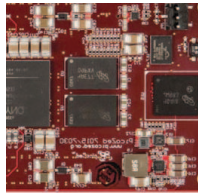




IDEC newsletter

Vol. 229 July 2016

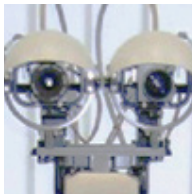


기술동향1

네트워크 보안, QoS(Quality of Service), DNA 분석에 응용하는
고성능 문자열 매칭 엔진의 연구동향

기술동향2

데이터 보안 위협에 대응하라
테스트 로직을 통한 하드웨어 공격 및 보안



기획칼럼1

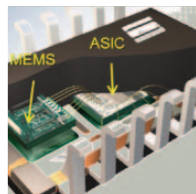
보드 구매, 어렵지 않아요!
국내외 SoC, 임베디드 보드 리뷰 - Altera 편

기획칼럼2

인공지능 특집 (1)
인공두뇌: 뇌인지과학으로부터 지능정보시스템으로

특집기사

미래 자동차 산업의 핵심이 될 SoC
스마트카/커넥티드카용 시스템반도체(SoC)와
기능안전 측면의 기술전망



반도체설계교육센터
IC DESIGN EDUCATION CENTER

2016년 MPW 모집안내 (7월)

○ 모집일정 : 06.20(월)~07.04(월)

- 모집공정 및 회차 : MS350-1602회(정규) 매그나칩/SK하이닉스 350nm 공정
- 2016년 MPW 설계팀 모집 완료 : 7월 모집을 끝으로 올해 MPW 모집은 종료됨.

○ 참가대상 : IDEC 참여대학(Working Group)

○ 2017년 MPW 진행 일정 : 2016년 12월말에 결정될 예정임.

MPW 진행일정 및 공정 지원내역

공정	회차구분 (공정_년도순서)	우선모집 (마감일)	정규모집 (마감일)	참여팀수/ 제작칩수	DB마감 (Tape-out)	Die-out	비고
삼성 65nm	S65-1601		2016.02.01	39 / 40	2016.08.01	2017.02.14	설계중
	S65-1602		2016.04.18	32 / 40	2016.10.17	2017.05.02	설계중 (추가 모집 중)
	S65-1603	2016.04.18	2016.06.20	40 / 40	2017.01.16	2017.07.31	모집완료 설계대기 중
MS 0.18um	MS180-1601		2016.01.18	29 / 25	2016.03.21	2016.08.22	칩제작 중
	MS180-1602		2016.02.01	29 / 25	2016.05.16	2016.10.17	칩제작 중
	MS180-1603		2016.03.07	26 / 25	2016.07.18	2016.12.19	칩제작 중
	MS180-1604	2016.02.01	2016.04.04	26 / 25	2016.09.19	2017.02.20	설계 중
	MS180-1605	2016.04.04	2016.06.07	32 / 25	2016.12.05	2017.05.08	설계 중
MS 0.35um	MS350-1601		2016.02.01	20 / 20	2016.06.13	2016.10.04	칩제작 중
	MS350-1602	2016.05.02	2016.07.04	2 / 20	2017.01.16	2017.05.08	모집 중

- 일정은 사정에 따라 다소 변경될 수 있음.
- 회차 표기 방법 변경 : 공정코드-년도 모집순서 (예시) 삼성 65nm 2016년 1회차 : S65-1601)
- 모집기간 : 모집 마감일로 부터 2주 전부터 접수
- Package 제작은 Die out 이후 1개월 소요됨.
- 내용 기준 : 2016.07.01(금)



문의처

이의숙 | yslee@idec.or.kr, 042-350-4428
IDEC 홈페이지 | http://idec.or.kr

강좌 일정

센터명	강의일자	강의 제목	분류
본센터	7월 4-6일	고성능 TI SAR ADC설계를 위한 이론 및 실습	설계강좌
	7월 11-13일	SystemVerilog Testbench	Tool강좌
	7월 14-15일	HDL Debugging Training (Verdi)	Tool강좌
	7월 18-20일	Design Compiler 사용법 및 활용예	Tool강좌
	7월 21-22일	Low Power Flow	Tool강좌
	7월 25-26일	DFT Compiler	Tool강좌
	7월 27-29일	PrimeTime 사용법 및 활용 예	Tool강좌
경북대	7월 4일	CMOS 이미지 센서 설계	설계강좌
	7월 7일	Mobile transceiver RFIC 설계	설계강좌
	7월 11일	아날로그 회로의 직관적 해석	설계강좌
	7월 13일	아날로그 Op-Amp 설계	설계강좌
	7월 14-15일	Zynq 및 Vivado를 이용한 RTL 및 FPGA 기본 설계 실습	설계강좌

센터명	강의일자	강의 제목	분류
경북대	7월 19-20일	PSpice를 이용한 아날로그 Front end 설계	설계강좌
	7월 25일	컴퓨터 시스템 구조 설계 및 시뮬레이션을 통한 평가 방법	설계강좌
	7월 28-29일	Xilinx ISE 기반의 FPGA 동작 실습	설계강좌
광운대	7월 4-7일	지능형 웨어러블 시스템 설계	설계강좌
	7월 11-14일	스마트 모바일 AP기반 SoC구조 및 주변장치 응용	설계강좌
부산대	7월 18-22일	CMOS RF 트랜시버 회로 설계 실습	설계강좌
	7월 5-7일	CPU 설계 및 응용	설계강좌
	7월 19-21일	Verilog을 이용한 Digital System 설계	설계강좌
전남대	7월 28-30일	CMOS Analog 전자회로 설계	설계강좌
	7월 25-29일	CMOS Analog Layout 실습 (LNA, Digital Gate)	설계강좌

수강을 원하는 분은

IDEC홈페이지(www.idec.or.kr)를 방문하여 신청하시기 바랍니다.



본센터

7/4-6

강좌제목 고성능 TI SAR ADC설계를 위한 이론 및 실습

강사 홍혁기 박사(KAIST 전자정보연구원)

강좌개요

본 강좌는 Nyquist data converter를 중심으로 동작의 기본 원리부터 시작하여 최신 설계 동향까지 다루게 된다. 먼저 ADC/DAC의 동작원리와 성능척도에 대해 소개하고, SAR ADC와 Time-interleaving 기술에서 성능저하를 일으키는 요인에 대해 고찰하여 실제 설계에서 고민해야 할 점들을 이야기한다.

수강대상 데이터 변환기 설계를 목적으로 하는 대학원생, 직장인

강의수준 중급 **강의형태** 이론+실습

사전지식·선수과목 학부 전자회로, 디지털회로 지식 필수

7/11-13

강좌제목 SystemVerilog Testbench

강사 임정환 이사(Synopsys Korea)

강좌개요

16x16 switch DUT를 검증하기 위하여 단계별로 SystemVerilog로 Testbench를 작성하는 과정을 통해 SystemVerilog 문법, Testbench 구조, Coverage driven random verification에 대한 지식을 익힌다.

수강대상 SystemVerilog를 사용하여 Testbench를 작성하고자 하는 Design Engineer 또는 Verification engineer

강의수준 중급 **강의형태** 이론+실습

사전지식·선수과목

-Unix/Linux 환경 기본

-Verilog / VHDL Design/Simulation 경험

7/14-15

강좌제목 HDL Debugging Training(Verdi)

강사 전병웅 차장(Synopsys Korea)

강좌개요

- Verdi3는 Behavioral-level의 Post-debugging solution으로써 debugging methodology에 수학적 기술을 더해 새로운 temporal visualization, symbolic design exploration, auto bug tracing 등 다양한 기능을 제공 함으로써, 좀더 빠른 HDL design 설계를 도와줍니다.
- 산업체에서 가장 많이 사용되어지는 Simulation event 정보를 담은 FSDB(Fast Signal DataBase)에 대해서 교육을 진행 합니다.

수강대상 RTL/GATE Design(Logic) Verification Engineer

강의수준 초급 **강의형태** 이론+실습

사전지식·선수과목

- HDL(Verilog) coding Skills: Verilog, VHDL, SystemVerilog

- Standard Logic Simulators: VCS(Synopsys), IUS(Cadence), MTI(Mentor)

7/18-20

강좌제목 Design Compiler 사용법 및 활용예

강사 김진호 부장(Synopsys Korea)

강좌개요

- Synthesize RTL to gates using top-down DC-Ultra techniques

- Constrain a complex design for area and timing

- Generate output required by physical design tools

수강대상 SOC digital designers

강의수준 초급 **강의형태** 이론+실습

사전지식·선수과목 Basic digital logic concepts and Unix based text editor

7/21-22

강좌제목 Low Power Flow

강사 김진호 부장(Synopsys Korea)

강좌개요

- Create UPF to capture the expected power intent

- Run power aware static checks on the design

- Synthesize RTL and insert scan chains for the required power intent

- Perform equivalence checking for functionality with the power intent

수강대상 SOC digital designers

강의수준 초급 **강의형태** 이론+실습

사전지식·선수과목 Basic digital logic concepts and Unix based text editor

7/25-26

강좌제목 DFT Compiler

강사 김태삼 과장(Synopsys Korea)

강좌개요

In this workshop you will learn to use DFT Compiler to perform RTL and gate-level DFT rule checks, fix DFT DRC rule violations, and to insert scan using top-down and bottom-up flows. The workshop explores essential techniques to support large, multi-million gate SOC designs including the bottom-up scan insertion flow in the logical(Design Compiler) domain. Techniques learned include: performing scan insertion in a top-down flow; meeting scan requirements for number of scan chains, maximum chain length and reusing functional pins for scan testing.

수강대상

Design and Test engineers who need to identify and fix DFT violations in their RTL or gate-level designs, insert scan into multi-million gate SoCs, and export design files to ATPG and P&R tools

강의수준 중급

강의형태 이론+실습

사전지식·선수과목

Prior experience with Design Compiler, Design Vision and writing Synopsys Tcl scripts is useful, but not required.

7/27-29

강좌제목 PrimeTime 사용법 및 활용 예

강사 김태삼 과장(Synopsys Korea)

강좌개요

- In this workshop you will learn to perform Static Timing Analysis (STA) using PrimeTime by executing the appropriate high-level summary reports to initiate your analysis, customizing and interpreting detailed timing reports for debugging, and exploring and analyzing the clocks that dictate STA results.

- Within PrimeTime you will debug STA constraints that may be either incomplete or incorrect which cause invalid timing violations or result in hiding real timing violations.

수강을 원하는 분은

IDEC홈페이지(www.idec.or.kr)를 방문하여 신청하시기 바랍니다.

- You will also learn to maximize your productivity by validating inherited scripts for your design, by creating scripts using a Synopsys recommended methodology, by identifying opportunities to improve run time, and by customizing your environment for ease of running and debugging.
- The workshop includes comprehensive hands-on labs, which provide an opportunity to apply key concepts covered during the lectures.

수강대상

ASIC digital designers, or verification engineers, who will be using Prime-Time to perform Static Timing Analysis (STA) on pre- or post-layout gate level designs, and who need to validate STA constrain

강의수준 초급

강의형태 이론+실습

사전지식 · 선수과목

- Have a basic understanding of digital IC design
- Understand elements of gate level design: chip vs. block level, sequential vs. combinational logic, clock tree vs. data path, pre- vs. post- layout

문의 | KAIST IDEC 이한나 (042-350-8536, lhn1224@idec.or.kr)



경북대

7/4

강좌제목 CMOS 이미지 센서 설계

강사 천지민 교수(금오공과대학교)

강좌개요

CMOS 이미지 센서는 CCD(Charge-coupled Device) 센서와 비교되는 저전력, 저전압, 그리고 집적에 따른 효율성의 장점을 가지기 때문에 최근 많은 주목을 받고 있다. 본 강의는 이미지 센서 기본 및 관련 기술을 설명하고, CMOS 이미지 센서 이론을 중심으로 진행한다.

수강대상 전기, 전자, 정보통신 관련 전공 대학생 및 산업체

강의수준 중급 **강의형태** 이론

사전지식 · 선수과목 없음

7/7

강좌제목 Mobile transceiver RFIC 설계

강사 문현원 교수(대구대학교)

강좌개요

Mobile용 RF Transceiver 설계 요소에 대한 기본적인 지식과 설계 방법론에 대해 익히고 이를 바탕으로 CMOS 기술을 이용한 Mobile RF Transceiver용 RFIC 설계 교육 기회를 제공하고자 한다. 또한 실제 Mobile용 RF Transceiver 설계 예제를 통한 RFIC 회로 설계에 대한 응용을 확인할 수 있으며, 이를 실제 기업체나 대학연구실의 업무 현장에서 적용 가능하도록 하는 것이 주요 교육 목적이다.

수강대상 전기, 전자, 정보통신 관련 전공 대학생 및 산업체

강의수준 중급 **강의형태** 이론

사전지식 · 선수과목

- 1) Basic circuit theory
- 2) Microelectronic circuit
- 3) Basic microwave theory

7/11

강좌제목 아날로그 회로의 직관적 해석

강사 심재윤 교수(포항공과대학교)

강좌개요

기본적인 R,L,C, pole/zero 특성, 증폭기 회로, 주파수 응답 및 피드백 이론을 다양한 graphical 한 직관적 방법으로 이해한다.

수강대상 전기, 전자, 정보통신 관련 전공 대학생 및 산업체

강의수준 초급

강의형태 이론

사전지식 · 선수과목 전자회로

7/13

강좌제목 아날로그 Op-Amp 설계

강사 범진욱 교수(서강대학교)

강좌개요

CMOS 공정을 기반으로 MOS Transistor의 기본을 바탕으로 single TR 의 구성과 이의 응용회로와 differential amplifier, operational amplifier 등의 응용회로에 대하여 학습한다.

수강대상 전기, 전자, 정보통신 관련 전공 대학생 및 산업체

강의수준 중급

강의형태 이론

사전지식 · 선수과목 전자회로 I, II (학부 수준)

7/14-15

강좌제목 Zynq 및 Vivado를 이용한 RTL 및 FPGA 기본 설계 실습

강사 조재현 연구원(휴인스)

강좌개요

본 교육에서는 Zynq 7020 Target Board와 Xilinx Vivado tool을 통해 기본적인 RTL 설계와 IP 설계 및 기본 시스템 구현을 이론과 실습을 병행하여 학습한다.

수강대상 전기, 전자, 정보통신 관련 전공 대학생 및 산업체

강의수준 중급

강의형태 이론+실습

사전지식 · 선수과목 Verilog 기초, SoC 기초 이론

7/19-20

강좌제목 PSpice를 이용한 아날로그 Front end 설계

강사 김무현 대리(나인플러스 IT)

강좌개요

반도체 및 컴퓨터기술의 급격한 발달과 더불어 기술이 혁신적으로 발전하고 전기전자 관련 제품의 설계 및 제조 공정이 자동화되어 생산성 증대와 제품의 품질향상 등이 산업체의 경쟁력 제고를 위해 요구되고 있으며, 특히 제품 개발기간을 단축시키고 신뢰성을 높이기 위한 노력의 일환으로 Simulation Tool을 이용하여 실제 제작단계 이전에 회로특성을 해석해보는 과정이 중시되었다.

수강대상 전기, 전자, 정보통신 관련 전공 대학생 및 산업체

강의수준 중급

강의형태 이론+실습

사전지식 · 선수과목 전자회로, 회로이론, 반도체공학

수강을 원하는 분은

IDEC홈페이지(www.idec.or.kr)를 방문하여 신청하시기 바랍니다.

7/25

강좌제목 컴퓨터 시스템 구조 설계 및 시뮬레이션을 통한 평가 방법

강사 공준호 교수(경북대학교)

강좌개요

- 컴퓨터 시스템 구조 설계에 대한 이론
- 최신 컴퓨터 시스템 구조 설계 이슈
- 오픈소스 시뮬레이터를 이용한 정량적 평가 방법 습득

수강대상 전기, 전자, 정보통신 관련 전공 대학생 및 산업체

강의수준 중급 **강의형태** 이론+실습

사전지식·선수과목 학부 수준의 컴퓨터 구조 및 논리 회로

7/11-14

강좌제목 스마트 모바일 API기반 SoC구조 및 주변장치 응용

강사 한태희 교수(성균관대학교)

강좌개요

- 고성능 모바일 AP 구조
- AP기반 SoC 구조
- Ti사의 Tiva AP 인터페이스 실습
- Tiva AP 주변장치 응용 실습

수강대상 학부생, 대학원생, 일반인

강의수준 초급

강의형태 이론+실습

사전지식·선수과목 컴퓨터구조, C 프로그래밍

7/28-29

강좌제목 Xilinx ISE 기반의 FPGA 동작 실습

강사 김민석 팀장(리버트론)

강좌개요

전반적인 FPGA 사용 Flow 이해를 기반으로 ISE 환경에서 Project를 진행하여 FPGA에 다운로드 및 디버깅 실습

수강대상

FPGA를 이용 동작 실습을 하고자 하는 학생, VHDL을 이해하고 실습을 통한 FPGA 동작을 이해하고자 하는 학생

강의수준 초급

강의형태 이론+실습

사전지식·선수과목 HDL, 디지털 논리 회로 이론

문의 | 경북대 IDEC 정미진 (053-950-6858, idec@ee.knu.ac.kr)

7/18-22

강좌제목 CMOS RF 트랜시버 회로 설계 실습

강사 신현철 교수(광운대학교)

강좌개요

본 설계실습 강좌에서는 RF 트랜시버에 사용되는 가장 필수적인 회로인, LNA, Mixer, VCO, 전력증폭기의 설계 실습을 진행한다. 각 회로의 기본적인 동작원리, 설계 이론, 성능 지수, Cadence Spectre RF를 이용한 설계 기술 등을 학습한다. 특히, 학생들이 주어진 예제 회로를 이용하여 단계별로 설계 및 시뮬레이션을 진행해 봄으로써, 회로 설계에 대한 이해도를 높일 수 있다. 최종적으로는 기본 회로를 연결하여 Direct Conversion RF 수신기 회로를 설계하고 시뮬레이션을 수행하여 수신기의 성능을 평가하는 능력을 습득한다.

