반도체설계교육센터
IC DESIGN EDUCATION CENTER

2018 September Vol. 254

IDEC Newsletter

IoT 보안, Internet of Things
안전하게 연결된 세상을 위한 필수 요소

MPW
Multi-Project Wafer

MPW 관련 문의
이의숙 책임 (yslee@idec.or.kr, 042-350-4428)

2018년 MPW 공정 및 진행 일정

• 지원 공정 세부 내역

회사	공정[㎛]	공정내역	설계면적 (팀별)	칩수 /1회	모집 횟수	Package 사용가능 pin수(Design)	Package type
삼성	65nm RFCMOS	CMOSRF 1-poly 8-metal	4mm x4mm	40	3	208pin	LQFP/ BGA 208pin
매그나칩/ SK하이닉스	180nm CMOS	CMOS 1-poly 6-metal (6 metal을 Thick metal(TKM)로만 사용 가능) (Optional layer (DNW, HRI, BJT, MIM) 추가)	3.8mm x3.8mm	25	5	200pin	MQFP/ BGA 208pin
	350nm CMOS	CMOS 2-poly 4-metal (Optional layer (DNW, HRI, BJT, CPOLY) 추가)	5mm x4mm	20	2	144pin	

진행 일정 및 공정 내역

• 2018년 MPW 모집 마감(2019년 지원 내역은 12월 이후 공지될 예정임.)

공정	회차구분 (공정_년도순서)	모집팀수 ((mmxmm)x칩수) /회별	정규모집 신청마감	참여팀수 ((mmxmm)x칩수)	DB마감 (Tape-out)	Die-out	비고 (08.30 기준)
MS 180nm	MS180-1801	(3.8x3.8) x25	2018.01.12	(3.8x3.8)x22 (3.8x1.9)x6	2018.03.19	2018.08.20	제작완료
	MS180-1802		2018.01.12	(3.8x3.8)x23 (3.8x1.9)x4	2018.05.21	2018.10.22	제작중
	MS180-1803		2018.02.09	(3.8x3.8) x25	2018.07.23	2018.12.24	제작중
	MS180-1804		2018.04.13	(3.8x3.8) x24 (3.8x1.9)x2	2018.09.17	2019.02.18	설계중
	MS180-1805		2018.06.08	(3.8x3.8) x24 (3.8x1.9)x2	2018.12.03	2019.05.06	설계중
MS 350nm	MS350-1801	(5x4) x20	2018.02.09	(5x4)x16 (5x2)x1	2018.06.11	2018.10.08	제작중
	MS350-1802		2018.07.06	(5x4)x11	2019.01.14	2019.05.13	추가모집 중 (선착순마감)
삼성 65nm	S65-1801	(4x4) x40	2018.01.12	(4x4)x34	2018.05.07	2018.11.12	제작중
	S65-1802		2018.03.09	(4x4)x39	2018.09.10	2019.03.18	설계중
	S65-1803		2018.07.06	(4x4)x40	2019.01.07	2019.07.19	설계중

- 일정은 사정에 따라 다소 변경될 수 있음.
- 회차표기 : 공정코드-년도 모집순서 (예시) 삼성 65nm 2018년 1회차 : S65-1801)
- 모집 기간 : 모집 마감일로부터 2주 전부터 접수
- 선정 결과 : 모집 마감 후 2주 후 결정
- NDA 접수, PDK 배포 : 선정 후 2주 이내 완료
- Package 제작은 Die out 이후 1개월 소요됨

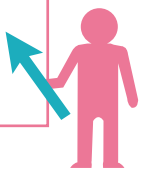
CDC
Chip Design Contest

CDC 관련 문의
김영지 주임 (yjkim@idec.or.kr, 042-350-8536)

IDEC에서는 MPW 참여팀에 한해 CDC 참여팀 등록비의 절반을 지원합니다.

CDC (Chip Design Contest)는

IDEC MPW 참여를 통해 제작한 칩 결과에 대한 발표를 진행하는 행사로,
각 참여팀에게 시스템 설계 분야의 정보 공유할 수 있는 장입니다.



ISOCC 2018 CDC

- 개최 일정 및 장소 : 2018. 11. 13(화), 대구 인터불고호텔
- 참가팀 모집 마감 : 8. 28(화)
- 선정 발표 : 9. 20(목)
- 최종 논문 접수 : 10. 2(화)

제26회 한국반도체학술대회 CDC

- 개최 일정 및 장소 : 2019. 2. 14(목), 강원도 웰리힐리파크
- 참가팀 모집 마감 : 2018. 10. 26(금)
- 선정 발표 : 12. 14(금)
- 최종 논문 접수 : 12. 28(금)

* 일정은 사정에 따라 조정될 수 있습니다.

교육
프로그램 안내
2018. 9

수강을 원하는 분은 IDEC 홈페이지 (www.idec.or.kr) 를 방문하여 신청하시기 바랍니다.

강좌일정

센터명	강의일자	강의 제목	분류
본센터	9.3-4	Low Power Flow : HLD (Front-end)	설계강좌
	9.5-6	Low Power Flow PnR	Tool강좌
	9.10-11	DFT Compiler with Advanced Features	Tool강좌
	9.17-19	Low Power Verification	Tool강좌

본센터

9/3-4

강좌제목 Low Power Flow : HLD (Front-end)

강 사 권영기 이사 (Synopsys)

강좌개요

For multi-voltage or multi-supply designs, you will learn how to apply the IEEE 1801 UPF flow that uses a power intent specification which is applied to RTL designs.

수강대상

ASIC designers with experience in one or more of : logic design, design verification, Place&Route or signoff verification. CAD engineers responsible for flow development will find this beneficial.

강의수준 초급 **강의형태** 이론+실습

사전지식 · 선수과목

- Design Compiler
- Formality
- PrimeTime
- Milkyway and .lib library concepts

9/5-6

강좌제목 Low Power Flow PnR

강 사 배명우 대리 (Synopsys)

강좌개요

- Floorplan a design with multiple power domains, including power-switched blocks
- Create voltage areas to provide the physical context of MV floorplanning

수강대상

ASIC, back-end or layout designers with experience in one or more of: logic design, design verification, Place&Route or signoff verification. CAD engineers responsible for flow development will find

강의수준 초급 **강의형태** 이론+실습

사전지식 · 선수과목

1. UNIX/Linux and X-Windows
2. A Unix text editor, e.g. Emacs, vi, pine
3. A basic working knowledge of Synopsys IC Compiler
4. An awareness of the basics of low-power design techniques

9/10-11

강좌제목 DFT Compiler with Advanced Features (OCC, DFTMAX_Ultra, Wrapper)

강 사 김태삼 과장 (Synopsys)

강좌개요

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.

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 고급 **강의형태** 이론+실습

사전지식 · 선수과목

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

9/17-19

강좌제목 Low Power Verification

강 사 이해창 과장(Synopsys)

강좌개요

Low power 검증 전체에 대해 체험해 볼 수 있다. 과정을 이수하면 UPF를 통해 저전력 구현 및 검증에 필요한 파워 구조를 작성할 수 있게되고, 해당 UPF를 가지고 VCS-NLP 시뮬레이션을 해서, 저전력 설계시 function 검증을 할 수 있게 된다.

수강대상 저전력 설계 및 검증 인력

강의수준 중급 **강의형태** 이론+실습

사전지식 · 선수과목 ASIC 기초, Low Power Methodology, Cell library

문 의 | 본센터 IDEC 김영지 (042-350-8536, yjkim@idec.or.kr)

"Intelligent SoC Driving the Fourth Industrial Revolution"

ISOCC 2018

15th International SoC Design Conference

November 12-15, 2018

Hotel Inter-Burgo Daegu, Daegu, Korea

About ISOCC

ISOCC has established a long tradition as an annual conference providing the world's premier SoC design forum for leading researchers from academia and industries. ISOCC 2018 welcomes articles in the field of semiconductor circuits and systems dealing with new advanced concept and developments in technology of analog/digital circuits or systems, theory, simulation, modeling, advanced experimental results and experience of SoC with SW, and an emerging technology for the future.

