a room for the original equipment manufacturers (OEMs) and Tier1 suppliers to extend their automotive applications and increase the amount of the exchanged information by these applications without affecting the performance.

The thesis is divided into nine chapters as listed below:

Chapter 1

This chapter introduces the thesis by presenting the research motivations, objectives, challenges, methodology (i.e., the SW tools, the HW devices, and the HW description language that we used during design, testing, and implementation of AUTOSAR COM ASIPs), and thesis organization.

Chapter 2

This chapter gives a brief introduction about the initial version of COM ASIP (i.e., COM ASIP V1) that is considered a base for the next versions of COM ASIPs. COM ASIP V1 introduced two instructions to handle transmission and reception of signals, with maximum length of 32 bits per each signal, inside PDUs with maximum length of 8 bytes.

Chapter 3

This chapter explains implementation details of the first version (i.e., COM ASIP V2) of AUTOSAR COM ASIP that is non-pipelined. COM ASIP V2 introduced two new instructions that are used to handle long signals and PDUs. COM ASIP V2 can handle (i.e., send or receive) 4 bytes of any signal in only one instruction so it can handle signals and PDUs of any arbitrary length.

Chapter 4

This chapter explains details of a highly secure hashing algorithm, named Galois/-Counter Mode of Operation (GCM). This algorithm will be used by the second version (i.e., COM ASIP V3) of secure AUTOSAR COM ASIP that is non-pipelined.

Chapter 5

This chapter explains implementation details of the second version (i.e., COM ASIP V3) of secure AUTOSAR COM ASIP that is non-pipelined. COM ASIP V3 introduced six new instructions that are used to secure exchanging PDUs between ECUs by applying a hashing algorithm on signals contained in these PDUs.

Chapter 6

This chapter explains implementation details of the third version (i.e., COM ASIP V4) of secure AUTOSAR COM ASIP that is pipelined. This version of COM ASIP increases throughput of instructions supported by the previous non-pipelined versions using a pipelined technique be entering a new instruction in pipeline each five clock cycles.

Chapter 7

This chapter explains implementation details of the fourth version (i.e., COM ASIP V5) of secure AUTOSAR COM ASIP that is pipelined. This version of COM ASIP increases throughput of instructions supported by the previous non-pipelined versions using a pipelined technique be entering a new instruction in pipeline each two clock cycles.

Chapter 8

This chapter discusses the experimental results for the first and second versions of AUTOSAR COM ASIP that are non-pipelined and the third and fourth versions of the AUTOSAR COM ASIP that are pipelined. This chapter shows synthesis results of all versions of our COM ASIP and compares throughput of these versions against each other and against different communication buses.

Chapter 9

This chapter ends the thesis by conclusions and the expected future work. This chapter lists our contribution by showing the four versions of COM ASIP (i.e., COM ASIP V2, COM ASIP V3, COM ASIP V4, and COM ASIP V5) that we implemented on top of our initial version of COM ASIP (i.e., COM ASIP V1). It also summarizes the differences and evolution from COM ASIP V1 to COM ASIP V5.

Keywords:

Authentication, Encryption, Automotive, Security, Communication, Signal