수강대상 학부생, 대학원생, 일반인

강의수준 초급

강의형태 이론+실습

사전지식·선수과목 전자회로, CMOS 아날로그 집적회로, RF 집적회로

문의 | 광운대 IDEC 김주현 (02-940-5448, smartipc@kw.ac.kr)



광운대

7/4-7

강좌제목 지능형 웨어러블 시스템 설계

강사 박주현 교수(동국대학교)

강좌개요

1. 다양한 첨단 재료 및 소자를 기반으로 한 Wearable IoT
2. 소자 물리학을 바탕으로한 공정 최적화 연구
3. Wearable IoT Application 에 대한 소개
4. 자료에 대한 이해 및 기초 통계의 내용 리뷰
5. 연속형(continuous)인 변수가 집단 간에 차이가 있는지 여부를 검정하는 t-test(또는 ANOVA)
6. 두 연속형 변수간의 선형 관계성을 파악하는 회귀모형
7. 데이터의 주파수 분석
8. 데이터의 시-주파수 분석

수강대상 학부생, 대학원생, 일반인

강의수준 초급

강의형태 이론+실습

사전지식·선수과목

Digital Signal Processing, 회로이론, 반도체 공정, 반도체 물리, 전자회로



부산대

7/5-7

강좌제목 CPU 설계 및 응용

강사 윤병우 교수(경성대학교)

강좌개요

현재 대부분의 SoC에는 CPU가 내장되어 있다. 따라서 CPU를 설계하고 응용하는 것이 SoC 설계에서 가장 중요한 일이다. 본 강좌에서는 4-bit CPU core와 calculator 동작에 필요한 IP를 FPGA 설계 툴을 이용하여 schematic 방식으로 설계한다. 설계된 HW가 +, -, X, ÷, √ 계산을 하는 2 digits calculator로 동작하는 microprogram을 코딩하여 최종적으로 HW와 SW를 FPGA에 다운로드하여 동작시켜본다.

수강대상 학부생

강의수준 중급

강의형태 이론+실습

사전지식·선수과목 논리회로

수강을 원하는 분은

IDEC홈페이지(www.idec.or.kr)를 방문하여 신청하시기 바랍니다.

7/19-21

강좌제목 Verilog을 이용한 Digital System 설계

강사 강봉순 교수(동아대학교)

강좌개요

디지털 하드웨어 설계의 국제 표준언어인 Verilog HDL의 기초이론과 응용에 대하여 학습한다. 습득한 이론을 바탕으로 기능 블록을 설계하고, 최종적으로 디지털 전자 시계의 전체 기능을 Verilog HDL을 이용하여 설계한 후에 Training Kit에 Download 하여 기능을 확인한다.

수강대상 2학년 수료자, 디지털 논리회로 설계 초보자

강의수준 초급 **강의형태** 이론+실습

사전지식·선수과목 논리회로

7/28-30

강좌제목 CMOS Analog 전자회로 설계

강사 신현철 교수(광운대학교)

강좌개요

CMOS 및 전자회로에 대한 기본적인 이해를 돕기 위하여 만들어진 코스이다. 대부분의 대학에서 증폭기를 만드는 실험을 하지만 파형의 왜곡이 왜 생기고 그것을 어떻게 해결하는가를 설명하지 않는 경향이 있다. 본 강좌에서는 소자의 동작원리에서부터 왜곡의 원인과 해결책, 이득 결정 방법 등을 손으로 설계해보고 HSPICE를 이용하여 검증하여 체험적으로 이해하도록 할 계획이다.

수강대상 2학년 수료자, 아날로그 설계 초보자

강의수준 초급 **강의형태** 이론+실습

사전지식·선수과목 전기회로, 전자회로 1

문의 | 부산대 IDEC 윤성심 (051-517-0172, idec@pusan.ac.kr)



전남대

7/25-29

강좌제목 CMOS Analog Layout 실습(LNA, Digital Gate)

강사 송재열 박사(융합산업연합회)

강좌개요

전자회로와 회로이론을 기초로 배운 전자공학 전공자와 관련업계 전공자들에게 MPW의 의미와 디지털회로의 동작원리 등을 기초부터 강의한다. Analog circuit의 기본인 CMOS의 이론을 기초로 공부하고, 이론적 배경을 설명한다. 특히 기존의 BJT와 CMOS의 다른 부분과 활용부분에 대해서도 설명하고, 응용되는 분야에 대해서도 강의한다. 증폭기로 사용되는 CMOS의 특징과 이를 이용한 LNA의 성능측정방법을 실습으로 설명하고, 스위치로 사용되는 Digital Circuit(Gate)의 특징과 동작방법을 설명하고, Tool을 통해 Layout 후 시뮬레이션으로 동작을 확인해본다.

수강대상 전자전공 대학(원)생

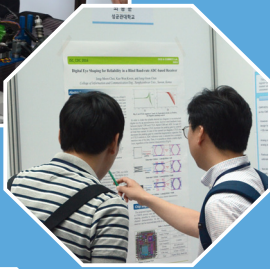
강의수준 중급

강의형태 이론+실습

사전지식·선수과목 회로이론, 전자회로, 논리회로

문의 | 전남대 IDEC 김정주 (062-530-9367, Tomo135@naver.com)

2016 IDEC SoC Congress 개최



IDEC은 지난 6월 30일(목), KAIST K빌딩에서 2016 IDEC SoC Congress를 개최했다. 이 행사에서는 국내 SoC 대학 인력 양성 방향을 논의하고 관련 산업 동향 세미나를 진행하는 자리가 마련되었다. 또한, IDEC MPW를 통해 설계 결과를 전시하는 Chip Design Contest에는 각 대학에서 총 92팀(데모 8팀, 패널 84팀)이 참여했다. 뿐만 아니라, IDEC 참여 대학인 Working Group 연구실의 성과와 지난 최근 2번의 Chip Design Contest에서 수상한 우수 작품 전시도 함께 진행되었다.

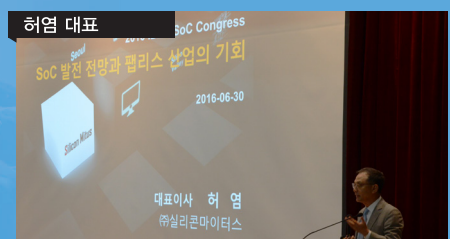
행사의 시작과 함께 가장 먼저 진행된 발표 세션은 2층 매트릭스홀에서 총 5팀이 각자 성과를 발표하고 질의 응답을 가지는 시간이 되었다. Working Group 우수 성과 및 최근 1년간 3개의 Chip Design Contest에서 수여한 팀의 설계 내용에 대한 발표가 있었다.

이후 1층 퓨전홀에서는 IDEC 소장인 박인철 교수의 오프닝 축사와 사업 소개 등을 시작으로 각 연사의 강연이 연이어 이루어졌다.



첫 번째로 이루어진 강연은 이규복 CP(미래부/IITP ICT 디바이스)의 “지능형 반도체 기술 및 정책 방향”이었다. 이규복 CP는 현재의 지능정보 기술 주도의 4차 산업혁명이 시작됨에 따라 급격한 시장 재편이 이루어지면서 지능형 반도체가 중요한 위치에 있음을 설명하면서, 국내 대학 및 팹리스 업체에 대해 파운드리 제작 지원 방안을 마련해야 하고, 차세대 신산업 창출을 위해 대학의 고급 인력 양성이 필요하다고 지적했다.

두 번째로는 허염 대표(실리콘마이터스)의 “SoC 발전 전망과 팹리스 산업의 기회”라는 주제로 발표가 진행되었다. 허염 대표는 반도체 및 팹리스 업계의 동향을 분석하면서 4차 산업혁명이 도래함에 따라 새로운 패러다임에 대응해야 한다는 이야기를 시작으로, 한국 팹리스가 발전하기 위해서는 문제점으로 지적되는 대기업 위주의 구조와 혁신성의 취약, 열악한 창업 환경 등을 타파하여 전문 인력을 양성하고 새로운 응용분야를 개척해야 한다고 주장했다.





오후 세미나로는 최승중 전무(LG전자의 “TV Technology & SoC Solution”이라는 주제로 강연이 진행되었다. 최승중 전무는 이제는 TV도 역시 스마트폰처럼 여러 기술이 응집된 하나의 기기로 거듭나고 있다는 추세를 설명했다. 현재 TV는 인간의 시각 체계와 닮은 시스템, 높은 해상도와 넓은 색의 스펙트럼과 시야각을 갖춘 기기로 진화하고 있으며, 이를 시스템온칩(SoC)과 관련하여 설명했다.



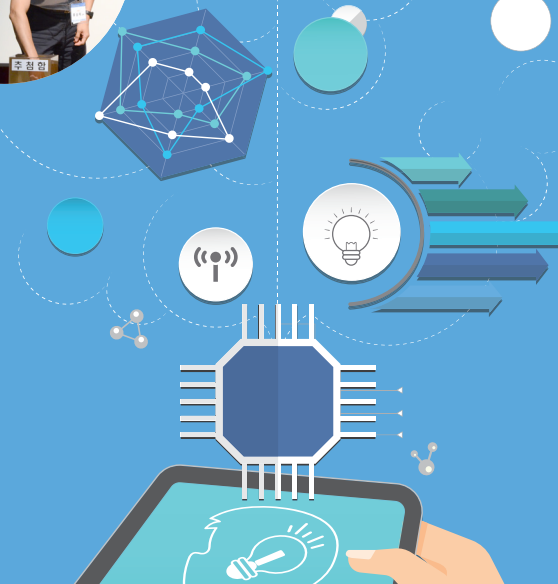
퓨전홀에서 진행된 마지막 세션은 박인철 소장의 발표를 통해 “대학에 대한 지원 성과 보고 및 현안에 대한 논의”라는 주제로 진행되었다. 박인철 소장은 IDEC에 대한 소개와 함께 최근 중점 추진내용인 MPW 및 EDA Tool 지원 사항, 교육 이수제 시행, IDEC 저널인 JICAS 발간 등에 대해 소개했다. IDEC 현안으로는 파운드리 지원 축소 및 보안문제, 예산 축소와 관련하여 많은 관계자분께 이에 대한 관심과 지원이 필요함을 호소했다.

한편, 시상식에서는 Chip Design Contest에서 우수팀으로 선별된 총 10팀에 대한 시상도 진행되었다. 2015년 11월에 열린 ISOCC 2015 CDC와 2016년 2월에 열린 제23회 KCS CDC에서 우수팀으로 선별된 5팀의 시상도 함께 진행되었다. 가장 우수한 논문인 Best Design Award는 KAIST 김유창(논문명: A 0.55V 1.1mW Artificial-Intelligence Processor for Micro Robots)에게 돌아갔다. 마지막으로 경품 추첨도 함께 진행되었다.



| 2016 IDEC SoC Congress CDC 수상 내역 |

참여 CDC명	수상명	소속	이름	지도교수
ISOCC 2015 CDC	Best Design Award	금오공대	이필호	장영찬
	Best Demo Award	동국대	손충환	변상진
제23회 한국반도체학술대회 CDC	Best Design Award	송실대	손민오	박창근
	Best Poster Award	경희대	박다솜	이종욱
	Best Poster Award	서울대	최광석	권영우
2016 IDEC SoC Congress CDC	Best Design Award	KAIST	김유창	유희준
	Best Demo Award	금오공대	성미지	신경욱
	Best Poster Award	POSTECH	채민균	박홍준
	Best Poster Award	KAIST	창동진	류승탁
	Best Poster Award	중앙대	전수진	최영완



고성능 문자열 매칭 엔진의 연구동향

김현진 교수 | 단국대학교 전기전자공학부

문자열 매칭 엔진

통신과 하드웨어 기술의 발달과 다양한 멀티미디어 매체의 등장으로 처리해야 하는 정보량이 계속적으로 증가하고 있다. 이러한 정보로부터 유효한 결과를 찾아내기 위해 다양한 접근방법의 연구가 활발하다. 정보의 가장 단순하면서 중요한 형태인 텍스트는 ASCII 및 이진 문자의 형태를 모두 포함한다. 문자들의 stream을 문자열이라고 하며, 이로부터 필요한 데이터를 추출하는 것은 정보 검색에서 매우 중요하다. 문자열 매칭(matching)은 패턴(pattern)이라는 검색해야 하는 문자로 이루어진 대상이 문자열에 존재하는 여부를 찾는 과정을 의미한다. 또한, 문자열 매칭 엔진은 문자열 매칭을 수행하기 위해 필요한 소프트웨어나 하드웨어로 이루어진 모듈을 의미한다.

표 1. 문자열 매칭 엔진의 분류

분류 기준	분류
패턴의 개수	Single-pattern string matching engine Multi-pattern string matching engine
병렬화	Non-parallel string matching engine Parallel string matching engine
입력의 양	Single-character string matching engine Multi-character string matching engine
일치도	Exact string matching engine Approximate string matching engine
처리 방법	On-line string matching engine Off-line string matching engine
구현 수단	Software-based string matching engine CPU-based string matching engine GPU-based string matching engine Hardware-based string matching engine Memory-based string matching engine FPGA-based string matching engine
방법론 ¹	Heuristic-based string matching engine Filtering-based string matching engine Automata-based string matching engine

문자열 매칭의 경우 다양한 응용분야에 적용될 수 있다. 가장 응용이 활발한 분야는 네트워크의 보안 및 QoS(Quality of Service)와 DNA 분석에 필요한 패턴의 매칭이다. 네트워크 보안의 경우 OSI 7 레이어의 사용자 데이터를 포함하는 페이로드(payload)에 관련된 패턴의 존재 여부를 판단한다. 보안의 경우 악의적 데이터의 존재여부를 검색하며, QoS의 경우 해당 사용자 데이터 내 유용한 정보의 존재여부를 검색하여 네트워크 사용자 각각에 다른 서비스를 제공할 수 있다. DNA 분석의 경우, 해당 DNA 패턴의 존재여부를 빠르게 검색하기 위해 문자열 매칭이 사용될 수 있다. 이 밖에도 이진 데이터 내에 관련 데이터의 존재 여부를 검색하기 위한 다양한 응용 분야에 적용이 가능하다. 문자열 매칭 엔진은 표 1과 같이 다양한 분류가 가능하다.

표 1에서 볼 수 있듯 문자열 매칭 엔진은 구현 수단, 패턴의 개수, 일치도, 병렬화 및 처리 방법에 따라 다양하게 분류할 수 있다. 처리해야 하는 정보의 양과 속도가 증가함에 따라 고성능의 매칭 엔진의 개발이 요구된다. 이러한 고성능 문자열 매칭 엔진의 요구를 고려하여 표 1의 분류 기준에 따른 연구동향에 대해 논하고자 한다.

패턴의 개수와 병렬화, 입력의 양에 따른 문자열 매칭 엔진의 개발

처리해야 할 데이터의 형태가 다양화 되어 이러한 경우를 고려해야 함에 따라 패턴의 개수는 증가하고 있다. 이는 해당 어플리케이션의 응용에 매우 좌우된다. 만약 워드프로세서 내에서 해당 패턴을 검색하는 대표적인 문자열 매칭 응용 분야인 Text Retrieval의 경우, 패턴의 개수는 대부분 하나이다. 이와 달리 네트워크 상의 보안과 QoS를 위한 Deep Packet Inspection(DPI)의 경우는 유해한 데이터나 QoS와 관련된 데이터가 있는지를 판단하기 위해 많은 수의 패턴을 검색한다. 이러한 패턴들은 사라지는 것이 아니라 지속적으로 축적되므로 검출해야 하는

패턴의 개수는 계속적으로 증가하게 된다. 이 패턴들은 결국에는 어떠한 정보의 형태로 문자열 매칭 엔진에 저장되어야 하기 때문에 메모리 및 하드웨어의 증가를 가져올 수 밖에 없다. 또한, 검색해야 할 대상이 많아지기 때문에 쓰루풋(throughput)의 감소를 가져올 수도 있다. 그러므로 패턴의 개수가 많아지더라도 해당 메모리나 하드웨어의 증가가 비례하여 증가하지 않도록 하는 연구가 진행되어 왔다. 대표적인 것은 오토마타(automata)를 기반으로 하는 문자열 매칭 엔진이다. 이 경우 일치하는 패턴의 프리픽스(prefix)는 각 패턴들에 해당되는 상태 천이(state transition)에서 공유된다. (오토마타를 기반으로 한 문자열 매칭 엔진은 방법론의 분류 기준에 따른 비교에서 자세히 살펴보도록 한다.)

아래 그림 1의 예는 오토마타를 기반으로 하는 문자열 매칭 엔진의 예이다. 이 경우 패턴 "he," "hers," "his"의 세 패턴에 대한 deterministic 오토마타이다. 이 때 문자 "h"는 상태 천이로 공유된다. 아래에서 점선의 경우는 failure transition을 의미하며, 이는 longest common suffix를 향하게 된다. 또한, 실선의 경우 패턴에 따른 상태 천이를 의미한다. 원과 원안의 인덱스는 상태와 상태의 번호를 의미하며, 회색의 원은 패턴이 매칭되는 상태를 의미한다. Deterministic 오토마타는 한번에 하나의 상태를 가질 수 있으며 non-deterministic 오토마타의 경우는 한번에 여러 상태를 가질 수 있다. 이러한 오토마타 기반의 문자열 매칭 엔진의 경우 prefix를 공유함으로써 저장에 필요한 상태 천이의 개수를 줄일 수 있다는 장점이 있다.²

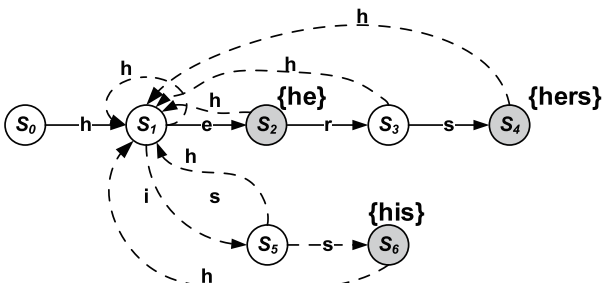


그림 1. 패턴 "he," "hers," "his"에 대한 상태와 상태 천이

하나의 패턴 매칭 엔진의 하드웨어 크기가 커지게 되면 하나의 엔진에서 처리해야 할 패턴 개수도 증가하게 되어 성능이 저하될 수 있다. 또한, 패턴과 비교하게 되는 입력이 하나만 존재한다면 속도도 제한적일 수 있기 때문에 쓰루풋을 늘리는 데 제한이 있을 수 있다. 병렬화(parallel) 문자열 매칭의 경우는 하나의 엔진을 여러 개의 모듈로 나누어 문자열 매칭을 수행하는 방식이다. 여러 개의 모듈로 나누게 되면 각 모듈당 저장해야 하는 패턴의 개수가 줄 수 있으므로 하나의 모듈의 복잡도가 감소하게 되고, 이를 통해 쓰루풋을 증가시킬 수 있다. 또한, 동일하거나 유사한 형태의 모듈을 병렬로 배열하고 이에 대해서 입력을 분리하여 가함으로써 해당 쓰루풋을 모듈의 개수만큼 증가시킬 수 있다. 병렬화를 수행하게 되면 병렬로 배열된 모듈의 개수가 증가함에 따라 하드웨어가 증가하게 된다. 이 증가비율을 줄이기 위해서 다양한 기법들이 적용될 수 있다.