ISOCC 2018 is technically co-sponsored by IEEE CAS Society. All accepted papers will be published in the conference proceedings and will be submitted for inclusion in IEEE Xplore. Authors of selected outstanding papers will be invited to submit extended versions of their papers for consideration of publication in the Journal of Semiconductor Technology and Science (JSTS) (www.jsts.org).

Topics of Interest

Topics include, but are not limited to:

- **Analog Circuits**
  - Analog Circuits
  - Amplifiers and Filters
  - Power Management Circuits
- **Data Converters**
  - Analog-to-Digital Converters
  - Digital-to-Analog Converters
  - Analog Circuits for Data Converters
- **RF/Microwave/Wireless**
  - RF Circuits and Transceivers
  - Microwave and Millimeter-Wave Circuits
  - Wireless Communication Circuits
- **Wireline**
  - High-Speed Interface
  - Wireline Link
- **Digital Architecture and Systems**
  - Multimedia Systems & Image Processing Applications
  - Digital Signal Processing & Communication Systems
  - Embedded Software and Systems
- **Digital Circuits and Memories**
  - Digital Integrated Circuits
  - Hardware Security
  - Nanoelectronics and Gigascale Circuits and Systems
  - Memory Circuits & Systems
- **SoC Design Methodology**
  - Software & Algorithm
  - Artificial Intelligence and Deep Learning
  - HW-SW Co-Design
  - Embedded SoC
  - SoC Testing
  - Design Verification
  - FPGA Design
  - Signal Integrity / Interconnect Modeling and Simulation
- **Circuits and Systems for Emerging Technologies**
  - Neuromorphic Computing
  - Sensory Circuits and Systems
  - Biomedical Circuits and Systems
  - Automotive Circuits and Systems
  - IoT/IoE Circuits and Systems
  - 3-D ICs and SoC Packages

Important Dates

- Submission of Special Session and Tutorial Proposals: **June 22, 2018**
- Notification of Acceptance of Special Session and Tutorial Proposals: **July 9, 2018**
- Submission of Regular Session Full Papers: ~~**July 13, 2018**~~ ~~**July 31, 2018**~~ **August 10, 2018**
- Submission of Special Session Full Papers: **August 17, 2018**
- Notification of Acceptance: **September 10, 2018**
- Submission of Final Papers (for all accepted papers): **September 21, 2018**
- Author & Early-Bird Registration: **September 21, 2018**

Paper Submission

A complete 2-page manuscript must be submitted electronlcally In PDF format (In Standard IEEE double-column format posted on the conference website). Only electronic submissions will be accepted. For more Information, please refer to the conference website (http://www.isocc2018.org).

International Organizing Committee

General Chair

- **Kwang Hyun Baek** *(Chung Ang Univ., Korea)*

General Co-Chairs

- **Jun Jin Kong** *(Samsung Electronics, Korea)*
- **Mohamad Sawan** *(Polytechnique Montréal, Canada)*
- **Yoshifumi Nishio** *(Tokushima Univ., Japan)*

Conference Secretary

- **Youngmin Kim** *(Kwangwoon Univ., Korea)*

Technical Program Committee

Technical Program Chair

- **Kyung Ki Kim** *(Daegu Univ., Korea)*

Technical Program Co-Chairs

- **Meng-Fan(Marvin) Chang** *(National Tsing Hua Univ., Taiwan)*
- **Chip Hong Chang** *(Nanyang Technological Univ., Singapore)*

Technical Program Vice Chairs

- **Kang-Yoon Lee** *(Sungkyunkwan Univ., Korea)*
- **Jongsun Park** *(Korea Univ., Korea)*

"Full Day Tour Around Daegu Area" (free except lunch)

Conference Venue: Hotel Inter-Burgo Daegu

The city of Daegu is surrounded by UNESCO World Heritage Sites (Gyeongju Seokkuram and Bulguksa, Gyeongju Historical Areas, Haeinsa Temple Tripitaka Koreana, and the historic villages of Hahoe and Andong). We are truly glad to host such a prestigious event in the central hub of world heritage sites of Korea.

■ Address:
212 Palhyeon-gil, Suseong-gu, Daegu, Republic of Korea

■ Website:
http://www.hotel-interburgo-daegu.com

■ Tel: +82-53-602-7114

전력 반도체 (Power Management Integrated Circuit)의 현재와 미래

홍성완 교수 | 숙명여자대학교 전자공학전공

1. 서론

앞으로 도래할 4차산업혁명의 시대에는 인간의 삶의 질을 더욱 향상시키기 위해 보다 많은 기능들이 전자기기에 요구될 것이다. 이에 따라 전자기기들은 복잡하고 더 많은 역할을 수행해야 한다. 복잡하고 다양한 전자기기의 기능들은 지금보다 더욱 큰 전력을 요구하게 될 것이고, 이는 배터리의 사용시간을 단축하게 된다. 따라서 사용자의 편의를 위해서는 배터리의 용량을 늘리는 것이 중요하다. 하지만 다음 세대의 획기적인 배터리 기술이 개발되기 전까지는 전자기기, 특히 모바일 제품에서는 크기의 제한으로 인해 배터리의 용량을 증가시키는데 한계가 존재한다. 그렇다면 배터리 사용 시간을 어떻게 증가시킬 수 있을까?

전자기기 내에서 각각의 기능을 수행하는 각 모듈로 전력의 손실 없이 최대한 효율적으로 에너지를 전달하는 방법이 한가지 해답일 것이다. 시스템에서 이러한 역할을 수행하는 집적회로를 Power Management Integrated Circuit (PMIC)라고 한다[1-9].

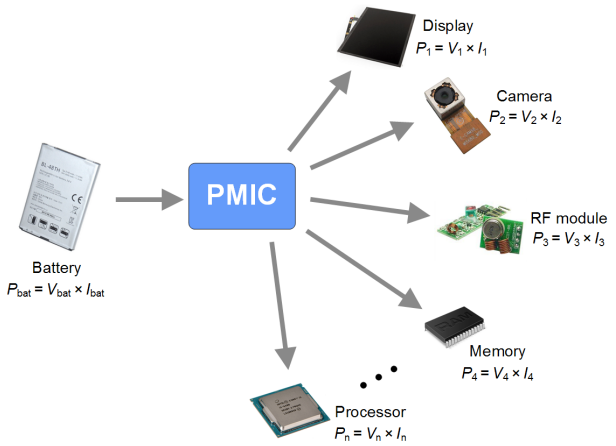


그림 1. 모바일 기기 내의 PMIC

그림 1에서와 같이 PMIC는 전력의 손실을 최대한 방지하면서 배터리의 특정 전압을 각 모듈이 필요로 하는 다양한 전압으로 바꿔주어 공급하는 역할을 한다. 그렇다면 배터리의 전압을 각 모듈로 바로 공급해주지 않고 왜 굳이 변환하여 공급하는 것일까?

그 이유는, 전자기기의 각 모듈에서 필요로 하는 전압이 다르기 때문이다. 또한, 사용시간이 지남에 따라 배터리의 전압이 낮아지기 때문에 각 모듈에서 필요로 하는 전압을 일정하게 공급해주는 PMIC가 필요한 것이다.