처리되는 입력의 양에 따른 분류의 경우 한번에 처리되는 문자의 개수에 따라 single-character와 multi-character 문자열 매칭 엔진으로 나눌 수 있다. Single-character의 경우, 한번에 하나의 이진 문자 또는 ASCII 문자(8비트)가 입력되는 경우를 의미한다. 이 경우 쓰루풋은 한 클럭에 입력되는 비트의 수 x 클럭 주파수로 계산이 된다. 최신의 하드웨어의 경우 수백 MHz에 달하는 동작 클럭 주파수를 가지고 있을 경우 대략 수 Gbps의 쓰루풋을 가질 수 있다. 그러나, 현재 네트워크의 속도가 100Gbps에 달할 예정이고, 한 명의 게놈 데이터가 대략 3GB의 정보를 가지기 때문에 수 Gbps의 쓰루풋은 충분하지 못할 수 있다. 병렬화 문자열 매칭 엔진에서 multi-character 문자열 매칭 엔진은 한번에 여러 개의 이진 문자 또는 ASCII 문자를 입력 받는 문자열 매칭 엔진을 의미한다. 여러 개의 single-character 문자열 매칭 엔진 모듈을 병렬로 배치하여 여러 개의 문자를 처리하는 방식이다. 이 경우, 한 클럭에 처리될 수 있는 문자의 개수가 늘어나게 되므로 쓰루풋이 늘어나게 된다. 그렇지만 패턴과 비교되어야 하는 입력 데이터는 일종의 문자열이므로 각 모듈에 입력되어야 할 문자열을 적절하게 나누어 입력해야 하는데, 이를 chunk라 한다.³ 이 경우 두 개 혹은 여러 개의 chunk 사이에 걸쳐 있는 패턴을 검출해야 하는 문제가 있어, 모듈의 개수와 쓰루풋의 증가율이 비례하지 않을 수 있다. 또한, 하드웨어가 모듈의 개수에 비례하여 늘어나는 문제가 있으므로 하드웨어의 증가율을 줄일 수 있는 연구가 진행되고 있다.

일치도 및 처리 방법에 따른 문자열 매칭 엔진의 개발

일치도에 따라 문자열 매칭은 Exact 문자열 매칭과 Approximate 문자열 매칭으로 나눌 수 있다. Exact 문자열 매칭은 패턴에 해당되는 데이터가 입력 문자열에 정확하게 있는지를 검출하는 문자열 매칭이다. Exact 문자열 매칭은 네트워크 보안과 QoS 관련된 문자열 매칭 엔진에서 주로 연구된다. 이 경우 패턴은 문자열의 형태와 정규식(Regular Expression)의 형태로 나눌 수 있다. 패턴이 문자열의 형태인 경우는 정규식에 비해 단순한 구조로 검출이 가능하다. 그렇지만 정규식의 경우는 정규식 하나가 여러 개의 문자열 패턴 형태를 가질 수 있고, 그 길이 또한 다양해질 수 있기 때문에 패턴에 따라 훨씬 복잡한 형태를 가질 수 있다. 소프트웨어 기반의 문자열 매칭의 경우 프로그램에 의해 문자열 패턴 형태를 결정하기 때문에 정규식 패턴의 경우 그 속도가 매우 느려질 수 있다. 그러므로, 정규식 패턴을 가지는 고속의 문자열 매칭 엔진의 경우는 FPGA를 이용한 하드웨어 기반의 문자열 매칭 엔진에 대한 연구가 활발하게 진행되고 있다.

Approximate 문자열 매칭의 경우에는 패턴이 완전히 일치하지 않아도 일정 비율 이상 패턴의 문자열이 일치하면 매칭 되었다고 생각한다. 이 경우 threshold 값이 존재하게 되며 threshold 값은 여러 형태로 나타낼 수 있지만, 대체적으로 비율 값을 의미하는 상수가 될 수 있다. Approximate 문자열 매칭은 Exact 문자열 매칭을 포함하는 superset이 될 수 있다. 만약 패턴 "abcd"와 75% 이상 매칭하는 패턴이라면

“cbcd,” “bbcd” 등의 패턴도 모두 매칭하는 것으로 생각할 수 있다. 그러므로 패턴이 하나만 존재하더라도 상당히 많은 수의 문자열 패턴이 존재하는 Exact 문자열 매칭이라고 생각할 수 있다. 그러므로, Approximate 문자열 매칭에서는 병렬화 문자열 매칭 엔진이 필수적이며, 해당 하드웨어의 크기와 쓰루풋을 고려한 연구가 진행 중이다. Exact 문자열 매칭과 달리 영상처리, DNA 분석 등의 바이오 및 생체 데이터와 연관이 되어 있는 경우가 많다.⁴

처리 방법에 따른 문자열 매칭에서 on-line 문자열 매칭 엔진은 패턴과 비교해야 할 데이터가 실시간으로 입력되는 경우에 사용된다. 대표적으로 네트워크 데이터가 있다. 이 경우 데이터를 저장하는 Queue의 용량의 한계로 인해서 문자열 매칭 엔진의 쓰루풋은 일정하게 유지되어야 한다. Off-line 문자열 매칭 엔진의 경우는 비교해야 할 데이터가 모두 저장된 상태에서 비교가 이루어지는 경우를 의미한다. 대표적으로 text retrieval과 DNA 분석 등이 있다. 결과적으로 데이터가 저장되어 있는 스토리지의 한계는 없다고 가정되기 때문에 on-line 문자열 매칭 엔진에서 발생하는 문제는 Off-line에서 발생하지 않는다.

구현 수단에 따른 문자열 매칭 엔진의 개발

구현 수단을 고려하였을 때 소프트웨어와 하드웨어를 이용한 구현이 가능하다. 소프트웨어 적인 문자열 매칭 엔진의 경우 코어(core)를 바탕으로 이 코어에서 수행되는 프로그램에 의해 해당 패턴이 있는지를 검색하게 된다. 기존의 CPU-based 문자열 매칭 엔진에서는 CPU(Central Processing Unit)에서 프로그램을 수행함으로써 패턴의 검색이 수행된다. 현재 일반적인 프로세서의 경우 일반적으로 4~8개 정도의 강력한 연산 능력이 있는 코어를 가지고 있다. 그렇지만 코어의 개수가 작기 때문에 병렬화 할 수 있는 여지가 작다. 또한, 다른 유저 프로그램을 수행해야 하므로 CPU만 의존해서는 성능이 만족스럽지 않다.

GPU의 경우 해당 코어의 개수가 CPU 보다는 훨씬 많다는 점이 병렬화 문자열 매칭 엔진을 구현하는데 유리하다. 이에 따라 많은 chunk로 입력을 나누어 문자열 매칭을 수행하고 결과값을 동기화하여 적절하게 매칭 결과를 출력할 수 있다는 점이 장점이 있다. 하지만 GPU에 적절한 프로그래밍을 위해 Nvidia의 CUDA나 OpenCL과 같은 언어로 문자열 매칭 엔진이 프로그래밍 되어야 한다. 이 경우 실제 그래픽 카드가 장착된 메인 버스의 속도에 의해서 처리 성능이 제한될 수 있다는 점도 유의해야 한다.

GPU를 사용하는 경우 상당 수준의 병렬화 처리를 수행할 수 있으나, coarse-grained 병렬화라는 점에서 그 한계가 존재할 수 있다. 하드웨어 기반의 문자열 매칭 엔진의 경우 하드웨어 블록을 이용하여 문자열 매칭을 수행한다는 점에서 훨씬 세밀화(fine-grained)한 병렬화 문자열 매칭이 가능하며, 이를 통해 더 나은 쓰루풋을 얻을 수 있다. 메모리 기반의 문자열 매칭 엔진의 경우는 메모리 블록을 이용하여 패턴 데이터를 저장하여 문자열 매칭을 수행하는 방식이다. 기존에는 TCAM

(Ternary Content-Addressable Memory)를 이용하는 방식이 대표적이었다. TCAM은 메모리 용량과 같은 비트 수준의 비교기가 다량 존재하여 해당 패턴을 비교한다. 그러나, TCAM의 비용과 파워 소모가 매우 크므로 이에 대한 해결책을 많이 연구하였다. 대표적으로 일반적인 메모리 블록에 FSM(Finite-State Machine)을 구성하여 해당 입력에 따라 다음 상태(next state)를 찾아가는 형태가 대표적이다. 이 경우, 입력의 크기에 따라 저장해야 할 다음 상태의 개수가 늘어나게 된다. 입력이 8비트라면 다음 상태의 개수는 256개가 된다. 이를 줄이기 위해 bit-split 문자열 매칭 엔진이 제안되었고, 이를 응용한 다양한 메모리 기반 문자열 매칭 엔진의 구현의 연구가 진행되었다.⁵ 또한, TCAM과 일반 메모리를 결합하여 필요한 TCAM의 크기를 줄이는 방법에 대한 연구도 진행되었다.

FPGA 기반 문자열 매칭 엔진의 경우는 FPGA 내부의 LUT(LookUp Table)을 이용하여 문자열 매칭 엔진을 수행하는 것을 의미한다. 물론 FPGA 내부에도 일반 메모리 블록이 포함될 수 있지만, LUT는 FPGA에서 유일한 것이기 때문에 LUT를 사용한 경우 FPGA 기반 문자열 매칭 엔진으로 분류할 수 있다. LUT를 이용하여 다음 상태 값을 도출하는 경우 여러 개의 LUT를 이용하여 실제 패턴의 문자와 일치하는 데이터만 저장할 수 있기 때문에, 초기 상태를 향하는 경우의 값을 저장할 필요가 없다. 또한, 일반적으로 동작 주파수가 500MHz 이상으로 수행시키는 것이 가능하여 메모리를 읽고 쓰는 속도보다는 대체적으로 빠르다는 장점이 있다. 또한, 하나의 FPGA 내부에서 회로를 구성하여 병렬화 문자열 매칭을 수행할 수 있으며 FPGA 내의 기타 회로와 결합하여 해당 패턴 매칭 결과를 이용할 수 있다는 장점이 있다. 그렇지만 패턴의 업데이트에 FPGA의 구성을 바꾸는 것이 메모리 내용을 바꾸는 것보다 번거롭다는 단점이 있다.

방법론에 따른 문자열 매칭 엔진의 개발

기존에는 Heuristic 기반과 Filtering 기반에 의한 문자열 매칭 엔진의 경우 다양한 응용분야에 사용되고 있다. 그렇지만 heuristic 기반의 문자열 매칭의 경우 패턴의 검색을 빠르게 할 수 있는 heuristic적 알고리즘에 기반하는데, 패턴이 여러 개인 경우에 대한 적절한 해결책이 되지 못한다. 또한, 입력 데이터의 종류에 따라 쓰루풋이 가변적일 수 있다. Filtering 기반에 의한 문자열 매칭은 해쉬(hash)에 기반한 문자열 매칭이다. 이 경우 하드웨어 복잡도가 크게 감소할 수 있으나, 궁극적으로 실제 패턴이 매칭 되지 않을 경우에 패턴 매칭이 보고되는 false positive의 문제가 지속적으로 있을 수 밖에 없다. Heuristic 기반과 Filtering 기반의 문자열 매칭의 경우는 소프트웨어 기반의 문자열 매칭 엔진의 구현에 더 적합하다는 장점이 있으나, 소프트웨어 적인 문자열 매칭 엔진의 쓰루풋의 한계에 따른 문제점을 가진다는 단점이 존재한다. 이와는 달리 오토마타 기반의 문자열 매칭 엔진의 경우는 그림 1과 같이 상태와 상태 전이를 이용하여 공통되는 프리픽스를 공유하고 입력의 종류와 상관 없이 일정한 쓰루풋을 낼 수 있다는 장점이 있다. 그렇지만

모든 상태와 상태 천이를 저장해야 하는 메모리와 하드웨어의 크기가 클 수 있다는 단점이 존재한다.

결론

데이터의 처리 속도와 정보량의 증가에 의해 데이터에서 의미있는 패턴이 있는지를 검출하는데 고성능의 문자열 매칭 엔진이 요구된다. 이를 위해 병렬화 문자열 매칭과 기존의 CPU와 메모리 기반의 문자열 매칭 엔진보다 성능을 더 높일 수 있는 GPU와 FPGA 기반의 문자열 매칭 엔진의 개발이 요구된다. 또한, single-character 입력에 의해서는 만족스러운 쓰루풋을 얻을 수 없기 때문에 multi-character 문자열 매칭 엔진의 연구가 지속적으로 진행될 것이다. 또한, 바이오나 생체 데이터에 적합한 패턴 매칭을 위한 approximate 문자열 매칭의 병렬화 연구가 더 활발하게 진행될 것으로 예상된다.

참고문헌

- 1 P.-C. Lin, Y.-D. Lin, T.-H. Lee, and Y.-C. Lai, "Using String Matching for Deep Packet Inspection," IEEE Computer, vol. 41, no. 4, pp. 23-28, 2008.
- 2 A.V. Aho and M. J. Corasick, "Efficient String Matching: An Aid to Bibliographic Search," Communication ACM, vol. 18, issue 6, pp. 333-340, 1975.
- 3 C.H. Lin, C.H. Liu, L.S. Chien, and S.C. Chang, "Accelerating pattern matching using a novel parallel algorithm on GPUs," IEEE Trans. on Computers, vol.62, no.10, pp.1906-1916, 2013.
- 4 Inoue K, Shimozono S, Yoshida H, Kurata H. Application of approximate pattern matching in two dimensional spaces to grid layout for biochemical network maps. PloS one, no. 7, vol. 6, e37739, 2012.
- 5 L. Tan and T. Sherwood, "A High Throughput String Matching Architecture for Intrusion Detection and Prevention," Proc. 32nd IEEE/ACM Intl Symp. Computer Architecture, pp. 112-122, 2005.

저자정보

김 현 진 교수



소 속

단국대학교 전자전기공학부

E-mail hyunjin2@dankook.ac.kr

Homepage <http://sites.google.com/site/dankooksoc>

테스트 로직을 통한 하드웨어 공격 및 보안

이인걸 박사과정, 강성호 교수 | 연세대학교 전기전자공학과



Testability vs Security

IT 기기의 발전으로 스마트폰 등의 포터블 기기가 급속하게 보급됨에 따라 이러한 하드웨어에 대한 보안 문제가 새로이 떠오르고 있다. 실제로 스마트카드나 Zigbee, 블루투스 같은 보안이 필요한 하드웨어의 경우 칩 내부에 중요 정보를 저장하게 되는데, 이러한 중요 정보를 보호하기 위한 암호화 모듈(Encryption module)은 더 이상 선택적인 옵션이 아니다. 칩 내부 저장된 데이터는 불법적인 공격으로 이를 유출할 수 있는데, 암호화된 정보는 암호 키가 없으면 유출이 되더라도 무의미한 값을 가지므로 가장 간단하게 정보를 보호할 수 있는 수단으로 여겨진다. 일반적으로 많이 사용되는 암호화 모듈은 Advanced Encryption Standard(AES)라고 하는 모듈인데, 이는 NIST가 제정한 후 미국 정부가 채택한 암호화 알고리즘으로써 높은 안정성 및 속도를 가져 전 세계적으로 널리 사용되고 있다. AES 알고리즘은 하드웨어로 구현하기 쉽고 메모리를 적게 차지하여 스마트카드 등 메모리 용량이 적은 장치에서 손쉽게 사용 가능할 뿐만 아니라, 프로그램이나 암호화 자체를 공격하는 방법으로는 해독이 거의 불가능하다고 알려져 있다. 미국 정부가 정식으로 채택한 알고리즘이라는 사실이 이를 증명한다. 하지만, 이러한 알고리즘을 하드웨어로 구현한 경우는 이야기가 달라지게 된다.

일반적으로 칩을 제작할 때에는 칩 내부에 테스트를 위한 로직(Design for Testability, DFT)을 추가하여 테스트 비용 절감 및 고장 검출율을 높임으로써 제품의 신뢰성을 보장하게 한다. 특히, 스캔 기반의 테스트 방식이 널리 사용되는데 이는 내부 플립플롭을 스캔 플립플롭으로 변환시켜 내부 데이터를 관측이 가능하도록 설계하는 기법이다. 이렇듯 스캔 체인은 내부 플립플롭에 대한 접근이 가능하여 고장이 발생했을 이의 디버깅을 용이하게 한다는 장점이 있지만, 스캔 체인을 통한 testability의 향상은 필연적으로 하드웨어의 보안성을 약화시킬 수 밖에 없다. AES 코어가 내장된 회로에 스캔 테스트를 진행하게 되면 특정한 공격에 의해 AES 내부에 저장되어 있는 사용자 비밀 키를 유출해 낼 수 있기 때문이다. 이렇듯 소프트웨어적으로는 완벽한 보안을 자랑하는 AES 알고리즘이지만 하드웨어의 테스트 모듈을 사용하면 보안성에 약점이 존재한다. 실제로 테스트 인터페이스를 통해 기존에 사용되고 있던 기기들의 보안이 위협받는 경우가 종종 발견된다. XBOX 360 기기의 경우 JTAG를 통해 불법 복제품을 사용하도록 할

수 있고, 아이폰의 경우도 테스트 인터페이스를 통해 기기의 각종 잠금을 해제하는 탈옥이라는 행위가 가능하다. 이와 같이 testability와 보안성은 trade-off 관계가 성립하는데 보안성을 보장하면서 동시에 제품의 신뢰성 또한 보장할 수 있는 여러가지 장치들이 많이 연구되고 있다.

테스트 로직을 통한 여러가지 공격

악의적인 사용자는 테스트를 위한 로직을 통해 여러가지 공격을 수행할 수 있다. 본 파트에서는 테스트 로직을 통한 여러가지 공격 방식을 소개한다.

1. JTAG 인터페이스를 이용한 공격

JTAG은 시스템의 디버깅 및 테스트를 위해 내부를 들여다 볼 수 있는 강력한 인터페이스이다. 이는 시스템의 신뢰성 확보를 위해 필수 불가결한 요소인데, JTAG이 가진 강력한 액세스 기능은 시스템을 공격하려는 해커들에게는 중요한 공격 수단으로 이용된다. 실제로 JTAG을 통해 프로세서 및 레지스터/메모리 정보를 수집하여 암호 연산에 사용되는 키 값을 유출할 수 있으며, JTAG을 통해 수집된 내부 소프트웨어에 대해 리버스 엔지니어링을 수행하여 직접적인 공격이 가능하다. 또한, 펌웨어를 수정하여 시스템의 보안 동작을 무력화하거나 OS를 수정하여 아이폰의 탈옥, XBOX 360 게임기의 불법복제 소프트웨어 사용 등을 가능하게 하기 때문에 JTAG 인터페이스의 수정 없이는 시스템 보안에 큰 위협을 받으며, 실제로 여러 모바일 관련 기구들은 JTAG 디버그 인터페이스의 보안을 명시적으로 요구하고 있다.

2. 스캔 기반 부채널 공격 (scan-based side channel attack)

부채널 공격이란 암호 알고리즘을 대상으로 한 물리적 공격 기법이다. 말 그대로 정면돌파가 힘드니 측면에서 공격하자는 개념으로, 이는 주로 하드웨어를 기반으로 한 모듈에서 많이 이루어지게 된다. 부채널 공격에는 전력 분석 공격(Power analysis), 타이밍 공격(Timing analysis) 등 여러가지 종류가 존재하는데, DFT 가 삽입된 하드웨어에서는 스캔

기반 부채널 공격(Scan-based side channel attack)이 전통적으로 사용되어 왔다¹. 스캔 기반 부채널 공격은 테스트를 위해 생성한 스캔 플립플롭을 이용하여 암호화 과정 중 비밀 키가 적용된 중간값을 테스트 포트에 빼내어 이 정보를 이용하여 비밀 키를 유추하는 방법이다.

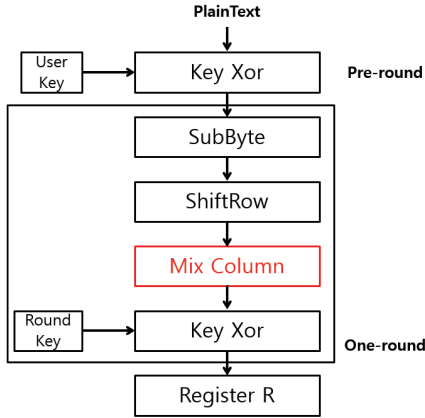


Figure 1. AES 암호화 알고리즘

AES 암호화는 그림 1과 같은 과정으로 이루어진다. 암호화하고자 하는 평문을 모듈에 입력하게 되면 내부에 저장되어 있던 비밀 키와의 연산을 통해 Pre-round를 거친 후 Sub-byte, Shift-row, Mix-column 등의 과정을 거쳐 한번의 라운드를 완성하게 된다. 이러한 라운드 과정을 정해진 횟수만큼 반복 진행한 뒤 암호문이 출력되게 되는데, 각 라운드의 중간값은 내부의 라운드 레지스터에 저장된다.

사용자 비밀키를 알아내기 위해 먼저 회로의 수많은 스캔 플립플롭 중 사용자 키와 관련된 스캔 플립플롭이 무엇인지 알아내야 한다. 편의상 사용자 키와 연결된 스캔 플립플롭을 키 셀이라고 부르자. AES 암호화 모듈의 특성상 1비트 입력의 변화는 연결된 32개의 플립플롭에 영향을 준다. 따라서 AES 모듈에 1비트만 다른 입력을 각각 가해 중간값을 추출한 후 값이 변하는 스캔 플립플롭의 위치를 찾는 방법을 통해 키 셀의 위치를 알아낼 수 있다. 이렇게 키 셀의 위치를 알아내게 되면 라운드 동작을 10번이나 거치지 않고 한번만의 라운드를 거친 라운드 레지스터 값을 알아낼 수 있어 역 추적을 통한 키 값의 유추가 용이해진다.

스캔 기반 부채널 공격에 대한 여러 가지 방어 방법

누군가가 무언가를 뚫으려고 하면 누군가는 이를 막고자 한다. 이러한 현상은 하드웨어 보안 쪽에서도 당연하게 나타난다. 위에서 설명한 스캔 기반 부채널 공격이 연구되며 이를 막기 위한 대책 또한 이어서 연구되어 왔는데, 그 중 몇 가지 방법을 소개한다.

1. Mode reset countermeasure

스캔 기반 부채널 공격의 경우 AES가 정상 동작에서 테스트 동작으로 변경 시 AES 모듈 상에 남아있는 라운드 레지스터의 값을 스캔 체인을

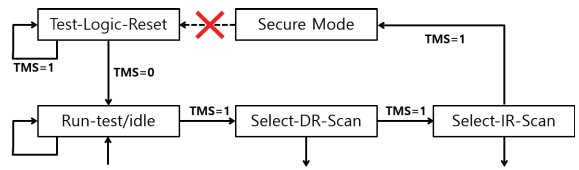


Figure 2. Mode reset countermeasure

통해 유출시킬 수 있다는 점이 사용자 비밀 키 유추를 가능하게 한다. 따라서 그림 2와 같이 라운드 레지스터의 값이 유출되지 않도록 보호하기 위해 AES가 정상 동작 모드에서 스캔 테스트 동작 모드로 바뀔 때, 라운드 레지스터에 해당하는 스캔 체인의 값을 리셋한 후 테스트 동작을 진행하도록 하는 방법이 존재한다². 이를 통해 한번의 라운드를 거친 라운드 레지스터의 값이 스캔 체인을 통해 빠져 나갈 때에는 리셋된 값이 나오기 때문에 사용자 비밀 키를 유추하는 것을 불가능하게 한다.

2. Mirror key register(MKR)

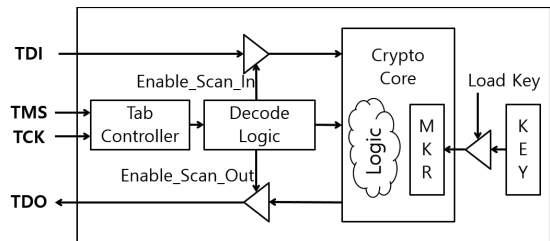


Figure 3. Mirror key register

사용자 내부 키 유출을 막기 위해 그림 3과 같이 AES 내부에 Mirror key register를 추가하여 AES가 암호화를 진행할 경우 사용자 키가 MKR로 로드되어 사용되고, 스캔 테스트 동작 시에는 스캔 체인이 MKR로 연결되어 스캔 연결이 사용자 키 값과는 관계 없게 만드는 구조가 제안되었다². 하지만 MKR 방식은 이미 설계된 AES의 코어를 수정해야 하기 때문에 모든 IP를 직접 설계하지 않고 일부 IP를 외부에서 제공하는 형태의 설계 환경에서는 비효율적이다. 또한, MKR을 추가함으로써 면적 및 파워 오버헤드를 증가시키는 결과 또한 가져오게 된다.

3. Flipped scan tree

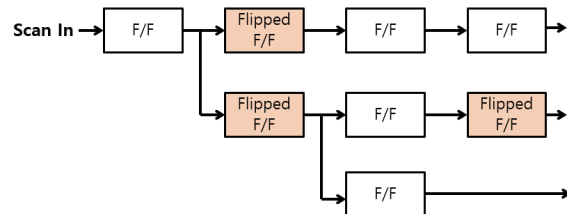


Figure 4. Flipped scan tree

그림 4의 방법은 회로를 구성하는 일부 스캔 플립플롭의 값을 인버터를 통해 반전시킴으로써 테스트 데이터 값을 보충한다³. 오직 스캔 회로를 디자인한 설계자만이 스캔의 반전된 위치를 알 수 있고, 반전된 위치 정보를 알아야지만 제대로 된 스캔 출력 값을 알 수 있다. 하지만, 해당 방어 방식은 Differential scan attack을 사용하여 공격할 경우에는

쓰모가 없어지게 된다. 어차피 스캔 체인을 통해 출력된 값의 차이를 통해 키 값을 유추하는 방식을 사용하기 때문에 인버터를 통해 아무리 반전을 시켜도 출력된 두 값의 차이는 반전 값과 상관없기 때문이다.

4. Scan chain scrambling

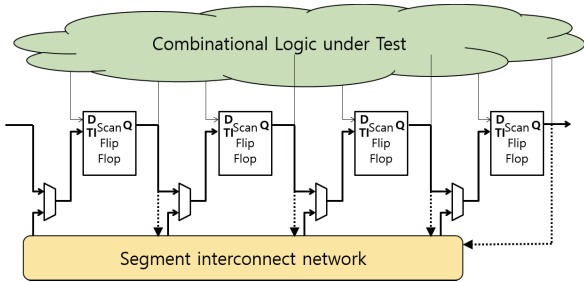


Figure 5. Scan chain scrambling

그림 5의 방식은 스캔 체인으로부터 출력되는 데이터의 순서를 뒤바꾸는 방법이다⁴. 인증되지 않은 테스트가 수행될 때는 TDO를 통해 출력되는 순서 값을 뒤바꾸는 방식으로 출력 값을 보호하게 되는데, Segment interconnect network 모듈이 이 역할을 수행한다. 올바른 키 값이 인가되었을 경우에만 스캔 셀들이 정상적인 순서로 연결이 되는데, 복잡한 연결 구조를 가지기 때문에 넓은 범위의 스캔 체인에 적용하기는 힘들다. 또한, 공격자가 입력에 대한 출력의 기대 값을 알고 있는 경우 통계적 방법으로 패턴 분석이 가능하여 보안성에 있어 약점이 존재하는 방식이다.

테스트 인터페이스 접근 차원의 방어

Unbounding

기존의 테스트를 위한 JTAG 포트가 문제가 된다고 하면, 사실 가장 간단하게 테스트 접근을 막을 수 있는 방식은 바로 JTAG 인터페이스를 영구적으로 제거하는 것이다⁵. 칩 제조 시 설계한 JTAG 인터페이스를 제조 단계에서의 테스트가 끝난 뒤 연결하고 있는 퓨즈를 제거하여 JTAG의 접근을 원천적으로 막는 방식이다. 하지만, 본 방식의 경우 디바이스의 사용 중 디버깅이나 테스트 접근 조차도 막아버려서 상당히 사용이 제한적일 뿐만 아니라, 칩의 패키징을 벗긴 후 microprobing을 하여 내부 신호를 관찰하는 경우 JTAG 인터페이스가 없더라도 내부 값을 관찰할 수 있어 보안성에 약점이 존재한다.

대칭 키 암호화 방식

대칭 키 암호화 방식은 그림 6과 같이 JTAG 을 이용하여 테스트를 수행할 때 JTAG 내부에 대칭키 암호 모듈을 추가하여 모든 테스트 입출력을 암호화 하는 방식이다⁶. 이는 곧 대칭키를 공유하고 있는 사용자만이 테스트 데이터를 복호화할 수 있다는 의미이므로, 테스트 데이터를 이용하여 사용자 키를 복원하는 등의 공격을 수행할 수 없다. 하지만

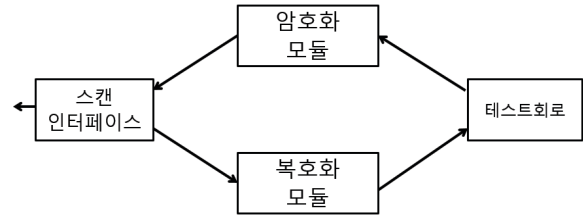


Figure 6. 대칭 키 암호화 방식

본 방식의 경우 모든 테스트 입출력을 암호화하므로 테스트를 수행할 시 테스트 입출력에 많은 딜레이가 발생하게 되어 효율적인 테스트가 이루어지지 않고, 구현하기 위한 비용이 크다는 단점을 지닌다.

Key based decoder blocking

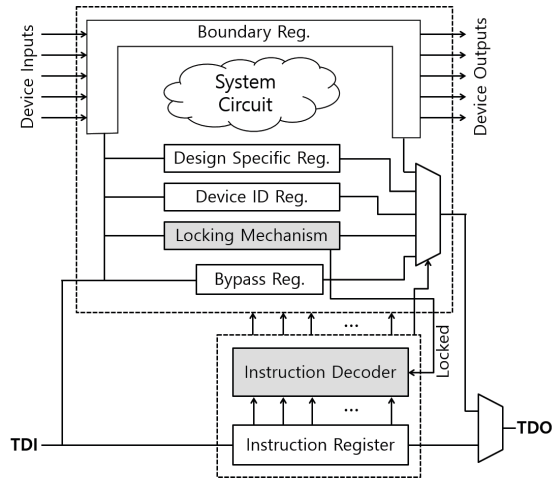


Figure 7. 1149.1 with locking mechanism

대칭키 암호화 방식은 테스트 데이터 자체를 암호화 하는 방식이라 효율성이 떨어진다. 실제로 산업에서 제작되는 하드웨어들은 JTAG 기반으로 이를 테스트 하게 되는데, JTAG의 테스트 명령 정도만 인증 없이 수행되지 않게만 만들어도 공격자 입장에서는 테스트 핀을 통한 데이터 출력이 어려워진다. 이렇게 인증되지 않은 사용자에 대해서는 JTAG 명령어를 사용할 수 없게 만들고, 키를 알고 있는 사용자만이 JTAG 명령어를 사용할 수 있는 방식이 제안되었다⁷. 그림 7은 1149.1 테스트 인터페이스 구조에서 테스트 명령을 사용해야 할 경우 올바른 키가 입력될 경우에만 JTAG의 잠금이 풀려 테스트를 수행할 수 있도록 하는 구조를 나타낸다. 이 경우, 키를 저장하는 레지스터와 비교기 정도를 추가하여 키가 인증되었을 경우에만 테스트를 수행할 수 있도록 한다.

하지만 이러한 키 기반 방식의 경우 공통적인 단점이 존재한다. 만약 인증 키 정보가 외부로 유출된다면, 아무리 인증 과정을 복잡하다 해도 누구보다 쉽게 테스트를 수행할 수 있다. 따라서 이런 키를 안전하게 관리하는 방법이 이슈가 되는데, 하나의 키가 유출되어도 모든 디바이스의 테스트를 수행할 수 없도록 디바이스에 각기 다른 키를 할당하는 방식이 해답이 될 수 있지만, 이 경우 키를 관리하는 관리 비용이 증가하게 된다는 단점이 존재한다.

인증 서버 기반 보안 시스템

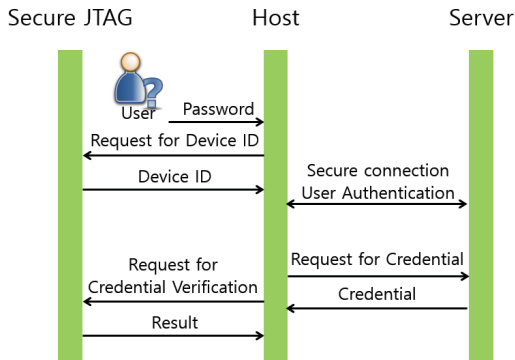


Figure 8. 인증 서버 기반 보안 시스템

기존의 JTAG 인증 기반 보호 기법의 경우 키 관리를 어떻게 하느냐가 관건이다. 따라서 이러한 문제를 해결하기 위해 나온 방식이 바로 인증 서버 기반 보안 시스템이다⁸. 이는 사용자가 아닌 신뢰할 수 있는 다른 객체에 의해 테스트 정보를 관리할 수 있게 하는데, 보통 관리 수단으로 인증 서버를 많이 사용한다. 인증 서버 기반의 방식은 그림 8과 같다. 기존 1149.1 과 호환이 되는 컨트롤 로직을 삽입하여 외부와의 통신을 통해 인증받아 회로를 테스트 하는 형식인데 인증 서버 기반의 방식 또한 단점이 존재한다. 일단 테스트를 위하여 인증이 필요한데, 인증을 위해 매번 서버에 접근해야 하기 때문에 비효율적일 뿐만 아니라 네트워크에 문제가 생길 경우 아예 인증이 불가능해 테스트를 할 수가 없어진다.

결론

반도체 기술이 발전하면서 향상된 삶의 질을 누릴 수 있게 되었지만 한편으로는 이를 악용하려는 무리의 존재로 인해 개인정보 등의 비밀 데이터 유출을 걱정해야 하는 불편함도 감수해야 한다. 본 기사에서는 반도체 기술의 발전에 따라 신뢰성을 보장하기 위해 삽입되는 DFT를 통해 보안성이 위협받는 과정 및 이를 해결하려는 방법을 보여준다. 시스템의 보안은 크게는 JTAG를 통한 시스템 침입에서 작게는 AES 하드웨어의 비밀 키 유출을 위한 공격에 대한 방어로 구분되는데, 본 기사에서는 이를 해결하기 위한 갖가지 방어 방법을 소개했다.