지금까지는 PMIC가 전자기기 내에서 필요한 이유를 알아보았다. 그렇다면 이번에는 PMIC 설계 시 중요한 특징을 살펴보자. 앞서 언급하였듯이 PMIC에서는 입력 전력을 출력 전력으로 바꾸어 줄 때 발생하는 전력 손실을 최소화 해야 한다. 다양하고 복잡한 기능이 수행되고 있는 최근의 전자기기에서는 상당한 양의 전력을 소비하고 있고, 따라서 전력 손실의 양 또한 증가하고 있다. 이러한 전력 손실은 열의 형태로 나타나게 되는데, 큰 전력을 소비하는 전자기기에서는 결국 매우 큰 열이 발생된다. 이상적으로는 PMIC의 입력 전력과 출력 전력이 같아야 하지만, 실제로는 여러 기생 성분들로 인해서 전력 손실이 발생할 수 밖에 없다. 대표적인 기생 성분은 그림 2에서 볼 수 있듯이 기생 저항 성분과 기생 커패시터 성분이다. 이 기생 성분들은 PMIC 설계 시 수반될 수 밖에 없는 것으로, 이 기생 성분에 의해 발생하는 전력 손실을 최소화 하는 것이 PMIC 설계의 기술이며 중요한 특징이 된다.

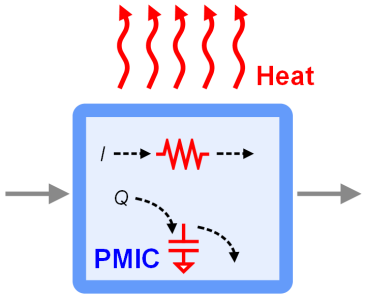


그림 2. 전력 손실 요인

2. PMIC 종류 및 특징

PMIC에는 다양한 종류의 회로가 존재한다. 이 회로들은 각각 특성이 다르고 이에 따라 쓰이는 목적이 다르다. 앞서 언급하였듯이, PMIC의 주 목적은 전력 손실을 최소화하며 각 모듈에 전원을 공급해주는 것이기는 하지만 모든 종류의 PMIC가 전력 손실을 최소화 하는 것에만 초점을 두는 것은 아니다. 어떤 회로는 큰 크기와 높은 가격을 갖더라도 전력 손실의 최소화에 집중하는 반면, 어떤 회로는 전력 손실을 다소 감수하면서도 크기와 가격을 줄이는 것에 주안점을 두고 있다. 이 단원에서는 이러한 관점에서, 자주 사용되는 세 가지의 PMIC들을 소개하려 한다.

2.1) (Inductive) DC-DC converter

DC-DC converter는 PMIC 중 가장 작은 전력 손실을 달성할 수 있는 회로이다. 이 회로는 상보적으로 동작하는 두 개의 스위치, 하나의 인덕터, 그리고 하나의 커패시터로 구성되어 있으며, 이 소자들의 배치에 따라 입력된 전압보다 높은 전압을 출력하는 step-up (boost) converter, 낮은 전압을 출력하는 step-down (buck) converter로 나눌 수 있다[1,2]. 이 두 가지 중 step-down DC-DC converter가 그림 3 (a)에 나와 있다. 이 회로를 구성하는 수동 소자 중, 인덕터와 커패시터는 에너지를 소모하지 않는 소자이므로 이상적인 DC-DC converter에서는 전력 손실이 발생하지 않는다. 하지만, 스위치, 인덕터, 그리고 커패시터에 있는 기생 성분으로 인해 전력 손실이 발생한다. 따라서, 기생 성분의 영향을 최소화 하기 위해 적절한 크기의 소자들을 사용해야 한다. 인덕터의 경우, 기생 성분을 줄이기 위해서는 그림 3 (b)에서와 같이 다른 소자보다 훨씬 더 큰 크기를 가져야 한다. 이는 시스템 측면에서 큰 부담이 되기 때문에 크기가 작은 인덕터를 사용하면서도 낮은 전력 손실이 발생할 수 있도록 설계해야 한다.

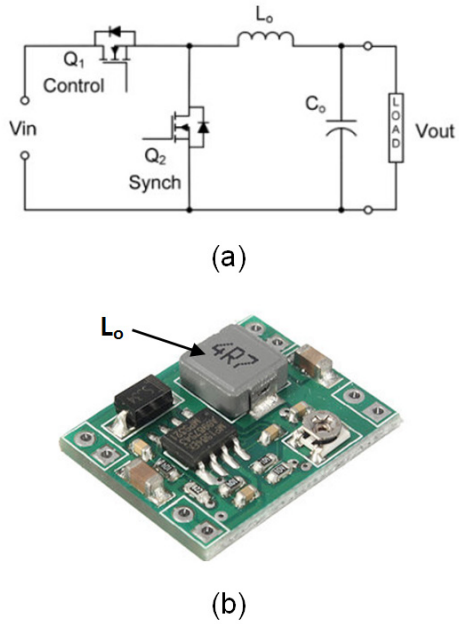


그림 3. (a) Step-down DC-DC converter (b) DC-DC converter 모듈

크기가 작은 인덕터를 사용하면서도 작은 전력손실을 달성할 수 있는 방법으로 여러가지 연구가 진행되어 오고 있다. 더 작은 두 개의 인덕터를 사용하여 전류 path를 나누는 multiphase converter[3], 추가적인 커패시터를 사용하여 인덕터 전류의 리플을 줄이는 multi-level converter[4], 그리고 추가적인 커패시터를 사용하여 인덕터 전류의 크기 자체를 줄이는 dual-path converter[5] 등이 그 예이다. PMIC에서 공급해주어야 하는 전력량이 증가함에 따라 이와 같은 회로들의 연구는 앞으로도 꾸준히 진행될 것이다.

2.2) Charge pump

DC-DC converter에 사용되는 인덕터가 부담스럽다면, 인덕터를 사용하지 않으면서도 전압을 증가시켜주거나 감소시켜줄 수 있는 charge pump를 사용할 수 있다[6]. 그림 4에 나와 있는 회로는, 입력 전압을 더 높은 전압으로 출력해주는 step-up charge pump이다. 이 회로는 상보적으로 동작하는 두 개의 clock과 여러 개의 다이오드와 커패시터로 구성되어 있다. 다이오드와 커패시터의 수에 따라 전압이 증가되는 비율이 달라지며, 다이오드 대신에 스위치를 사용할 수도 있다. 인덕터를 사용하지 않기 때문에 시스템 측면에서 DC-DC converter보다 부담이 되지 않는다는 장점이 있으나, 커패시터의 개수에 따라 정해진 출력 전압 밖에 생성할 수 없으며, 또한 커패시터가 병렬 연결될 때 상황에 따라 비교적 큰 전력 손실이 발생할 수 있다는 단점이 존재한다.

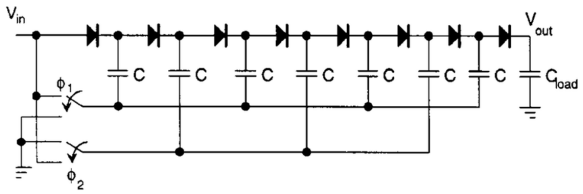


그림 4. Step-up charge pump

2.3) Low-dropout regulator

Low-dropout regulator (LDO)는 PMIC 중 가장 간단한 구조의 회로로, 그림 5에서 보이는 것과 같이 하나의 트랜지스터, 하나의 외부 커패시터, 그리고 부담 없는 크기의 제어 회로로 구성이 된다[7].

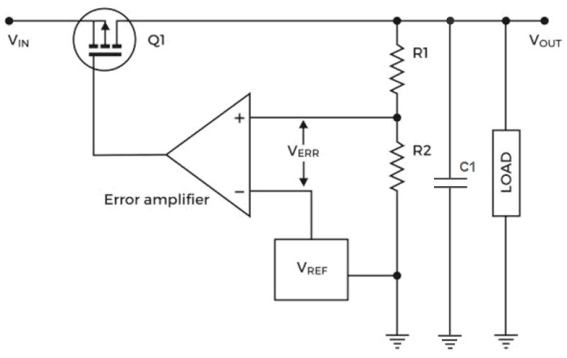


그림 5. Low-dropout regulator

앞의 두 가지 종류의 회로들과는 다르게 이 LDO의 출력 전압은 항상 입력 전압보다 낮다. 따라서, 입력 전압보다 높은 출력전압을 생성하고 싶다면, 이 LDO를 사용해서는 안된다.