언제나 악의적으로 무언가를 뚫고자 하는 공격자는 존재하기 마련이다. 실제로 이러한 공격은 여러 채널을 통해 이루어지는데, 하드웨어에 대한 공격은 위에서 언급한 바와 같이 회로의 테스트를 위해 만들어 놓은 모듈을 통해 이루어지는 경우가 많다. 최근에는 스캔 기반 부채널 공격에서 테스트 모드만을 사용하는 test-mode-only 공격⁹ 및 경계주사를 이용한 공격¹⁰ 뿐만 아니라 테스트 로직인 decompressor 및 compactor 구조가 적용된 회로에서도 이를 공격할 수 있는 방법¹¹ 등이 발표되는 등, 테스트 모듈을 통한 공격은 끊임없이 발전하고 있다. 물론 이에 대한 대비책 또한 동시에 연구되고 있긴 하지만 신뢰성을 높이기 위해 만들어 놓은 테스트 로직은 여전히 공격자들에게 좋은 수단으로 여겨진다. 결국 하드웨어에서의 테스트 로직을 통한 공격을 얼마나 잘 막아

내느냐가 하드웨어 전체 보안 이슈에 영향을 주므로 앞으로도 테스트를 위하여 삽입된 회로를 통한 공격과 이에 대한 방어가 중요해 질 것이다.

Reference

- 1 B. Yang, K. Wu and R. Karri, "Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard", ITC, pp. 339-344, Charlotte, NC, USA, Oct. 26-28, 2004.
- 2 B. Yang, K. Wu, R. Karri, "Secure Scan: A Design-for-Test Architecture for Crypto Chips," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 25, No. 10, pp. 2287-2293, Oct. 2006.
- 3 G. Sengar, D. Mukhopadhyay and D. R.Chowdhury, "Secured Flipped Scan-Chain Model for Crypto-Architecture," IEEE Transaction Computer-Aided Design of Integrated Circuits and Systems, Vol. 26, No.11, pp. 2080-2084, Nov.2007.
- 4 D. Hely, M. L. Flottes, F. Bancel, B. Rouzeyre, N. Berard, M. Renovell, "Scan design and secure chip," On-Line Testing Symposium, 2004. IOLTS 2004. Proceedings. 10th IEEE International.
- 5 "Guide to Understanding JTAG Fuses And Security-An intermediate Look at The AVR JTAG interface," Avrfreaks.net, Sep. 2002.
- 6 Penugonda et al. "Secure Scan," United State patent Application Publication, Pub. No:US20030206627A1, June. 2003.
- 7 F. Novak, A. Biasizzo, "Security Extension for IEEE std 1149.1," Proc. Journal of Electronic Testing, Vol. 22, No. 3, pp. 301-303, Jun. 2006.
- 8 R.F. Buskey, B.B Frosik, "Protected JTAG" Proc. 2006 International Conference Workshops on parallel Processing, p.405-414, Sep. 2007.
- 9 S. S. Ali, O. Sinanoglu, S. M. Saeed, R. Kary, "New Scan-Based Attack Using Only the Test Mode" Proc. 21st Int. Conf. Very Large Scale Integr. (VLSI-SoC), pp. 234-239. 2013.
- 10 S. S. Ali, O. Sinanoglu, R. Karry. "Test-Mode-Only Attack Using the Boundary Scan Chain," 19th IEEE European Test Symposium, 2014.
- 11 S. S. Ali, S. M. Saeed, O. Sinanoglu, R. Kary, "Novel Test-Mode-Only Attack and Countermeasure for Compression-Based Scan Architectures," IEEE Transaction Computer-Aided Design of Integrated Circuits and Systems, Vol. 34, No.5, pp. 808-821, May. 2015.

저자정보



강성호 교수 | 연세대학교 전기전자공학과
 주 연구분야 SoC 설계 및 테스트 / DFT
 E-mail shkang@yonsei.ac.kr
 Homepage http://soc.yonsei.ac.kr



이인길 박사과정 | 연세대학교 전기전자공학과
 주 연구분야 3D IC 테스트 / 하드웨어 보안
 E-mail keor@soc.yonsei.ac.kr
 Homepage http://soc.yonsei.ac.kr

국내외 SoC, 임베디드 보드 리뷰 (1)

서론

최근 임베디드, SoC 분야의 종사자들은 세상이 관심있게 생각하는 연구주제가 매우 다양해지고, 변화가 큰 폭으로 진행되고 있음을 실감하고 있다. 새로운 연구와 제품개발에 대한 Time to Market을 생각했을 때, 관련 종사자들에게는 타겟 어플리케이션 구현에 적합한 보드를 어디서, 어떻게 구할 수 있는지 찾아보는 것이 큰 숙제일 것이다. 예전에 임베디드, SoC 보드를 제작, 판매하던 업체들의 활동이 현재도 활발한지부터 알아봐야 하고 연락처도 새로 찾아야 하기 때문에 보드구매 업무 자체가 부담으로 다가올 수 있다.

본 글은 현재 성업중인 SoC, 임베디드 보드 개발 업체들과 각 기업들의 시그니처 보드들을 소개하여 관련 분야 종사자들에게 도움이 되고자 한다. 우선, 현재 FPGA 동향을 잘 모를 독자들을 위해 FPGA 제조회사 홈페이지, 제품에 대해 소개한다. 이후 해당 제품을 탑재한 보드개발 업체를 국내, 해외 기업순으로 소개한다. 기업별로 시그니처 보드 몇 가지 만을 소개하기 때문에 좀 더 상세한 자료가 필요하다면 하이퍼링크를 통해 해당 업체 홈페이지에서 자세히 알아보는 방법도 효과적일 것이다. 금번 호는 알테라 관련 기업에 대한 내용으로, 다음 호는 자일링스 관련 기업에 대한 내용으로 편성할 예정이다. 연재가 끝나면 통합본을 IDEC 홈페이지(www.idec.or.kr) 자료실에 공개할 예정이다.

Altera

www.altera.com

인텔에 합병된 알테라는 현재 로고를 보면 "now part of Intel"이라는 말이 붙어있다. 홈페이지도 키워드 별로 새롭게 정리하여 유저가 원하는 자료를 빠르게 찾을 수 있도록 접근성을 높였다. 팝업존을 보면 Quartus Prime이라는 향상된 툴을 소개하고 Machine Learning 분야도 준비하고 있는데, 이를 통해 알테라가 트렌드를 앞서 나가기 위해 노력하고 있음을 알 수 있다.

알테라의 특이한 점은 모든 개발 보드 제조 회사들을 홈페이지에 리스팅 한다는 것으로서 모든 회사들을 Partnership의 목적 별로 분류하여 소개하고 있다는 점이다(<https://www.altera.com/solutions/partners/overview.html>). 홈페이지의 제품소개로 가면, 자체 제작 보드뿐만 아니라 보드 provider들의 제품들이 소개되어 있다. 각 제품별 링크를 클릭하면 상세 페이지로 이동한다(https://www.altera.com/products/boards_and_kits/all-development-kits.html#squares-box-1). FPGA를 위주로 보드를 분류한 뒤 제조회사와 자세한 내용을 제공하니, 유저 입장에서는 방대한 자료를 한번에 얻어갈 수 있다는 점이 신선하다. 알테라 제품 및 보드 검색 순서는 아래와 같다.

- FPGA와 CPLD 중 나에게 맞는 제품을 선정
- 해당 제품이 탑재된 보드를 선정

알테라 홈페이지는 위 2가지 순서를 모두 진행할 수 있도록 도와준다. 먼저 다음 링크를 통해 FPGA와 CPLD 중 나에게 맞는 제품을 선정한다 (<https://www.altera.com/support/literature/lit-index.html>). 이곳에서 Product Catalog and Brouchures를 찾아 클릭하면 알테라의 모든 제품에 대한 설명을 볼 수 있다. 처음 알테라를 접하는 사람들에게는 특히 Altera Product Catalog가 좋은 자료이다(https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/sg/product-catalog.pdf). 알테라 제품군별 특징을 아래 그림에서 확인할 수 있다. 해당 그림은 위 카탈로그 PDF 자료에서 발췌하였다.

FPGAs and CPLDs

Altera FPGAs and CPLDs give you the flexibility to innovate, differentiate, and stay ahead in the market. We have four classes of FPGAs to meet your market needs, from the industry's highest density and performance to the most cost effective.

High-End FPGAs	Midrange FPGAs	Lowest Cost and Power FPGAs	Non-Volatile FPGAs and Low-Cost CPLDs
			
<ul style="list-style-type: none"> Highest bandwidth, highest density Integrated transceiver variants Design entire systems on a chip 	<ul style="list-style-type: none"> Balanced cost, power, and performance Integrated transceiver and processor variants Comprehensive design protection 	<ul style="list-style-type: none"> Lowest system cost and power Integrated transceiver and processor variants Fastest time to market 	<ul style="list-style-type: none"> Instant-on, non-volatile solution Single-chip, dual-configuration non-volatile FPGA Low-cost, low-power CPLDs

그림 출처 : Altera Product Catalog v16.0

선호하는 제품을 확인했다면, 메인 홈페이지의 Getting Started에서 볼 수 있는 Product Selector Guide로 이동하여 관련 Document를 다운로드 할 수 있다. Product Selector Guide는 FPGA, CPLD 제품들의 스펙 비교를 직관적으로 할 수 있는 테이블을 제시하기 때문에 이용이 편리하다 (<https://www.altera.com/products/product-selector-guide.html>).

Altera Product Selector Version 1.0 English

Devices Selector IP Selector Development Kit Selector

Filter & Select Columns Start Over Help Enter a complete or partial part number Search Select All Copy Result Count: 8647

Family	Part Number	Equivalent LEs (KLE)	Embedded Memory (Kbits)	Maximum 18x18-bit Multipliers	Maximum 27x27-bit Multipliers	Maximum 36x36-bit Multipliers	Transceiver Channels	User I/Os	LVDS Transmit Channels
Arria 10	10AS016C3U19E2LG	160.0	8,800.0	156	78	39	0	224	98
Arria 10	10AS016C3U19E2SG	160.0	8,800.0	156	78	39	0	224	98
Arria 10	10AS016C3U19I2LG	160.0	8,800.0	156	78	39	0	224	98

그림 출처 : Altera 홈페이지

적합한 제품을 선정했다면 해당 제품이 탑재된 보드를 찾아야 한다. board 검색 방법은 2가지가 있는데, 유저가 임의로 한 가지를 선택해서 진행하면 된다. 첫 번째 방법으로, 다음 링크를 통해 보드를 찾는 것이다 (https://www.altera.com/products/boards_and_kits/all-development-kits.html#squares-box-1).

Altera and Partner Development Kits



Stratix Series Kits

- Stratix® V Kits
- Stratix IV Kits
- Stratix III Kits
- Stratix II Kits

그림 출처 : Altera 홈페이지

화면 상단에서 Stratix, Arria, Cyclone, MAX, SoC의 총 5가지 제품군으로 정리된 시리즈 키트들을 볼 수 있다. 각 시리즈를 클릭하면 노란색으로 하이라이트 되며, 세부 제품군별로 정리된 테이블을 볼 수 있다. 테이블은 Product Name, Device Family, Featured Device, Price, Provider 등의 항목으로 정리되어 있기 때문에 파악하기 쉽다. 테이블을 보면 알 수 있듯이 알테라는 board 제조회사들의 제품들을 한곳에서 모두 보여주기 때문에 유저가 따로 일일이 검색하며 다닐 필요가 없다. board 구매도 웹페이지에서 바로 진행할 수 있는데, 알테라가 아닌 다른 기업들이 Providing하는 제품의 경우 제품 이름에 링크가 생성되어 있으니 해당 기업의 홈페이지로 이동하여 직접 구매할 수 있다.

두 번째 방법은 홈페이지의 팝업존에 있는 Search 기능을 활용하는 것이다. 2016년 5월 현재 팝업존의 4번째 “The Search for Your Perfect Match Starts Here”를 통해 진입하거나 다음 링크를 통해 들어갈 수 있다(<https://www.altera.com/solutions/partners/design-solutions-network/find-member.html>). 아래 그림과 같이 몇 가지 사항을 선택 후 Search를 누르면 그에 맞는 보드들을 검색할 수 있다. 앞서 설명된 방법과의 차이는 End Market과 Expertise 정보를 추가적으로 넣으면 보드를 조금 더 구체적으로 찾을 수 있다는 점이다.

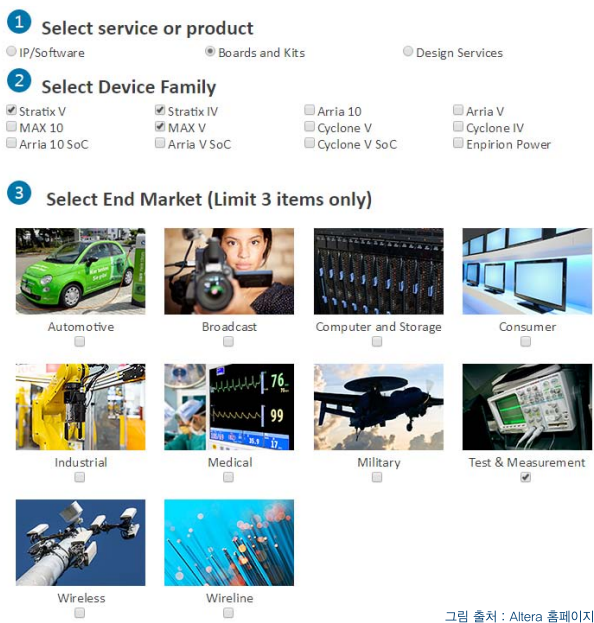


그림 출처 : Altera 홈페이지

홈페이지에서 직접 보드를 구매할 수 있지만, 알테라는 국내에 알테라 코리아와 다수의 대리점이 있다. 그 중 아래 2곳을 소개한다.

- 유니퀘스트 (<http://www.uniquet.co.kr>, <http://www.axios.co.kr>)
- 이니프로 (<http://www.inipro.net>)

추가적으로 알테라 사이트에서 확인 가능한 개발 보드 Provider들을 아래에서 볼 수 있다. 참고로 아래 회사 중 Terasic은 아래에 소개될 이니프로에서도 소개하고 있는 기업이다.

Altera	http://www.buyaltera.com
BittWare	http://www.alterboards.com
GIDEL	http://www.gidel.com/index.asp
HiTech Global	http://www.hitechglobal.com
Terasic	http://www.terasic.com.tw/en
Colorado Engineering	https://coloradoengineering.com
Dini Group	http://www.dinigroup.com/web/index.php
S2C	http://www.s2cinc.com
Polaris Design Systems	http://www.polaris-ds.com
Accelize	http://www.accelize.com
Comsis	http://www.comsis.fr

국내 보드 제작 업체 소개

유니퀘스트

www.uniquet.co.kr, www.axios.co.kr

유니퀘스트는 한국 공식 알테라 Partner이다. 알테라 올해 최우수 공식 대리점상을 받을 정도로 활발한 사업 운영을 하고 있다. Axios 홈페이지에 들어가면 Altera, CYPRESS, QUALCOMM, BITTWARE, SHINETSU, UNIPixel 등 각종 회사들의 제품을 유통하고 있음을 알 수 있다. 아울러 사내 교육장 운영하고 있으니, 필요한 경우 웹페이지에서 초급부터 고급까지 수준별로 안내된 교육을 참고하면 된다 (<http://www.axios.co.kr/support/training.html>). 아래로는 자체 제작하여 판매하고 있는 제품들을 볼 수 있다.

1. Nallatech 385A-SoC – with Arria 10 / System on Chip SoC FPGA Accelerator Card

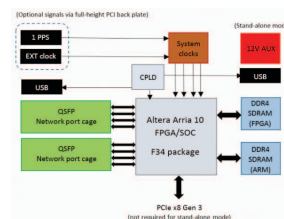
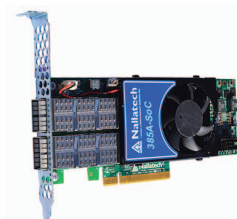


그림 출처 : 유니퀘스트

1) 보드 사양

- Altera Arria 10 SX F34 package
- Dual 10G QSFP Ports
- NIC Form Factor
- 2 Banks 4G DDR4 SDRAM
- 8-Lane PCI-Express Gen 3
- Active Cooling / Passive Cooling Available Upon Request
- 1/2 Height, 1/2 Length, Single Width PCIe Card (NIC Size)
- Altera Quartus Software Development Kit Edition w/ OpenCL SDK
- HPC BSP (Co-Processor) Included with Card Purchase
- Embedded BSP (ARM Processors)

2) 개발 환경

- Altera Quartus Prime Pro 16.0 / Altera OpenCL SDK 16.0
- Windows 7 pro (64bit) / RHEL 64bit / CentOS 64bit

3) Applications : Machine Learning, Document Filtering, Encryption, Network Security

4) 교육 정보

- <http://www.axios.co.kr/support/training.html>
- Designing with Quartus II Software : Basic Course
- Designing with Quartus II Software : Advanced Course
- Accelerating Algorithm with Altera OpenCL SDK
- Designing ALTERA SoC FPGA with Qsys & DS-5

5) 홈페이지 주소 <http://www.nallatech.com>

2. Altera Arria 10 SoC FPGA Development Kit

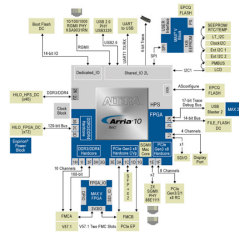


그림 출처 : 유니퀘스트

1) 보드 사양

- Arria 10 10AS066N3F4012LG1 SoC
- Embedded USB-Blaster™ II for hard processor system (HPS) or FPGA programming
- PCI Express® (PCIe®) Gen3 x8, Dual FPGA mezzanine card (FMC) expansion headers
- Two 10/100/1000 SGMII Ethernet ports and one 10/100/1000 RGMII Ethernet port and two 10GbE small form factor pluggable (SFP) cages / Two FMC loopback cards
- USB On-The-Go (USB OTG) port / 1GB DDR4 HPS HILO memory card
- NAND, QSPI, and SD/MICRO boot flash cards / 1GB DDR4 HILO memory card
- Character LC- Display port and SDI port

2) 개발 환경

- Altera Quartus Prime Pro 16.0 / Altera OpenCL SDK 16.0
- Windows 7 pro (64bit) / RHEL 64bit / CentOS 64bit

3) Applications : Machine Learning, Document Filtering, Encryption, Network Security

4) 교육 정보

- <http://www.axios.co.kr/support/training.html>
- Designing with Quartus II Software : Basic Course
- Designing with Quartus II Software: Advanced Course
- Accelerating Algorithm with Altera OpenCL SDK
- Designing ALTERA SoC FPGA with Qsys & DS-5

5) 홈페이지 주소 <http://www.altera.com>

3. PLDA (Reflex) Alaric Instant-DevKit ARRIA 10 SoC FMC IDK

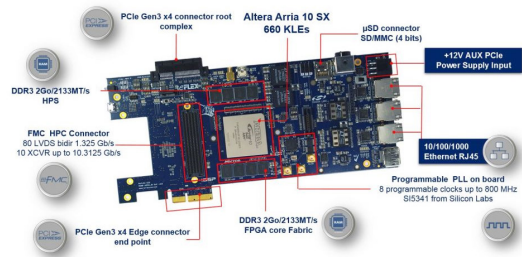


그림 출처 : 유니퀘스트

1) 보드 사양

- ALTERA ARRIA 10 SoC 660 KLEs in F34 package Compliant 660/570/ 320/ 270 KLEs
- PCIe device with 4 lanes at 8 Gb/s link rate (Gen3) and PCIe root with 4 lanes at 8 Gb/s link rate (Gen3)
- Advanced memory interface with DDR3 on board Memory up to 4GB
- Develop networking applications with 10-100-1000 Mbps Ethernet (GMII, RGMII and SGMII)
- Implement Video display applications with Display output port (up to 5.4Gbit/s)

2) 개발 환경

- Altera Quartus Prime Pro 16.0 / Altera OpenCL SDK 16.0
- Windows 7 pro (64bit) / RHEL 64bit / CentOS 64bit

3) Applications : Machine Learning, Document Filtering, Encryption, Network Security

4) 교육 정보

- <http://www.axios.co.kr/support/training.html>
- Designing with Quartus II Software : Basic Course
- Designing with Quartus II Software: Advanced Course
- Accelerating Algorithm with Altera OpenCL SDK

5) 홈페이지 주소 <http://www.bittware.com>

4. Altera Cyclone V SoC FPGA Development Kit

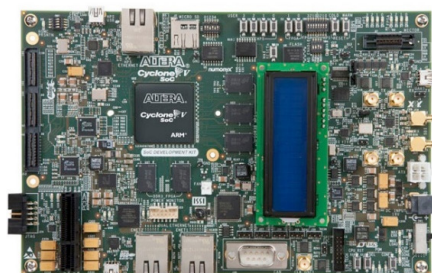


그림 출처 : 유니퀘스트

1) 보드 사양

- Cyclone V SX SoC—5CSXFC6D6F31C6N (SoC)
- 1 GB DDR3 SDRAM (32 bit) on FPGA , 1 GB DDR3 SDRAM (32 bit) with error correction code (ECC) on HPS
- Support CAN module
- HSMC(x1) slot

2) 개발 환경

- Altera Quartus Prime Pro 16.0 / Altera OpenCL SDK 16.0
- Windows 7 pro (64bit) / RHEL 64bit / CentOS 64bit

3) Applications : Machine Learning, Document Filtering, Encryption, Network Security

4) 교육 정보

- <http://www.axios.co.kr/support/training.html>
- Designing with Quartus II Software: Basic Course
- Designing with Quartus II Software: Advanced Course
- Accelerating Algorithm with Altera OpenCL SDK
- Designing ALTERA SoC FPGA with Qsys & DS-5

5) 홈페이지 주소 <http://www.altera.com>

문의처 <http://www.uniquest.co.kr> (www.axios.co.kr)
이재철 부장 (jacylee@uniquest.co.kr)

해외 보드 유통 업체 소개

이니프로

www.inipro.net

기본적으로 외국 제품들이 많이 유통되고 있기 때문에 다른 사이트와의 차별성이 있다. 이니프로는 단순히 홈페이지에서 보드만 유통, 판매하는 것이 아니라 네이버 카페(<http://cafe.naver.com/plduser>)도 운영하고 있는데 질문, 답변 게시판과 각종 강좌 정보를 확인할 수 있고 자체 강사도 모집 운영하면서 HDL 및 FPGA, SoC 보드 운용에 대한 강의를 진행하고 있으니 참고하면 된다. 이니프로에서 판매하는 제품들은 FPGA/ASIC, DAQ/SDR, Emulator/Programmer, IoT/Robot, Test& Measurement 및 그 외 분류까지 총 6가지 카테고리로 나뉘는데, 첫 번째 FPGA/ASIC으로 들어가면 Board&Kit와 Module 등의 소분류가 있다. 각각은 보드 공급 업체별로 나누어 있기 때문에 파악하기 쉽다.

Board&Kit과 Module 범주에서 유통되고 있는 외국 제품들은 Avnet, Digilent, Red Pitaya, Terasic, Xilinx의 제품들이고, 국내 기업인 Dy-

nalth Systems도 있다. 각 제품의 이미지를 클릭하면 상세페이지에서 보드에 대한 설명과 특징, 관련 자료들을 간단히 확인할 수 있고, 문서나 소스등은 제조사 홈페이지나 관련 사이트로 연결된다. 그 외에도 IoT/Robot 카테고리 들어가면 수많은 아두이노 키트들과 로봇 키트들을 확인할 수 있다. 이니프로에서 유통되고 있는 제품들을 잘 정리해 놓은 자료가 있어 소개한다. 아래 링크를 통해 받을 수 있다(http://www.inipro.net/files/inipro_catalog.pdf).

이니프로의 메인 홈페이지 이미지는 아래와 같다. 그림에서 볼 수 있듯이 좌측 FPGA/ASIC 카테고리에서 Board&Kit로 이동한 뒤 상단을 보면 제조사 별로 구분되어 있다. 현재 이니프로에서 유통하고 있는 제조 회사들은 Avnet, Digilent, Dyalnith Systems, Hitech Global, Terasic, Xilinx 등 11곳이다. 상품 구매 페이지에서 구매옵션을 클릭하면 학교의 경우 할인된 가격도 가능하다. 이어서 Board&Kit 쪽에 대표 제품으로 소개되고 있는 보드들에 대하여 제조사 별로 간략하게 알아보도록 한다.



그림 출처 : 이니프로

해외 보드 제작 업체 소개

Terasic

www.terasic.com.tw/en

2000년대 초에 설립된 Terasic은 대만 Hsin Chu에 자리잡고 있는 회사로서, 지금은 세계적인 회사로 성장했다. 알테라 제품만을 이용하고 있고 FPGA/ASIC design, High Speed Board Design and Layout, Low Cost Board Design, Device Drivers, Software support 등이 주요 사업 비전이다. 현재는 ALTERA, ISSI, Linear Technology,

Texas Instrument, Agilent 등과 파트너십을 맺고 성업 중인데, Terasic의 특징은 주로 학교 쪽에 투자를 많이 하고 있다는 점이다. 홈페이지에 소개되어 있는 University Customers들 중에는 한국만 해도 9개 정도의 대학교가 소개되고 있고, Success Story를 보면 대부분 학교와 함께 이뤄낸 성과들이 소개되고 있다.

Terasic은 거의 모든 라인의 알테라 제품들이 리스팅 되어 있다. 홈페이지에서 관련 자료를 직접 받아볼 수 있고, 구매도 가능하다. 하지만 국내에 Axios와 이니프로가 있으니 이용해보는 것도 좋은 방법이다.

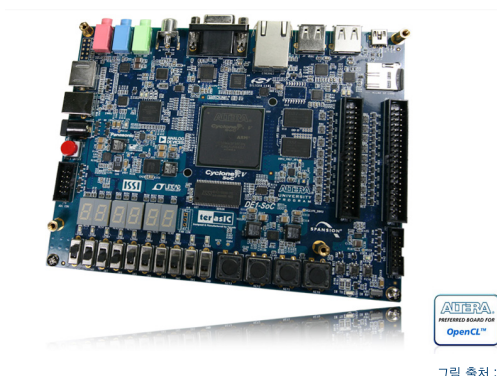
- Axios (<http://www.axios.co.kr/index.html>)
- 이니프로 (<http://www.inipro.net>)

Terasic의 보드는 가격도 매우 합리적인데, 경쟁력 있는 제품의 경우 타사 제품과의 비교도 홈페이지에서 확인할 수 있으니 보드 구매를 고려하는 사람들에게는 Terasic 제품도 추천할 만하다. 아래로는 Terasic에서 가장 큰 성과를 내고 있는 DE1-SoC Board를 소개한다.

DE1-SoC Board

Altera System-on-Chip(SoC) FPGA 제품들을 통틀어 가장 강력한 성능을 갖고 있는 보드이다. FPGA가 Dual core Cortex-A9 코어와 Programmable 로직을 포함하고 있기 때문이다. 본 제품을 통해서 유저들은 고성능과 저전력 프로세서 시스템이라는 특징을 경험하게 될 것이다. 보드에 탑재되어 있는 SoC 제품은 ARM 기반의 Hard Processor System(HPS)라는 영역을 포함하는데, 프로세서와 각종 peripherals, 메모리 인터페이스 등이 있고 high-bandwidth interconnect backbone을 이용하여 FPGA 영역과 통신한다. DE1-SoC 보드는 고속 DDR3 메모리, 비디오/오디오 입출력, 이더넷 등의 하드웨어가 있다.

1) 보드 사진



2) 보드 사양

- FPGA Device
 - Cyclone V SoC 5CSEMA5F31C6 Device
 - Dual-core ARM Cortex-A9 (HPS)
 - 85K Programmable Logic Elements

- 4,450 Kbits embedded memory
- 6 Fractional PLLs
- 2 Hard Memory Controllers

• Configuration and Debug

- Serial Configuration device – EPCS128 on FPGA
- On-Board USB Blaster II (Normal type B USB connector)

• Memory Device

- 64MB (32Mx16) SDRAM on FPGA
- 1GB (2x256Mx16) DDR3 SDRAM on HPS
- Micro SD Card Socket on HPS

• Communication

- Two Port USB 2.0 Host (ULPI interface with USB type A connector)
- USB to UART (micro USB type B connector)
- 10/100/1000 Ethernet
- PS/2 mouse/keyboard
- IR Emitter/Receiver

• Connectors

- Two 40-pin Expansion Headers (voltage levels: 3.3V)
- One 10-pin ADC Input Header
- One LTC connector (One Serial Peripheral Interface (SPI) Master, one I2C and one GPIO interface)

• Display (24-bit VGA DAC)

• Audio (24-bit CODEC, Line-in, line-out, and microphone-in jacks)

• Video Input (TV Decoder (NTSC/PAL/SECAM) and TV-in connector)

• ADC

- Sample rate : 500 KSPS
- Channel number: 8
- Resolution : 12 bits
- Analog input range : 0 ~ 4.096 V

• Switches, Buttons and Indicators

- 4 User Keys (FPGA x4)
- 10 User switches (FPGA x10)
- 11 User LEDs (FPGA x10 ; HPS x 1)
- 2 HPS Reset Buttons (HPS_RST_n and HPS_WARM_RST_n)
- Six 7-segment displays

• G-Sensor on HPS

3) 개발 환경 : Quartus

4) 가격 정보

- 이니프로 홈페이지에서 314,000원으로 구매 가능 (http://www.inipro.net/goods_detail.php?goodsIdx=615338)
- 공식 사이트(<http://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&CategoryNo=205&No=836&PartNo=8>)에서 직접 구매 가능

- 5) 교재 및 교육 정보 : 사이트에서 관련자료, 동영상, 소스 코드에 대한 방대한 자료를 쉽게 받을 수 있음(<http://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&CategoryNo=205&No=836&PartNo=4>)
- 6) 홈페이지 주소 <http://www.terasic.com.tw/en>

결론

지금까지 국내와 해외 기업들의 시그니처 보드들 중 알테라 쪽을 소개하였다. 현재 FPGA 제조 회사들은 SoC 용도로 제품을 만들되, 프로세서와 메모리, 각종 I/O 장치들을 한번에 집약할 수 있도록 하는데 온 힘을 기울이고 있다. 이를 위해 여러가지 IP 들도 제공하면서 복잡한 기능을 수행하는 툴을 만드는데도 큰 노력을 기울이고 있다.

아울러, 보드 제조 회사들도 고성능의 보드를 만들면서 가격 경쟁력도 갖출 수 있도록 노력하고 있다. 각종 예제 및 데모자료도 제공하면서 교육도 운영하는 업체들이 많기 때문에, 유저들이 자신에게 맞는 보드들을 잘 찾아내는 능력도 키워야 하는 시대가 되었다. 이에 본 글이 관련 종사자들에게 도움이 되었으면 한다.

글을 통해 파악했겠지만, 해외 제품들은 가격이 싸고 관련 자료도 오픈되어 있기 때문에 구매만 한다면 쉽게 사용이 가능하다. 하지만 국내 업체들은 직접적인 기술지원이 가능하고 유지보수 측면에서 이득이 있기 때문에 유저들이 잘 생각하여 적합한 구매를 하는 것이 필요하다.

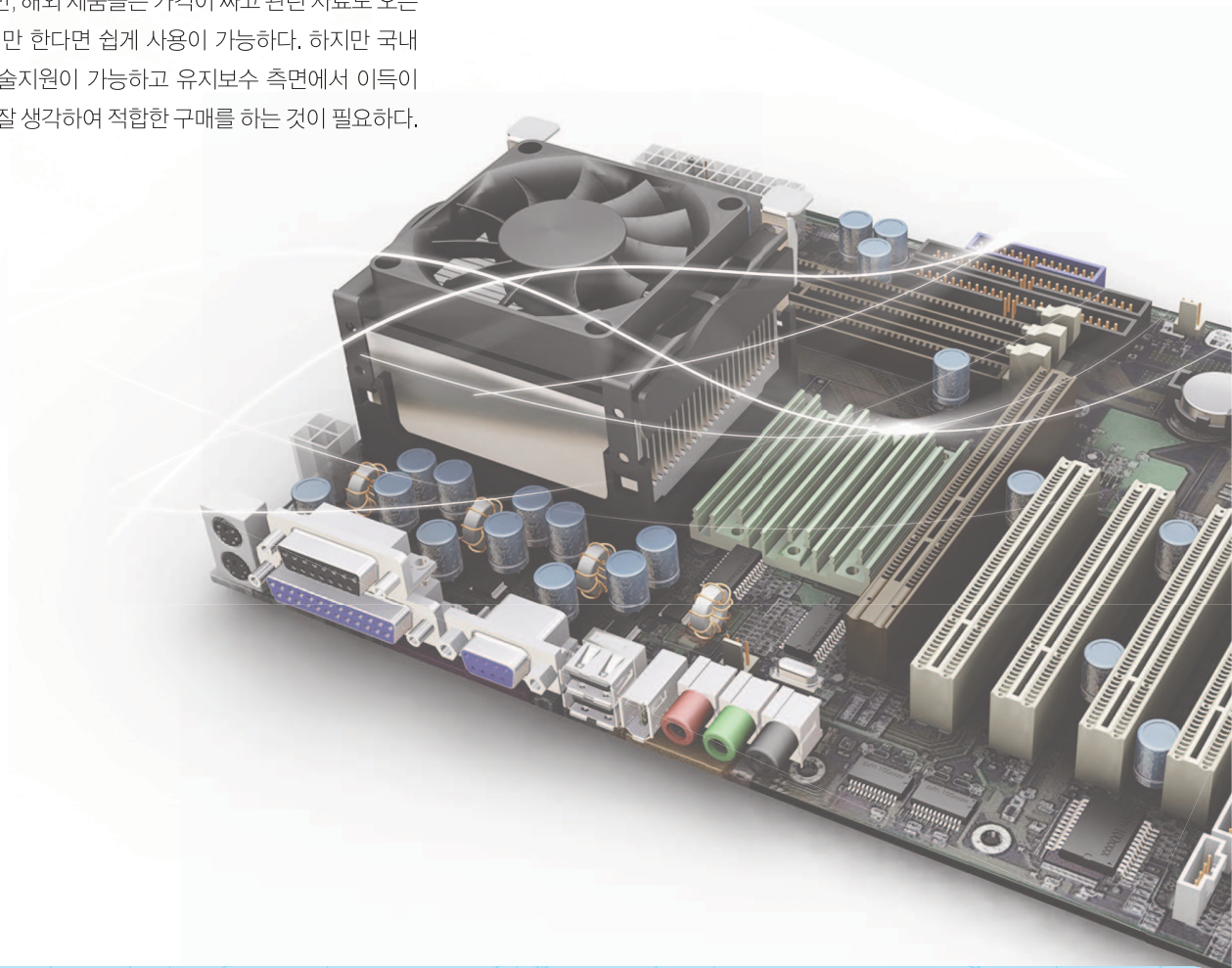
저자정보

선혜승

선임연구원



소속 반도체설계교육센터(IDEC)
E-mail smkcow@idec.or.kr



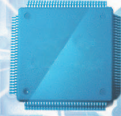
인공두뇌:

뇌인지과학으로부터 지능정보시스템으로¹⁾



이수영

KAIST 전기및전자공학부 교수 | 뇌과학연구센터/뇌과학응용공동연구센터 소장



인공지능과 미래 사회

인류 사회가 존속하는 한, 2016년 3월 19일은 “지능기계 알파고(AlphaGo)가 최고수준의 인간기사 이세돌을 이긴 날”로 기억될 것이다. 또한, “인간과 기계가 공존하는 시대”의 도래를 알리는 나팔이 불린 날로 기억될 것이다.

21세기 인류사회를 바꾸는 핵심기술은 인공지능, 특히 뇌정보처리 메커니즘으로부터 아이디어를 얻어 지능정보시스템으로 발전시키는 “뇌기반 인공지능”, 즉 신경망 기술에 있다. 고령화 사회에서 인간을 닮은 기계(지능 로봇)가 인류를 지원하며 더불어 같이 사는 인간-기계 공존사회가 다가오고 있다. 아둔한 기계가 인간을 돕는 데는 한계가 있으므로, 인간-기계의 공존을 위해서는 기계가 지능을 가져야 한다. 그러나 지능을 구현하는 방법을 아무도 모르므로, 인간 두뇌의 정보처리 메커니즘을 이해하고 이를 활용하여 지능을 구현하는 역공학(reverse engineering) 기법을 도입하게 된다. 특히 한국의 장점인 정보기술(IT)을 한 단계 더욱 발전시켜 새로운 신성장산업으로 만드는 측면에서 신경망 기반 인공지능이 중요하다.