LDO의 동작원리는 매우 간단하다. 우선, 부하 (LOAD)는 저항으로 생각할 수 있다. 이 부하에 원하는 전압을 출력해주고자 하면 제어회로를 통해 트렌지스터 (Q1)의 온-저항을 조절해주어 전압 분배 비율을 조절해주면 된다.

동작원리와 구성이 간단한 반면에, 입력 전압과 출력 전압의 비율에 따라 전력 손실이 발생한다는 단점이 있다. 만약 입력 전압과 출력 전압 사이에 상당한 차이가 존재한다면, 매우 큰 전력 손실이 발생할 수 밖에 없다. 따라서, 이 LDO는 주로 큰 전력이 요구되지 않는 곳에 사용이 된다.

최근에는 이 회로의 구성을 더욱 간단하게 하기 위해, 외부 커페시터를 제거한 capless LDO도 많이 연구되고 있다[8]. 또한, 디지털 회로의 장점을 이용하여 제어회로를 설계한 digital LDO도 활발히 연구되고 있다[9].

3. PMIC 설계의 확장

PMIC의 개념이 확장될 수 있는 분야는 매우 다양하다. 전력 전달 혹은 에너지의 변환이 필요한 곳이라면 모두 PMIC의 설계 개념이 확장될 수 있는 분야라고 할 수 있다. 이 단원에서는 PMIC 설계 개념이 확장되어 활발히 연구가 진행되고 있는 에너지 하베스팅과 무선전력전송에 대해 이야기를 나누고자 한다.

3.1) 에너지 하베스팅 회로

에너지 하베스팅 회로는 주변 환경의 에너지를 모아 사용자가 필요한 곳에 사용할 수 있도록 에너지를 저장하는 역할을 수행한다. 이 회로는

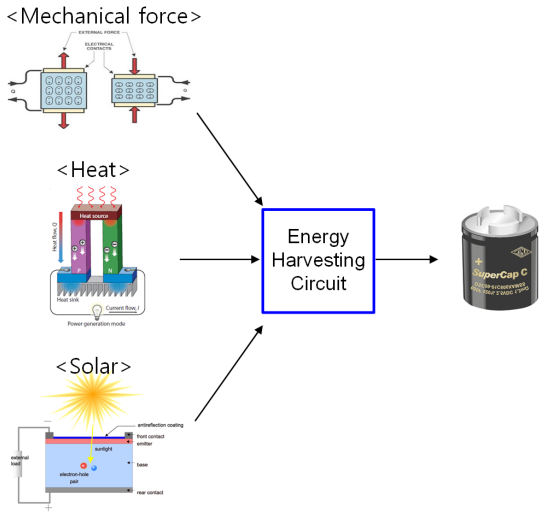


그림 6. 에너지 하베스팅 개념도

그림 6과 같이 다양한 형태의 에너지를 전하의 형태로 바꾸어주는 여러 소자의 도움을 받아, 물리적인 힘 (압력 또는 진동), 열, 태양열 등으로부터 전기에너지를 추출할 수 있다. 전하의 형태로 변환된 에너지를 모아 저장을 할 때, 저장되는 에너지 양을 극대화 하기 위해서는 에너지를 변환하는 과정 중에 발생하는 전력 손실을 최소화 해야 한다. 이를 위해 에너지 하베스팅 회로 설계에 PMIC 설계 기술이 요구된다. 주로 DC-DC converter의 설계가 응용이 되며[10], 최근에는 charge pump의 구조를 응용한 에너지 하베스팅 회로도 활발히 연구되고 있다[11].

3.2) 무선전력전송

마주 보는 두 개의 코일 중 한쪽 코일에 교류 전원을 인가하면, 반대 쪽 코일에 교류 전류가 유도된다. 이를 이용하여 무선으로 전력을 전송하는 기술이 산업 여러 곳에 이용되고 있다. 무선으로 전송 받은 교류 전류는 정류되어 배터리와 같은 에너지 저장장치에 저장된다. 이 과정에서 에너지의 변환이 필요하다. 따라서 그림 7과 같이 PMIC가 응용된 무선전력전송 회로가 사용이 되며, 이 회로에서도 전력 손실의 최소화가 가장 중요하다[12]. 다양한 전자 기기의 충전 방식으로 무선 충전이 각광받고 있는 트렌드를 미루어 보아, 무선전력전송 회로도 활발하게 연구가 될 것이라고 예측된다.

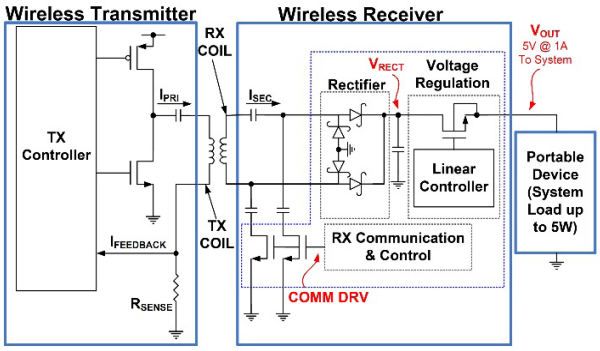


그림 7. 무선전력전송 회로도

4. PMIC 시장 현황 및 전망

전세계 대부분의 국가들이 스마트 도시 개발에 힘을 쓰고 있다. 스마트 도시에서는 네트워크를 통해 도시의 많은 것들을 제어할 수 있는데, 이에 따라 사람들은 스마트폰, 태블릿과 같은 전자기기를 통해 네트워크에 접속하게 될 것이다. 따라서 이러한 스마트 도시 개발의 증가는 더 많은 전자기기의 사용을 유도할 것이고, 이에 따라 PMIC에 대한 수요가 꾸준히 증가할 것이다.

그리고 하이브리드 및 전기 차량의 증가로 인해 차량용 PMIC 또한 그 수요가 꾸준히 증가할 것으로 예상된다.

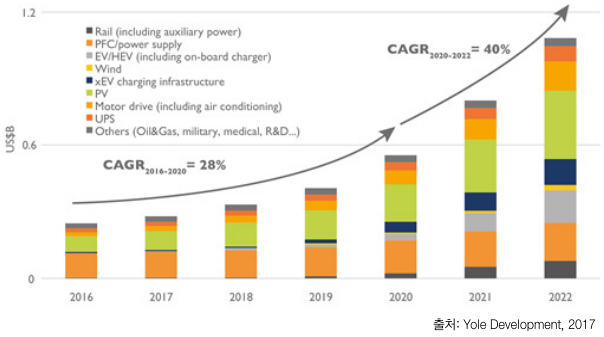
위와 같은 예측에 따라 그림 8과 같이 글로벌 PMIC 시장은 앞으로도 꾸준히 성장할 것이라고 예상된다.

출처: Market Research Future, 2018

그림 8. 글로벌 PMIC 시장 규모 전망

*새로운 소자로 설계하는 전력 반도체

PMIC의 수요가 증가하고 신뢰성과 효율성이 주요 이슈가 되면서, PMIC의 소재로 탄화규소(SiC)가 차세대 소재로 주목을 받고 있다. 이 SiC는 고전압과 고내열 성능이 우수하기 때문에 전기차, 스마트카 시장의 발전에 따라 활용 가능성이 점차 증가되고 있다. 이에 따라 프랑스 시장조사 업체 Yole development는 SiC 기반의 PMIC 시장이 2019년에 전환점을 맞이하여 2020년부터 연평균 40%의 성장률을 보일 것으로 예상했으며, 2022년에는 약 10억 달러 이상의 규모를 가질 것으로 전망했다.



출처: Yole Development, 2017

그림 9. SiC 기반 전력 반도체 시장 규모 전망

5. 결론

모든 종류의 전자기기, 전자제품에는 PMIC가 필수적으로 사용될 수 밖에 없다. 앞으로 더 많은 전자기기가 우리 생활 속에서 이용될 것이고 전기차의 보급도 늘어날 전망이기 때문에, 이를 위한 PMIC의 수요가 지속적으로 증가될 것이라 예상한다. 또한, 전자기기 및 전기차의 성능의 증가에 따라 PMIC에서 공급해주어야 할 전력량은 꾸준히 증가하게 될 것이고, 이를 위해 더 높은 성능을 갖는 PMIC의 연구를 지속적으로 해야 할 것이다. 동시에 비용 절감을 위한 설계 기법과 안정도를 높일 수 있는 설계 기법도 연구가 진행되어야 할 것이라 생각된다.

PMIC에 대한 꾸준한 수요, 설계에 대한 남아있는 숙제, 그리고 다른 분야로의 확장성으로 인해 PMIC의 연구는 앞으로도 활발히 진행되리라 예측할 수 있다.

참고문헌

1. T. Nabeshima, et al., “Analysis and Design Considerations of a Buck Converter with a Hysteretic PWM Controller,” Proc. IEEE Power Electronics Specialists Conf., vol. 2, pp. 1711–1716, 2004.
2. T.-H. Kong, S.-W. Hong, and G.-H. Cho, “A 0.791 mm^2 on-chip self-aligned comparator controller for boost DC-DC converter using switching noise robust charge-pump,” IEEE J. Solid-State Circuits, vol. 49, no. 2, pp. 502–512, Feb. 2014.
3. P. Li, X. Lin, P. Hazucha, T. Karnik, and R. Bashirullah, “A delay locked loop synchronization scheme for high-frequency multiphase hysteretic DC-DC converters,” IEEE J. Solid-State Circuits, vol. 44, no. 11, pp. 3131–3145, Nov. 2009.
4. Xun Liu, Cheng Huang, and Philip K. T. Mok, “A 50MHz 5V 3W 90% Efficiency 3-Level Buck Converter with Real-Time Calibration and Wide Output Range for Fast-DVS in 65nm CMOS,” IEEE Symp. VLSI Circuits Dig. Tech. Papers, pp. 1-2, June 2016
5. Se-Un Shin, et al., “A 95.2% Efficiency Dual-Path DC-DC Step-Up Converter with Continuous Output Delivery Current,” ISSCC Dig. Tech. Papers, pp. 430-432, Feb. 2018.
6. H.-P. Le, J. Crossley, S. R. Sanders, and E. Alon, “A sub-ns response fully integrated battery-connected switched-capacitor voltage regulator delivering 0.19W/mm^2 at 73% efficiency,” in Proc. IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers, Feb. 2013, pp. 372–373.
7. M. Al-Shyoukh, and H. Lee, “A transient-enhanced low-quiescent current low dropout regulator with buffer impedance attenuation,” IEEE J. Solid- State Circuits, vol. 42, no. 8, pp. 1732–1742, Aug. 2007.
8. S. Hong and G. Cho, “High-gain wide-bandwidth capacitor-less low-dropout regulator (LDO) for mobile applications utilizing frequency response of multiple feedback loops,” IEEE Trans. Circuits Syst. I, Regul. Papers, vol. 63, no. 1, pp. 46–57, Jan. 2016.
9. Kye-Seok Yoon, Hyun-Sik Kim, Wanyuan Qu, Young-Sub Yuk, Gyu-Hyeong Cho, "Fully Integrated Digitally Assisted Low-Dropout Regulator for a NAND Flash Memory System", Power Electronics IEEE Transactions on, vol. 33, pp. 388-406, 2018.
10. P. Gasnier, et al., “An Autonomous Piezoelectric Energy Harvesting IC Based on a Synchronous Multi-Shot Technique,” IEEE JSSC, vol. 49, no. 7, pp. 1561–1570, 2014.
11. S. Du and A. Seshia, “An Inductorless Bias-Flip Rectifier for Piezoelectric Energy Harvesting," IEEE JSSC, vol. 52, pp. 2746-2757, Oct. 2017.
12. H.-M. Lee and M. Ghovanloo, “An Adaptive Reconfigurable Active Voltage Doubler/Rectifier for Extended-Range Inductive Power Transmission,” ISSCC, pp. 286-287, Feb. 2012.

저자정보

홍 성 완 교수

소속
숙명여자대학교 전자공학전공

주 연구분야
Analog Integrated Circuit (IC) Design

E-mail hsw0930@sookmyung.ac.kr

Homepage https://advanced-iclab.wixsite.com/aiclab

Blue Pearl Software 사 Visual Verification Suite 소개

한국지원사: LeadingEdgeProvide (엘이프로)
박상호 대표이사
휴대폰 +82-10-3314-4462 이메일 sangho.park@leprovide.com 웹페이지 http://www.leprovide.com/

A 목 적

(RTL 코드 디버깅) Blue Pearl의 Visual Verification Suite는 RTL 구조 검증, CDC 분석 및 디버그를 위한 통합 솔루션입니다.

B 구 분

(RTL Lint, CDC and SDC 자동 생성) : Blue Pearl의 Visual Verification Suite는 ASIC, FPGA 및 IP에 대한 RTL (Register Transfer Level) 디자인을 검증하고 디버깅하는 EDA 소프트웨어 제품군입니다.

C Supported platform and O/S System

The supported platforms are Linux (RedHat Enterprise v.5 and v.6, Centos 5.x & 6.x), and Windows (XP and Windows 7).

Visual Verification Suite 가 필요한 경우

1 RTL code 작성시 검증

- 코딩이 끝날 때까지 기다리지 않고 코딩하면서 RTL을 깨끗하게 처리
- 통합 검증 환경은 빠르고 사용하기 쉬움
- 레거시 코드의 이해및 읽기 그리고 효율적인 코딩을 통한 복잡한 소스 코드 시각화
- 강력한 메시지 필터링 기능 - 잡음이 없음
- 포괄적 인 통합 디버그 기능
- 디자인 반복을 대폭 감소