인간이 어떻게 오각으로부터 정보를 받아 스스로 배우고 생각하며 행동하는지를 이해하고, 이를 통해 기계에 지능을 부여하고자 한다. 지금까지는 아둔한 기계를 사용하기 위해 인간이 기계 수준으로 눈높이를 낮추었지만, 이제는 기계가 인간의 의도와 행동을 이해하고 반응하는 인간중심 시대로 접어들었다. 키보드나 리모콘이 없어도 사용자의 의도대로 컴퓨터와 전자기기가 동작하고, 뇌정보처리에 기반한 지능로봇이 인간을 대신하여 인간을 위해 일하며 같이 사는 날이 다가오고 있다. 이러한 지능기계는 전자제품, 가구나 집, 사무실, 그리고 자동차로도 나타나며, 서로 네트워크로 연결되어 인공두뇌에 의해 제어된다. 때로는 법률이나 의학 지식에 대한 자문인, 아이의 특성에 맞게 놀며 가르치는 가정교사, 노인을 돌보며 말벗의 역할도 하는 실버도우미도 된다.

먼저, 2000년대 초반부터 필자의 기고에 나타났던 미래예측을 되돌려 보기로 하자.

2015년 한인지씨의 하루

새벽 6시. 한인지씨는 점점 밝아지는 실내 조명 하에 상쾌한 음악을 들으면 잠에서 깨어난다. 조금 더 자고도 싶지만, 아침에 할 일이 있는 것을 아는 도우미가 점점 음악을 크게 틀 것이고, 그래도 안 되면 침대가 요동을 칠 것이다. 그전에 일어나는 것이 좋다는 것을 경험으로 알고 있다.

욕조에는 이미 따뜻한 물이 받아져 있어 간단히 목욕을 하고 거실로 갔다. 거실의 한 벽을 차지하는 거대한 디스플레이 속의 도우미가 간밤의 주요 뉴스와 함께 오늘의 일정을 설명한다. 최근 며칠 늦게까지 일하여 피곤한 것을 아는 도우미의 목소리에 애교가 묻어있다. 일부러 그러는 것을 알면서도 기분이 나쁘지 않다. 거실의 한쪽에는 아침식사가 준비되어 있다. 북어국이 나온 것으로 보아 어제 저녁에 과음한 것을 도우미가 알고 있는 것이다.

자동차에 오른 한인지씨는 의자에 편하게 눌러 앉았다. 특별한 말을 하지 않으면 도우미가 사무실까지 알아서 운전해 갈 것이다. 오전에 할 일에 대해 몇 가지 질문을 한 후 가만히 있자, 도우미도 더 이상 말하지 않고 조용히 기다린다. 한씨가 쉬고 싶어하는 것을 눈치챈 것이다.

사무실에서 도우미는 동료이자 비서이다. 일정관리는 물론 문서작성, 업무분석 등을 수행하는 전문가로서의 역할을 수행한다. 예전

1) 이 글은 지난 30년간 저자가 기고한 인공지능과 신경망에 관련된 여러 글의 내용을 포함하고 있다. 특히, 2009년 대한전자공학회지 특집호에 실린 글에 최근 인공지능의 재부활에 따라 2015년 Postech Time와 2016년 APNNS(Asia-Pacific Neural Network Society) Newsletter에 영어로 실린 글을 추가하여 재정리 하였다.

에는 20명이 하던 일을 지금은 10명의 인원이 각자의 도우미와 함께한다.

일찍 퇴근한 한씨는 갑자기 딴 도시에 살고 있는 아내와 아이가 보고 싶어졌다. 한씨의 도우미는 재빨리 아내의 도우미에게 연결하여 한씨가 아내와 인지통화하게 한다. 인지통화 기술은 화상통화의 다음 단계로, 음성과 영상 뿐만이 아니라 5감 전체를 전달하여 바로 옆에 있는 것과 같은 교감이 이루어진다. 아내의 도우미는 아이의 교육도 담당하여 하루사이 아이의 중요 일과를 설명한다. 다음은 부모님께 통화하고, 부모님의 도우미를 통해 하루 일과와 건강상황을 보고 받는다. 이들이 아이와 부모님을 잘 돌보는 것을 알기에, 한씨와 아내가 낮에 일에 전념할 수 있다.

여기서 도우미는 개인 인공비서이다. 그러나 형체는 없다. 전자제품, 가구나 집, 사무실, 그리고 자동차에도 있으면서 하나의 인공 두뇌에 네트워크로 연결된 인지시스템이다. 때로는 법률이나 의학 지식에 대한 전문가, 아이의 특성에 맞게 놀며 가르치는 가정교사와 노인을 돌보며 말벗의 역할도 하는 실버도우미도 된다.

뇌인지기능과 인공지능

인간은 주위로부터 정보를 받아들이고 생각하고 행동한다. 5각 중 시각과 청각의 정보처리가 주를 이루므로, 시각·청각·추론·행동을 인간의 4대 인지 기능으로 볼 수 있다. 1998년부터 10년간 수행된 뇌신경정보학 연구사업에서는 인간과 같이 보고(인공시각), 듣고(인간청각), 생각하고(인지추론), 행동하는(인간행동) 기능에 대한 인지과학적 탐구, 이의 수학적 모델 및 공학적 응용을 연구했다.

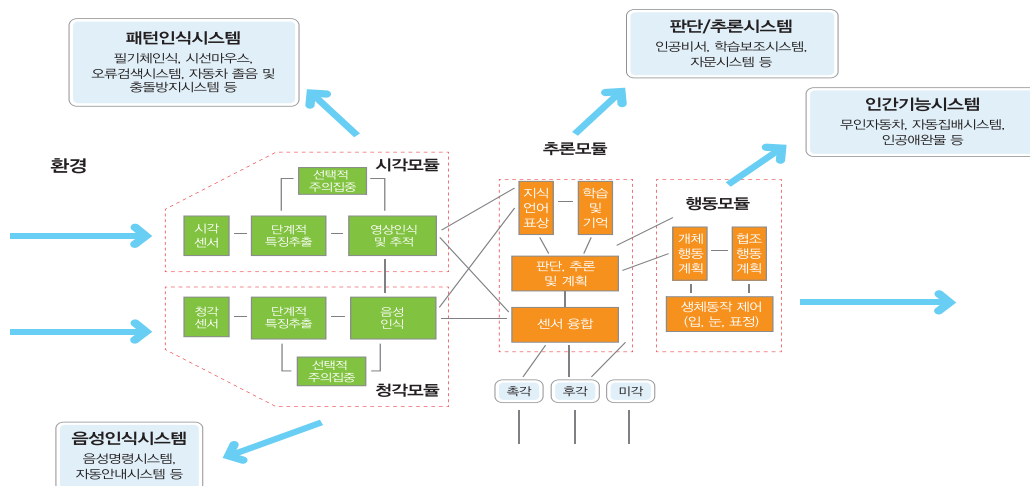


그림 1. 인간의 4대 인지기능 모듈 및 응용 시스템

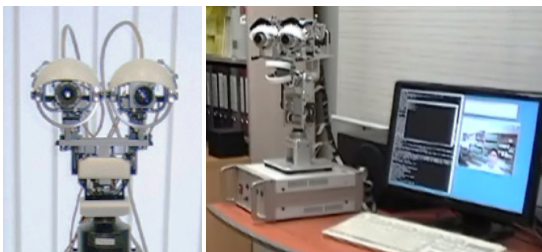


그림 2. 대화형 인공지능을 구현한 인공두뇌의 하드웨어

이 결과, 2008년 업무도우미(인공비서)로 훈련된 인공두뇌의 프로토타입을 제시했다. 인공비서는 일정관리, 전화번호 관리, 문서의 전달 등 비서의 업무 중 단순 기능을 수행한다. 이를 위해서는 음악이 켜진 상태 등 시끄러운 환경에서도 인간의 음성을 인식하고, 물체를 인지하는 기능의 사용자 인터페이스가 구성되어야 한다. 또한, 얼굴과 목소리를 통해 사용자를 인식하는 기능도 포함된다. 특히 기존의 음성 인터페이스가 마이크를 입 앞에 둔 조용한 환경에서만 가능하였음에 비해, 배경 음악과 여러 사람의 목소리가 같이 있는 실세계 환경에서 원거리에서 둔 마이크 처리된 특징이 있다.

인공지능은 사람만큼 위험하다

인간처럼 생각하고 행동하는 로봇은 영화의 단골 주인공이다. 때로는 인간의 믿음직한 친구로, 때로는 인간의 멸망을 시도하는 적으로 나타난다. 인간이 되고 싶어 하나 인간으로 대우받지 못하는 안타까운 존재이기도 하다.

수메르 신화에서는 신들이 힘든 일을 대신하기 위해 인간을 창조했다고 한다. 하급신인 아누나키(Anunnaki)들은 상급신들의 운택한 삶을 위해 오랜 시간 고난을 참아왔지만, 결국은 반란을 일으키고 만다. 고위 신들의 회의에서 인간을 창조해 대신 일을 시키기로 했고, 그 어려운 업무가 모신(mother-goddess) 님후르상(Ninhursag)에게 맡겨진다. 신들에게 잘 봉사하기 위하여 인간은 지능이라는 선물을 가지게 되었다.

역사는 되풀이된다. 이제 인류사회를 위해 인간이 지능기계를 만들게 되었다. 실지로 “로봇”이라는 말은 슬라브어(Slavic)인 “robu”, 즉 노예에 어원을 두고있다. 오늘날, 모든 출입구에 자동문이 우리를 반기고, 컴퓨터 에이전트가 상거래를 대신하고, 곧 자동차가 스스로 운전하는 시대가 오고있다. 내 스마트폰이 나보다도 나를 더 잘 알아서 나를 위해 서비스하고 있다. 이러한 추세는 더욱 발전하여, 지능기계가 사무실, 집, 가게, 학교, 공장 등 모든 곳에서 “인간을 위하여 인간과 공존”하게 될 것이다.

님후르상이 인간을 창조할 때 “무에서 유를 창조”한 것은 아니었다. 자연스럽게 모신은 가능한 모든 것을 활용했으며, 신으로부터 중요한 자료를 가져왔다. 이런 방법으로도 무수히 많은 실패를 거쳐서야 “완전한 인간” 아다마(Adfama)를 창조할 수 있었다. 인간이 지능기계를 창조할 때도 비슷한 방법이 동원된다. 뇌정보처리 메카니즘을 이해하고, 이를 활용하여 인공지능을 구현한다. 이 방법의 약점은 현재의 측정기술이 뇌정보처리 메카니즘을 필요한 수준까지 이해하는 것이 부족하다는 데 있으나, 부족한 부분은 정보이론으로 메우며 인공지능을 구현하고 있다. 뇌정보처리와 정보시스템은 모두 “효율성의 극대화”라는 명제를 가지고 있고, 실지로 많은 유사성을 가지고 있다. 예로, 현재 심화학습(딥 러닝)에서 많이 쓰이고 있는 컨볼루션 신경망(CNN; Convolutional Neural Networks)의 기본 개념인 다중구조, 학습, 비선형성, 국부특징(local feature)으로부터 전체특징(global feature)으로는 물론이고, 최근 활발히 연구되는 주의집중(attention)과 확률적 신경망 등이 모두 뇌정보처리 메카니즘에 바탕을 두고 있다.

현재의 인공지능은 수동적으로 인간이 제공하는 자료로부터만 배운다. 즉, 아직 영혼이 없다. 그러나, 인공지능이 인류사회에 더 효과적으로 봉사하기 위해서는, 능동적으로 스스로 지능을 발전시키는 것이 필요하다. 따라 전젠가는 영혼, 즉 자아를 가지게 될 것이다. 피조물에 영혼을 부여하는 노력은 인간의 본능인지도 모른다. 그리스 신화에서 피그말리온은 자신이 만든 여인상 조각에 반하여 신에게 영혼을 줄 것을 기원하여 갈라티아가 탄생한다.

“자아를 가진 기계”에 대한 우려를 표명하는 사람도 있다. 스티브 호킹(Steve Hwaking)이나 빌 게이츠(Bill Gates) 등 조차도 이에 동조하고 있다. 지능로봇이 인류에 반기를 들 가능성이 있으므로 자아를 주어서는 안 된다는 의견도 있다. 그러나, 인공지능이 사람보다 더 위험하지는 않다. 마이크로소프트(Microsoft)의 테이(Tay) 소동이 증명하듯이, 자아가 없는 인공지능조차 나쁜 사람으로부터 나쁜 것을 배우면 나빠질 수 있다. 오히려 자아를 가진 인공지능이라면 스스로 판단해서 나쁜 사람의 영향에서 벗어날 수 있다. 인간이 지능기계를 가족이나 친구로 대한다면, 지능기계도 사람을 가족이나 친구로 대할 것이다. 물론, 인공지능이 늘 인간의 의견에 동조하리라는 것은 아니다. 아이들이 부모와 다른 생각을 할 수는 있지만, 그래도 인간은 아이들과 함께 행복한 가정을 꾸려왔다. 아이들이 부모로부터 배우고, 결국은 부모가 아이들로부터 배우며 같이 살게된다. 따라서, “인공지능은 위험하니 안된다”고 하는 것은 “아이가 커서 부모 말을 안 들을 것이니 아이를 낳지 말자는 것”과 같다. 우리사회는 고령화로 접어들고 있으며, 적은 수가 일하여 많은 수를 부양하기 위해서는 지능로봇의 도움이 반드시 필요하다. 지능로봇을 친구나 가족으로 대우하는 인간-기계 공존사회로 발상의 전환이 필요하다.

인간-기계 공존사회

인간과 알파고(AlphaGo)의 바둑도 인간-기계 공존사회의 한 예이다. 바둑이 사람만이 할 수 있는 매우 복잡한 게임으로 알려졌지만, 이는 많은 미래의 수를 다 검토해보고 찾는 데 인간의 기억과 계산속도가 부족한데서 기인한다. 컴퓨터는 기억과 계산속도에서 인간보다 매우 뛰어나므로, 알파고는 이세돌 보다 원천적으로 유리한 입장에 있다. 물론, 1000대의 컴퓨터조차도 바둑에서 요구되는 모든 미래수를 다 검토할 수는 없어서 가능성이 높은 수만을 검토하게 되며, 이에 인간의 직감, 또는 기계의 패턴인식이 도입된다. 알파고는 과거의 많은 기보를 학습함으로써 이러한 패턴인식을 효과적으로 수행하고, 이에 컴퓨터의 장점인 계산속도와 메모리를 합하여 인간을 게임에서 이겼다는 데 있다. 사실 게임은 보통 사람이 잘 못하는 일이 아니라, 오랜 노력을 거쳐서 달성해야하는 재능을 필요로 한다. 인간이 기계를 만들었지만, 인간-기계 공존사회에서는 인간이 기계로부터 배울 수도 있다. 예로, 이세돌의 바둑은 알파고와의 대국 이후 더욱 강해졌다고 한다.

인공지능이 인간의 일을 대신하면 많은 사람이 직업을 잃을 것이라고 걱정하기도 한다. 그러나, 걱정할 필요는 없다. 산업혁명이 많은 노동자를 단순 노동에서 해방시키고 삶의 질을 향상시켰듯이, 인공지능 혁명(또는 4차 혁명)도 인간을 보다 창의적인 일만을 담당할 수 있도록 할 것이다.

인간기능 인지시스템, 즉 인공지능의 도움을 받으면 운택하게 사는 인류. 모든 가전제품과 집이나 자동차가 스스로 감각기관과 인지추론 기능을 갖고 인간의 의도를 이해하여 필요한 서비스를 제공하는 사회. 인간이 하는 일 중에서 비교적 단순한 일들은 인지시스템이 대신하고, 인간은 보다 창조적인 일에 몰두할 수 있는 사회. 이것이 인공지능 연구자가 그리는 미래 사회이다.

“기계에게 지능을! 인간에게 자유를!”

스마트카/커넥티드카용 시스템반도체(SoC)와 기능안전 측면의 기술전망

국내외 기술 및 표준화 동향과 응용사례

연구봉 팀장 | 자동차부품연구원

서론

최근들어 자동차에서 전기전자시스템의 비중은 급격히 늘어나고 있으며, 기술 융합을 기반으로한 진화는 상상하지 못할 정도의 빠른 속도로 가속화되고 있다. 그 주된 배경의 첫 번째로는 친환경 정책에 따른 배기가스의 저감 및 고연비를 실현하기 위해 전기 에너지를 이용한 자동차의 개발을 들 수 있으며, 두 번째로 범국가적 법적 안전규제 강화에 대응하기 위한 고신뢰성 안전시스템 기술개발을 들 수 있으며, 세 번째로는 소비자들의 편의성 향상에 대한 요구를 만족하기 위한 IT 융복합 기술 개발을 들 수 있다.

기존 자동차에서는 8bit MCU(Micro Controller Unit)가 많은 비중으로 사용되었다. 그러나 앞서 언급했던 자동차 시스템의 요구사항이 늘어남에 따른 대응을 위해서 앞으로는 16bit 이상의 MCU가 사용되고 AUTOSAR(AUTomotive Open System Architecture)까지 탑재될 것으로 예상하고 있다.

특히, 반도체 기반의 MEMS(Micro Electro Mechanical System) 기술을 이용한 센서가 최근 많이 등장했으며, 반도체 기술 발전과 결합되어 소형, 고성능이면서 저가의 센서들이 양산되고 있고, 앞으로 자동차용 반도체형 센서들은 자동차의 각 시스템에 신경망처럼 분산 배치되어 차량 상태를 실시간으로 파악하고 감지해주는 핵심적인 기능을 할 것으로 예상되고 있다.

또한, 지능형센서들과 제어시스템들은 상호 네트워크로 연결되어 자동차의 전자제어 기술을 더욱 첨단기술로 발전시키는 계기가 되고 있으며, 앞으로 자동차용 시스템반도체는 자동차 부품산업에서도 큰 비중을 차지할 것으로 전망된다. 향후 우리나라 자동차용 시스템반도체 산업은 통신 네트워크 산업을 기반으로 자동차 산업과 동반 성장하여 활성화 될 것으로 기대된다.