2 RTL 디자인 성능 향상

- 구조 분석 및 제약 조건 생성을 통한 타이밍 향상
- 더 깨끗한 RTL 코드로 더 나은 성능과 수율 제공

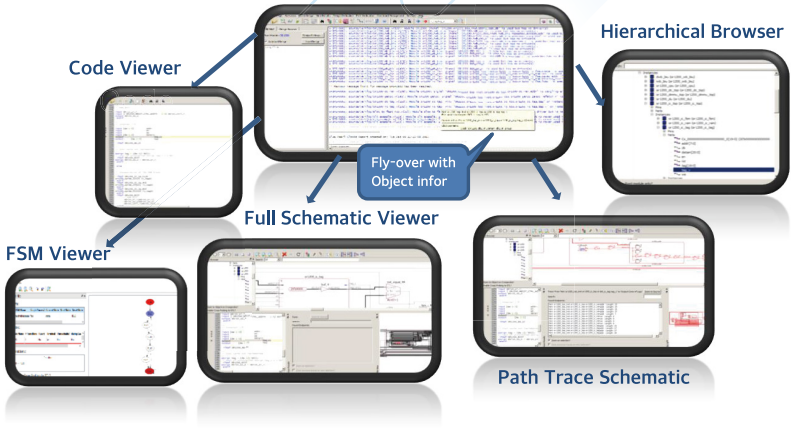
3 비싼 EDA 툴의 비용절감

- 합리적인 가격의 EDA 툴
- 고성능, RTL 코드 디버깅에 매우 효율적

Visual Verification Suite 만의 특징적인 기능

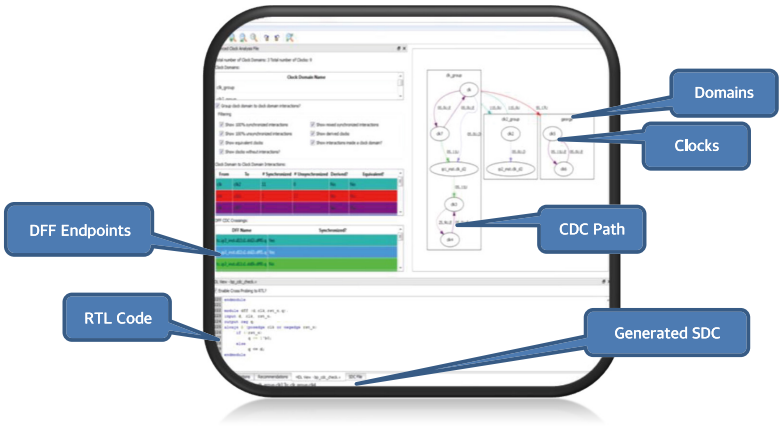
1 통합적인 디버그 환경

모든 설계의 객체를 설계 brower을 통해, 회로도 및 RTL을 교차 탐색 할 수 있는 환경 제공



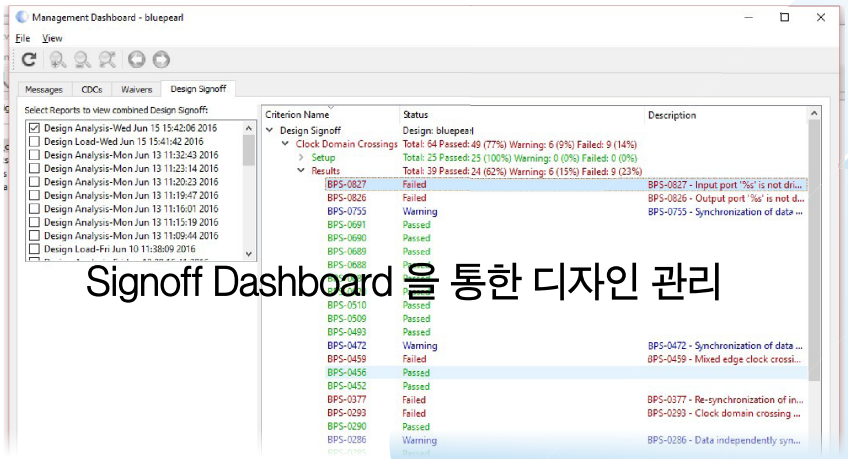
2 고급 Clock 환경

- 클럭 및 도메인을 올바른 상태로 유지하는 데 도움
- 앞선 CDC 분석
- 클럭 및 클럭 도메인의 그래픽 표현 제공
- 클럭 그룹화에 대한 권장 사항 제공
- CDC 분석 도구을 통해 사용할 SDC 템플릿 제공



3 Dashboard 을 통한 디자인 signoff 관리

- signoff 검증 확인
  - 분석이 올바르게 실행 되었나?
  - 결과는 정확히 나왔는가?
- 디자인 signoff 표준 및 우선 순위
  - 실패, 성공에 대한 검증 보고
  - 다양한 signoff 우선순위 허용
  - 통과/실패, 통과/경고/실패 등 결과 제공
- 고객사의 특정 DRC(Design rule checking)에 맞게 사용자 정의 가능



Signoff Dashboard 을 통한 디자인 관리

Visual Verification Suite 구성 요소

RTL 검증

ASIC 및 FPGA는 메모리, 트랜시버, 써드 파티(third party) IP 및 프로세서 코어 그리고 수백만 개의 게이트를 일상적으로 갖추고 있습니다. 실험 및 시뮬레이션을 통해 문제를 디버그하는 데 많은 시간과 비용이 소요될 수 있습니다. 디자이너는 문제를 신속하게 파악하여 시뮬레이션 전, 합성 전, 그리고 랩에 칩을 굽기 전에 문제를 신속하게 식별하여 디버그 및 검증시간을 단축 할 수있는 검증 도구가 필요합니다.

특징

- EEE Verilog / System Verilog 및 VHDL 언어 사양 준수 및 구문 표준검사
- STARC 및 Xilinx UltraFast와 함께 사용자 구성 가능 검사
- 디버그를 간소화 하기 위한 GUI; 통합 RTL, 회로도 및 메시지 뷰어
- 간편한 디버그 메시지 정렬 및 검출, 문제 식별을 위한 waive 기능
- 플로우 자동화, 명령 행 인터페이스 (CLI) 및 재사용 가능한 메시지 면제 파일
- 설치 마법사로 학습 시간 단축

설계문제를 빠르게 확인

시각적 검증 환경을 통해 Analytic RTL™ 사용자는 지능형 정렬 및 메시지 필터링을 사용하여 신속하게 설계 문제를 디버그 할 수 있습니다. 주요 기능으로는 저소음, 특정 디자인 스타일에 대한 사용자 정의 확인, 쉬운 설정 및 waiver 재사용 등이 있습니다.

HDL Creator™

HDL Creator는 생산성, 예측 가능성 및 코드 품질을 원하는 RTL 및 테스트 벤치를 코딩하는 개발자에게 이상적인 스마트 에디터입니다. HDL Creator는 직관적이고 사용하기 쉬운 고급 기능보기의 편집기를 통해 실시간 구문 및 스타일 코드 검사를 제공하여 코드 작성시 이해, 디버그 및 검증 할 수 있는 기능을 제공합니다.

중요 혜택

- 코드 개발을 빠르게 할 수 있음
- 복잡한 소스 코드의 시각화을 통한 레거시 코드의 효율적인 코딩, 읽기 및 이해 하는데 도움을 줌
- 확실하게 고품질의 코드를 개발 할 수 있음
- 후속 개발을 간소화 할 수 있음

기능

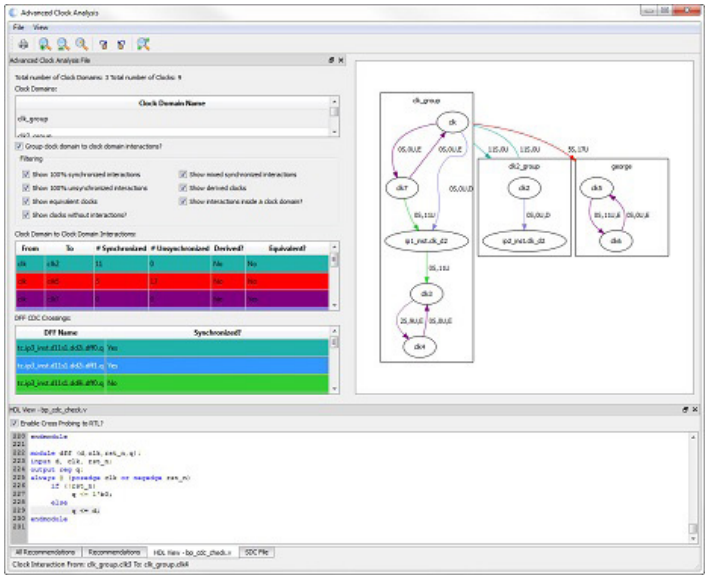
- 들여 쓰기 차단 (탭 또는 공백으로 설정)
- 새 줄 자동 들여 쓰기
- 접기 (코드 블록 숨기기 또는 보기)
- 자동 완성
- 구문 강조
- Brace matching
- 블럭 댓글 (여러 스타일)
- line end 스타일 선택
- 그래픽 보기
- 현재 파일의 자동 분석 - 구문 문제 표시
- 실시간 구문 및 코딩 스타일 검사
- 실시간 분석을 위해 70개 이상의 “로드 검사” 활성화
- 2000 라인 이상의 Verilog 및 VHDL의 parsing 분석 관련 메세지 제공
- 프로젝트 및 비프로젝트 모드에서 사용 가능
- PDF 문서로 생성이 가능
- 시뮬레이터와의 결합 및 후속 디자인 분석에 도움

2 Advanced Clock Environment (ACE)

Blue Pearl Software의 ACE는 RTL 디자인에서 클록 및 비동기 클록 도메인 크로싱을 시각화하는 기능을 제공하여 사용자가 CDC 준 안정성 (metastability)을 분석 할 수 있도록 도움을 드리고 있습니다.

주요 기능

- clock, clock group 그리고 clock 간 상호관계에 대한 상세한 분석
- 빠른 디버깅을 위한 비주얼 디스플레이 필터링
- RTL 디자인에서 정확한 문제 위치 파악



3 CDC Analysis

칩의 복잡성이 증가함에 따라 설계자는 시장 진입 시간, 고성능 및 저전력 요구 사항을 해결하기 위해 첨단 멀티 클럭 기술 및 IP 통합에 점점 더 의존하고 있습니다. Analyze Plus는 이러한 주요 문제를 해결하기 위해 전체 칩 클럭 도메인 교차 (CDC), 최장 경로을 위한 사전 합성 및 Grey Cell (BPS's IP) 방법론을 제공합니다.

기능

- GUI 또는 batch mode (Tcl base)에 의한 CDC 분석
- 다향한 시나리오에도 쉽게 CDC 분석을 수행 할 수 있음.
- 특정 clock group check을 통한 쉬운 설정
- 전체 TCL parser을 통해 이미 설정된 clock과 domain을 읽어 냄.
- clock의 상호 연관성을 확인 하여 상호 교차하는 clock의 동기화 문제를 인식할 수 있음.
- Clock Domain Crossing Analysis Types:
  - Missing synchronizers
  - Re-converging nets
  - Combinational logic in synchronizers
  - Combinational logic before synchronizers

쉬운 설정

Blue Pearl eases design set up with automatic Clock and reset identification, SDC input of Domain information, understanding of clock generator blocks to propagate clocks and our advanced clock interaction diagram.

Blue Pearl은 자동 클럭 및 리셋 식별, 도메인 정보의 SDC 입력, 클럭 생성기 블록의 propagate clocks에 대한 이해 그리고 클럭 상호 작용 다이어그램으로 구성되어 있어 쉽게 설정을 할 수 있습니다.

4 자동 SDC 생성

RTL 설명에서 false 및 multi-cycle path를 식별하고 검증을 위한 SVA 또는 PSL assertions의 구현을 위한 SDC를 작성합니다. SDC 생성은 iteration을 줄여 timing closing을 더 빨리 달성하고 설계 위험을 최소화 할 수 있습니다.

특징

- 빠른 FSM 검증 및 behavior analysis의 제어
- false and multi-cycle paths의 순차적 분석
- 다음과 같은 타이밍 예외 조건 생성:
  - 클록 도메인을 교차하는 신호의 신호를 대문자로 표시
  - 리셋 및 제한된 신호
  - 레지스터 구성
  - Functional false paths (FPs)
  - Multicycle paths (MCPs)
  - 순환 신호가 블록 포트에서 분리되는 블록 레벨 MCP
- 서로 다른 SDC file의 제약 조건 비교
- block 레벨의 timing constraints을 top-level constraints로 반영하여 사용 할 수 있음

Accelerates Timing Closure

Blue Pearl의 SDC는 자동으로 타이밍 예외, 즉 잘못된 경로와 다중 사이클 경로를 찾아 주고 해당 정보를 implementation tools에 제공합니다. Timing closure에 도움이 되는 다른 기능으로는 최대 팬 아웃 확인, if-then-else depth 그리고 가장 긴 경로 (longest path) 기능이 있습니다.

5 설계 관리 Dashboard

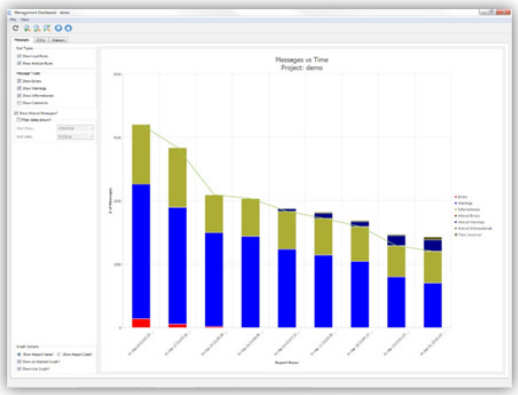
Blue Pearl Management Dashboard는 ASIC, FPGA 및 IP RTL 디자인 규칙 및 CDC 검사에 대하여 실시간으로 가시화 하여 보여 드리고 있어 설계일정, 위험성 및 전반적인 설계 품질을 잘 평가 할 수 있도록 도움을 드리고 있습니다.

기능

- 매일 매일 waivers , CDC, log file message 등을 감시함으로써 RTL 검증 경과를 실시간으로 보실 수 있도록 제공하고 있습니다.
- 오류, 경고, 의견 및 정보를 생략하거나 표시하도록 보고서 사용자가 정의 할 수 있습니다.
- Interactive and batch mode서 작동하므로 개별 시스템 설계에 유용합니다.
- Microsoft office에서 문서 및 표준 보고서를 쉽게 만드실 수 있도록 데이터를 내보낼 수 있어 프로그램 업데이트 및 디자인 검토에 도움이 되실 수 있도록 해 드리고 있습니다.
- Windows 및 Linux 운영체제 모두에서 실행됩니다.

Time and Risk Management

측정 할 수 없는 것은 관리 할 수 없습니다. 설계주기의 진행 상황을 시각적으로 파악하면 설계자와 관리자는 검증 진행 상황을 추적 및 모니터링 할 수 있습니다. 관리 대시 보드는 매일 진행 상황을 추적하고 실행되어 보다 정확한 일정 예측과 design cycle slosing 에 드는 전체 비용을 추정할 수 있도록 도움을 드립니다. 프로젝트 상태에 대해 실시간으로 보여 드리고 있어 이를 통해 사용자는 수정된 사항, waiver된 내용 및 아직 해결해야 할 사항을 볼 수 있습니다.



GUI 및 Tcl 플로우 모두에 대해 보고서를 생성 할 수 있으며 Microsoft Office 도구로 쉽게 내보낼 수 있으므로 설계 검토를 위한 문서를 빠르고 쉽게 작성할 수 있습니다.

Internet of Things

IoT 보안, 안전하게 연결된 세상을 위한 필수 요소

맥심 인터그레이티드 코리아
류제필 부장

우리 주위 사물들의 연결이 점점 더 늘어나고 있다. 시스코는 커넥티드 기기 수가 2020년에는 500억 대에 이를 것으로 전망했다. ARM은 더 나아가 2035년에 사물인터넷(IoT) 디바이스의 개수가 1조에 다다를 것으로 예상하고 있다.

IoT는 업무와 일상에서 효율성을 높이면서 연결되어 있다. 오늘날 사물은 내가 언제 집에 있는지, TV에서 어떤 프로를 보는지, 집에서 어떤 가전이 전기를 소비하는지를 알고 있다. 가정에서 활용되는 IoT 디바이스는 전기 공급, 온도 설정, 차고 문 개폐 등을 제어한다. 스마트한 사물은 이렇게 사용자의 사적인 데이터를 수집한다. 이런 상황에서 보안은 IoT가 풀어야 할 큰 숙제가 되었다.

가정용 IoT 외에 산업용 IoT도 있다. 산업용 IoT를 겨냥한 위협은 가정용 IoT보다 더 많은 피해를 불러온다. 멀웨어(malware) 같은 보안 위협에 산업용 IoT가 피해를 입으면 도시에 전기가 끊기고, 발전소가 멈추고, 공장 생산 라인이 중단될 수 있다.

사이버 보안 전문업체 맥아피와 전략국제문제연구소(CSIS)는 올해 2월 발표한 보고서에서 지난 한 해 사이버 범죄가 글로벌 경제에 미친 피해액을 6000억 달러로 추산했다. 이는 전세계 GDP의 0.8%에 해당한다. 사이버시큐리티 벤처스는 2021년에 발생될 전세계 사이버 범죄 피해액을 6조 달러로 전망했다.