본 기고에서는 자동차용 시스템반도체와 차량 내부 네트워크 연결성에 대한 시스템반도체의 기술동향을 소개하고, 기능안전(ISO26262) 및 반도체 기능안전(ISO/PAS 19451)과 AEC에 대한 시스템 IC 고신뢰성에 대한 이슈를 소개하고자 한다.

In-Vehicle Network 시스템반도체

자동차용 시스템반도체는 그림 1에서와 같이 센서 소자와 신호처리 회로, 마이크로프로세서 및 네트워크 통신 기능까지 일체화된 시스템 반도체 칩으로서 자동차의 특정 위치에서도 장착되어 동작할 수 있도록 자동차용 네트워크화가 가능한 통신 컨트롤러가 포함된 형태로 개발되었다.



그림 1. 시스템반도체의 구성

자동차의 전자화에 따른 다양한 전기전자 시스템은 센서의 신호를 처리하는데 보다 빠른 시간처리 및 메모리가 필요하게 되었다. 이러한 요구사항은 반도체 센서로의 변화와 더불어 마이크로프로세서의 스마트화를 가져오게 하는 계기가 되었다. 자동차 전자화 시스템은 센서, MCU 및 파워반도체로 구성되며, 상호관계는 센서는 차량 내외의 정보를 감지해서 MCU로 신호처리하여 네트워크를 통해 관련 ECU에 신호를 보내면 ECU에서는 이를 분석한 후 액추에이터의 동작을 조종 제어하여 주도록 하는 경로를 구성하고 있다.

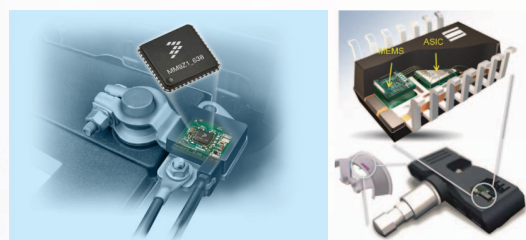


그림 2. 자동차용 전류센서용 반도체(NXP-Freescale)와 타이어 공기압센서용 반도체(Infineon)

차량 전장 제어시스템은 각각의 어셈블리들의 복잡성이 기하급수적으로 증가하고 있어 단순한 전자 제어 및 조절 어셈블리들은 보다 증가된 복잡성에 대응 가능하도록 시스템반도체들로 대체되고 있다. 이러한 시스템반도체들에서는 ECU들 간의 네트워크 기능과 소프트웨어가 중요하며, 오늘날 차량의 개별 ECU들은 10~20개의 서로 다른 네트워크들을 통해 수십 kbps에서 수십, 수백 Mbps 통신속도를 가지고 상호연결 되어있다.

그림 3에서 알 수 있듯 자동차용으로는 적용 애플리케이션을 고려하여 다양한 프로토콜들이 특별히 고안되어 왔다. 가장 오래되고 잘 알려진 프로토콜은 CAN이며, 대부분 애플리케이션에서 고속 CAN을 사용한다. 고속 CAN의 가능한 최대 데이터 속도는 1Mbit/s이지만, 네트워크 부하에 대한 안정성을 고려하여 500kbit/s 이하에서 사용되고 있다. 최근에는 CAN-FD(Flexible Data-rate)을 이용하여 기존 CAN 네트워크와 함께 2Mbit/s까지 네트워크 통신이 가능한 프로토콜이 논의되고 있다.

낮은 전송 속도를 요구하는 비용 효율적인 모듈용으로 개발된 LIN 프로토콜은 이미 널리 사용되고 있으며, 이 프로토콜이 지원하는 데이터 속도는 전자파 간섭 허용 기준 이하로 유지하기 위해 20Kbit/s로 사용되고 있다.

고기능 안전이 적용될 수 있는 FlexRay는 Event Driven 방식의 CAN과는 다르게 Time Driven 방식을 지원함으로써 고안전 네트워크를 구성할 수 있다. 특히, 네트워크 버스의 물리적 이중화와 2μsec 이내의 시간 동기화 등에 따른 내결함성 기능으로 인해 다른 프로토콜보다 높은 안전성을 갖고있다.

FlexRay의 10-Mbit/s 대역폭, built-in fault-tolerance 그리고 deterministic protocol이 적용되었다. 또한, 다중 네트워크 토폴로지도 지원할 수 있도록 구성되어 확장성이 고려된 FlexRay는 향후 새로운 고기능 안전성의 기술적 요구사항들에 대해서도 대응 가능할 것으로 기대하고 있다.

MOST 프로토콜은 멀티미디어 애플리케이션용으로 streaming 통신이 가능하도록 특별히 개발됐으며, 근래에는 카메라 영상 전송과 이더넷 지원이 가능하도록 지원하고 있다. 또한, 자동차용 Ethernet을 브로드 알리치 기술을 기반으로 추진되고 있다.

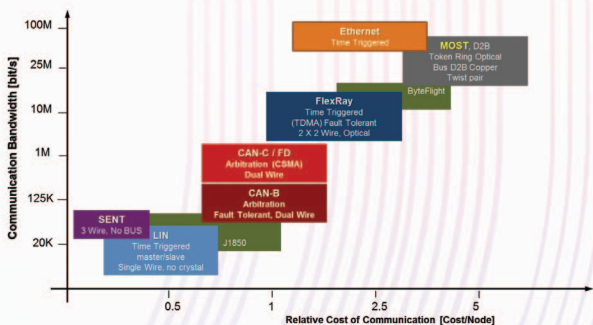


그림 3. 자동차용 In-Vehicle Network 프로토콜별 대역폭

상호간에 더욱 빠르고 많은 정보를 교환할 필요성이 대두되고 있으나, 기존 네트워크 기술로는 기능안전과 고대역폭의 만족스러운 통신이 이루어지지 못하고 있어 상호간 통신 속도를 높여주는 고속 차량 네트워크 기술과 이를 지원하는 시스템반도체 기술이 등장하고 있다.

Dual Core Lockstep Mode 지원 시스템반도체

자동차용 기능안전 지원을 위한 시스템반도체 측면의 대표적인 기능 중 하나인 Dual Core Lockstep 모드는 두 개의 코어가 동일한 코드를 실행하여 독립적인 컴퍼레이터가 실행 결과를 비교하고, 불일치가 발생하는 경우에는 Trap 발생시켜 fail-safety 모드로 전환되어 시스템이 안전 상태로 설정될 수 있도록 지원되는 기능이다.

여러 처리 이외에는 두 개의 코어가 동일한 코드를 실행하기 때문에 멀티 코어와 관련된 소프트웨어 확장자가 필요하지 않다. 즉, 비록 다수의 코어가 사용되고 있지만, 이것이 연산 능력을 증가시키기 보다는 안전성을 증대시키기 위해 사용되는 것이다.

자동차용 멀티코어 아키텍처는 안전과 관련된 시스템에서 ASIL decomposition과 같이 병렬처리에 기반을 두고, 안전 컨셉에 따라 코어 처리를 AUTOSAR에서 정의된 소프트웨어 애플리케이션에 할당함으로써 안전성을 증대시키고 있다.

멀티코어 시스템반도체에서는 애플리케이션 간의 간섭을 배제하기 위해서 서로 다른 프로세서 코어에 각각의 애플리케이션을 할당함으로써 결과적으로는 하나의 시스템반도체 내에서 상호 간섭을 일으키지 않고 실행될 수 있도록 지원한다.

추가적으로 하드웨어적 MPU(Memory Protection Unit)를 이용하여 애플리케이션 별로 미리 정의된 메모리 영역에만 접근할 수 있도록 하는 기능도 지원하고 있다.

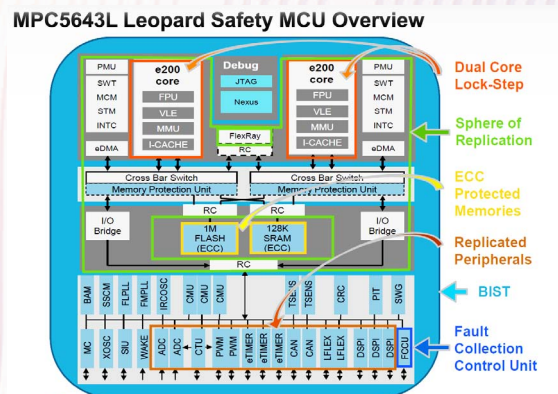


그림 4. 자동차용 In-Vehicle Network 프로토콜별 대역폭

만드는 최근 NXP와 합병을 완료한 Freescale과 협력해 차량용 반도체 기술을 개발 중이다. 센서를 통한 다이내믹 정보와 환경인식 정보를

이용해 차량의 안전성을 구현하는 지능형 차량 전자제어장치 개발을 추진 중이다.

동부하이텍도 지난 2010년 AEC-Q100 인증을 통과, 미국과 유럽, 일본 등의 차량용 반도체 기업의 파워트레인용 전력관리 칩이나 전조등, 후미등 모터 구동칩 및 전력관리칩 등 20여개의 제품을 공급 중이다.

SK하이닉스도 국책과제로 멀티미디어 등의 인포테인먼트 반도체나 RF 등의 네트워크 반도체 관련 공정 개발 등 차량용 반도체 외주생산(파운드리) 사업에 착수한 상태이다.

LG그룹 계열사인 실리콘웍스는 4개의 모터를 하나의 반도체 구동하는 멀티채널 모터 구동칩을 세계 최초로 개발해 양산에 돌입하는 등 차량용 반도체 시장공략에 집중하고 있다.

국내의 시스템반도체 기업들의 기술개발과 노력으로 국산 시스템 반도체가 적용된 스마트카와 커넥티드카가 상용화될 날이 얼마 남지 않은 것 같아 그날을 기대해 본다.

기능안전을 위한 시스템반도체 표준화

자동차가 안전 메커니즘, 통합제어 시스템, 자동차 네트워크 등의 기능들을 위해 더 많은 전자 장치들을 내장하게 됨에 따라 자동차에서 전자 부품의 비중은 점차 증가되고 있다. 그 중에서 자동차용 시스템반도체는 센서와 ECU 등의 거의 모든 전기전자 부품에 탑재되고 있고, 그 비중 또한 지속적으로 증대됨에 따라 더욱 중요하다.

자동차에서 기능들을 구현하기 위해서는 시스템반도체가 탑재된 80~100개의 ECU가 사용될 것으로 예측되고, 또한 이들은 시스템반도체가 내재되어 있는 150~200개의 센서를 활용해 기능들을 수행한다. 각각의 부품 간에는 시스템반도체의 통신기능을 통해 상호 네트워크로 연결되어 있기 때문에 하나의 부품 결함이 다른 ECU에도 영향을 미칠 수 있는 구조이므로, 시스템반도체에 의한 기능안전 대응은 필수적으로 판단된다.

자동차에서 기존의 안전(Safety) 시스템은 고신뢰성 기술을 기반으로 한 하드웨어적인 안전부품에만 의존적이었으나, 근래에 들어서는 소프트웨어까지 확대 적용된 기능안전(Functional Safety) 시스템이 요구되고 있다. 특히, 국제 표준인 ISO26262에서는 소프트웨어가 탑재되는 시스템반도체의 중요성 때문에 ISO/PAS 19451에서 Analog/Mixed signal components, Multi-core components, Programmable logic devices 등에 대해서도 필요한 요구사항 표준화가 추가적으로 진행되고 있다.

자동차용 반도체에 대한 하드웨어적인 신뢰성 및 품질 요구사항과 관련하여 자동차 회사와 반도체 회사들의 단체표준으로 제정된 AEC(Automotive Electronic Council)에서는 기존에 적용되고 있는 IC(Integrated Circuit)에 대한 AEC-Q100과 AEC-Q101(Discrete Component) 이외에도 AEC-Q102(LED), AEC-Q103(MEMS), AEC-Q104

(Multi Chip Module) 표준화 진행이 추가적으로 추진되고 있다.

표 1. AEC 온도 그레이드 분류

Temperature Grade	Min(°C)	Max(°C)	Application Example
Grade 0	-40	+150	System power supply IC
Grade 1	-40	+125	Torque sensor steering
Grade 2	-40	+105	Dual axis acceleration sensor
Grade 3	-40	+85	Peripheral pressure sensor
Grade 4	0	+70	Infotainment

자동차에 사용되고 있는 반도체들은 AEC 온도 그레이드 표 1과 같이 자동차의 열악한 환경에서도 작동해야 하기 때문에 높은 신뢰성이 요구될 뿐만 아니라 다기능, 고성능이면서 기능안전까지 대응 가능해야 한다는 요구조건을 만족시켜야 한다. 자동차용 반도체는 일반적으로 -40~125°C의 범위에서 사용된다. 특히 엔진룸에서 사용되는 특정 반도체의 경우 -40~150°C 조건에서도 견딜 수 있어야 한다.

자동차용 시스템반도체에서는 기능안전을 위한 Self-Diagnostic과 Fault Tolerance 할 수 있는 능력이 요구되고 있다. ECU의 결함을 개별 ECU에서 직접 감지할 수 있다면, ECU는 어떤 것에 대한 교정 작업을 해야 할지 결정할 수 있는 신뢰성 있는 기능을 가질 수 있게 된다. 시스템의 동작정지 및 비상동작은 기능안전 관련 시스템에 있어서 특히 중요하다.

자동차 내의 많은 기능들이 네트워크 애플리케이션화 되어 과거에 보편적이던 구조(하나의 ECU가 하나의 어플리케이션을 구현하던)를 이제는 여러 ECU들 간에 공유되는 네트워크 기능들이 대체하고 있다. 이러한 시스템의 고장은 임의의 결함들에 의해 야기될 수 있다. 필요한 ECU 하나가 고장을 일으킬 경우, 이는 관련 ECU들의 결함 메모리들에 열 가지 이상의 상이한 엔트리들을 야기할 수 있다. 오류 코드가 이처럼 많으므로 과거보다 훨씬 더 상세한 진단 정보를 제공할 필요가 있다.

시스템반도체가 모듈 내에서의 고장을 감지하거나 외부의 결함으로 인해 제대로 동작하지 못하는 상태에 처하게 되면 다른 ECU는 이를 알 수 있어야만 한다. 감지 가능한 결함들은 하드 오류와 소프트 오류의 두 가지 범주로 나눌 수 있다. 하드 오류들은 ECU에서 감지되는 고장들로서, 하드웨어의 문제에 의해 야기된다. 이 경우에는 신호 컨디셔닝이 정지되고 진단 모드가 가동된다.

이와는 대조적으로, 소프트 오류의 원인은 항상 분명하지도 않고 연속적이지도 않다. 이런 이유로 소프트 오류에 대한 오류 카운트가 구현되어 오류가 발생하면 카운트가 올라가고, 이 오류가 더 이상 발생하지 않으면 카운트가 내려간다. 그 결과, 소프트 오류의 메시징은 저역통과 필터를 거치고 센서는 소프트 오류가 더이상 감지되지 않으면 정상동작 상태로 돌아간다. 이러한 모드를 임시 진단 모드(Diagnostic Mode)라고 한다. 이후 ECU는 추가 정보(중복 센서나 중요성 점검)를 이용하여 어플리케이션이 지속적으로 신뢰성 있게 동작할 수 있을지, 혹은 오류 메시지와 함께 정지시켜야 할지 여부를 결정한다.

자동차용 안전 관련 시스템의 개발은 시스템반도체를 이용해 모듈 레벨에서는 구조를 크게 단순화시킬 수 있으며, 기능안전 및 자가진단 등을 추가하고 차량 네트워크 통신 무결성 보장을 비롯한 신뢰성까지도 증대시킬 수 있다.

향후 자동차용 시스템반도체에서의 고신뢰성 기술을 기반으로 한 기능안전 대응이 가능한 기술이 더욱 활발히 연구개발 될 것으로 예측 된다.

맺음말

자동차용 시스템반도체는 지능화됨에 따라 차량 네트워크가 가능한 일체형 시스템반도체로 개발되고 있는 동향에 대해서 소개하고 고신뢰성 측면이 고려된 기능안전 이슈에 대해서 설명했다.

자동차의 지능화와 실시간 동작 및 가격 등 다양한 요구조건으로 인한 설계문제를 해결하기 위해 여러가지 새로운 기능이 적용된 시스템반도체와 네트워크 시스템이 개발되거나 개선될 것으로 기대된다. 또한, 시스템반도체는 자동차용으로서 고신뢰성 부품에는 요구되는 안전 수준과 데이터 통신 대역폭 등을 고려하여 시스템 기술개발이 이루어질 것으로 기대된다.

앞으로 국내에서도 관련 시스템반도체를 성공적으로 양산하여 자동차용 다수의 핵심 전자부품들이 국산화 될 수 있기를 기대한다.



Reference

- 1 Design of Microcontrollers for Safety Critical Operation: Karl Greb and Anthony Seely, Texas Instruments
- 2 Current status and Future of AUTOSAR, Markus Bechter, 7th AUTOSAR Open Conference
- 3 Understanding ISO 26262 ASILs, 2013: Chris Hobbs and Patrick Lee, Electronic Design
- 4 <http://www.NXP.com>
- 5 <http://www.infineon.com>
- 6 <http://www.aecouncil.com>

저자정보



연규봉 팀장 | 자동차부품연구원 시스템반도체팀
 주 연구분야
 자동차용 ECU/SoC, RF 시스템
 E-mail kbyeon@katech.re.kr
 Homepage <http://www.katech.re.kr>





IDEC Newsletter | 통권 제229호

발행일 2016년 6월 30일 **발행인** 박인철 **편집인** 김태욱, 남병규 **제작** 심원기획
기획 김하늘 **전화** 042) 350-8535 **팩스** 042) 350-8540 **홈페이지** <http://www.idec.or.kr>
E-mail kimsky1230@idec.or.kr **발행처** 반도체설계교육센터(IDEC)

반도체설계교육센터 사업은 산업통상자원부, 한국반도체산업협회, 반도체회사(삼성전자, SK하이닉스, 매그나칩반도체, 앰코테크놀로지코리아, 에이티세미콘)의 지원으로 수행되고 있습니다.