해킹과 보안 침해 사고가 날마다 뉴스 헤드라인을 장식하는 가운데도 제조업체 대부분은 보안 설계를 나중 문제로 취급한다. 강력한 보안을 위해서는 시간과 자원, 비용이 많이 든다는 선입견 때문이다.

보안에 신경쓰지 않은 대가

보안 침해는 줄어들 기미가 없다. 2017년 대대적인 워너크라이(WannaCry) 랜섬웨어 공격은 유럽, 남미, 아시아, 북미 등 최소 150개 국가에서 병원, 대학, 제조업체, 기업, 정부 기관 컴퓨터에 피해를 입혔다. 2016년 가을에는 CCTV 비디오 카메라와 DVR을 해킹하는 대규모 인터넷 공격이 있었다. 이는 미라이(Mirai) 멀웨어 스트레인 기반의 봇넷 소행이었다. 잘 알려진 대규모 공격 외에도 소비자와 기업 모두가 우려할만한 사고는 끊임 없이 일어나고 있다. 제품과 시스템의 연결성(connectivity)이 높아질수록 해커의 공격은 정교해지고 산업 분야에 미치는 위험성도 확대된다.

보안 설계를 간과하면 이는 매출 저하, 브랜드 손상, 심지어 인명 피해까지도 일으킬 수 있다. 피해가 발생한 후 뒤늦게 시스템을 손질하는 것은 효과적이지 않다. 제품을 출시하고 개발 비용을 낮추려는 것은 당연하지만 기업은 보안 공격을 받았을 때 얼마만큼 피해가 발생할지 신중하게 생각해야 한다. <그림 1>을 보면 보안에 신경 쓰지 않았을 때 발생하는 피해가 보안을 구현하는 비용보다 크다는 사실을 알 수 있다.

Without Security IC	
10 Mu Sales @ $10	$100M
Less 15% counterfeit	-$15M
Net Sales	**$85M**
COGS, 10Mu @ $3	-$30M
Profit	**$55M**
With Secure Authenticator @$0.50	
10 Mu Sales @ $10	$100M
Less 0% counterfeit	$0M
Net Sales	**$100M**
COGS, 10Mu @ $3.50	-$35M
Profit	**$65M**

그림 1. 위조로 인한 피해액이 보안을 구현하기 위한 비용보다 더 높다.

임베디드 보안 IC로 신뢰받는 보안 구축

하드웨어 기반 보안은 사이버 공격자가 디자인의 물리 계층(physical layer)을 조작하기 어렵게 만든다는 점에서 보안의 견고함을 보장한다. 물리 계층은 멀웨어가 디자인의 운영체제나 가상 계층으로 침투하지 못하도록 한다. 설계 작업 초기 단계에 디자인 토대 계층부터 보안을 구축하고 이를 통해 그 위에 오는 모든 계층을 보호할 수 있다.

변경 불가능한 내부 메모리에서 코드를 실행하는 마이크로컨트롤러(MCU) 같은 보안 집적회로(IC)를 사용함으로써 전자 장비의 하드웨어에 대한 공격을 방어할 수 있다. 이 MCU의 ROM에 스타트업 코드를 저장한다. 이것을 변경 불가능한 '신뢰점(root of trust)'으로 삼을 수 있다. 변경 불가능하고 신뢰할 수 있는 소프트웨어를 사용해 애플리케이션 소프트웨어의 서명을 검증하고 인증한다.[1] 토대 계층부터 하드웨어 기반 '신뢰점' 기법을 구현함으로써 디자인으로의 잠재적 침투를 차단할 수 있다.

보안 MCU와 보안 인증 디바이스 같은 임베디드 보안 IC는 각각의 센서 노드부터 클라우드까지 전체적인 시스템을 보호하는 턴키 솔루션을 제공한다. 그러나 모든 보안 IC가 똑같이 개발되는 것은 아니다. 어떤 보안 MCU는 가격, 전력 소모, 복잡한 펌웨어 개발로 IoT 디바이스나 엔드포인트에 적합하지 않을 수 있다. 이럴 때 펌웨어 개발이 필요치 않은 임베디드 커넥티드 제품용 암호화 컨트롤러가 하나의 대안이 될 수 있다. 맥심 MAXQ1061 딥커버(DeepCover) 디바이스가 좋은 예다. 이 코프로세서를 시작 단계부터 디자인에 포함하거나 기존 디자인에 통합함으로써 디바이스의 기밀성, 신뢰성, 무결성을 보장할 수 있다.

보안 인증 디바이스는 일련의 핵심적인 고정 기능 암호화 동작, 보안 키 저장, IoT 및 엔드포인트 보안에 필요한 기능을 제공해야 한다. 보안 인증 디바이스는 IP(Intellectual Property)를 보호하고 복제를 방지하며 주변장치, IoT 디바이스, 엔드포인트를 인증하는 경제성 뛰어난 수단이 될 수 있다.

1) http://www.embedded.com/design/safety-and-security/4438300/Securing-the-IoT--Part-2---Secure-boot-as-root-of-trust-

임베디드 보안 기술을 선택할 때는 암호화 엔진과 보안 부트 로더를 포함하는 보안 MCU를 선택해야 한다. 이를 통해 암호 분석 공격, 물리적 위변조, 리버스 엔지니어링 같은 공격을 막을 수 있다. 디자인 쉬프트(Design SHIFT)는 캘리포니아주 멘로파크에 위치한 디지털 보안 및 컨슈머 제품 엔지니어링 회사다. 이 회사는 보안용 PC ORWL을 설계할 때 2 팩터(two-factor) 인증과 물리적 공격에 대한 방어가 필요했다. 강력한 신뢰점 보안을 위해 이 회사가 선택한 솔루션이 MAX32550 딥커버 ARM Cortex-M3 보안 MCU다.

존재하지 않는 키는 훔칠 수 없다: 칩DNA(ChipDNA) 기술

보안 IC로 PUF(Physical Unclonable Function)라는 좀 더 진화된 암호화가 도입되고 있다. PUF는 IC 디바이스의 복합적이고 다양한 물리적/전기적 특성으로부터 도출되는 함수다. PUF는 제조 시에 발생되는 임의적인 물리적 요소(예측 불가능 및 조작 불가능)를 바탕으로 해 복사나 복제가 거의 불가능하다.[2] PUF 기술은 해당 IC의 물리적 전기적 특성을 이용한 고유의 디지털 지문을 생성한다. 이것을 고유 비밀 키로 사용함으로써 인증, 신원확인, 위변조 방지, 하드웨어-소프트웨어 바인딩, 암호화/암호해독 같은 알고리즘을 지원한다.

맥심의 PUF 회로는 암호화 키를 생성하기 위해 기본 MOSFET(금속 산화막 반도체 전계 효과 트랜지스터) 디바이스가 자연적으로 발생시키는 임의적 아날로그 특성을 기반으로 한다. 이 솔루션을 '칩DNA' 기술이라고 한다. 이 기술은 고유의 특허 기법을 사용해 각 PUF 회로가 생성하는 고유의 바이너리 값이 온도와 전압, 디바이스 노후화에 대해서 반복적으로 일관되게 한다. 고유의 바이너리 값이 필요에 따라 PUF 회로에 의해 생성되었다 사라지며, 실제 칩 상의 비휘발성 메모리에 저장되지 않아 높은 수준의 보안을 자랑한다.

물리적 공격으로 비밀 키가 유출 가능했던 이전 보안 디바이스와 달리 PUF 기반 디바이스는 물리적 공격에 취약하지 않다. 존재하지 않는 키를 훔칠 수는 없기 때문이다. 또한 PUF 기반 디바이스가 침투적 물리 공격을 당하면 이 공격 시도 자체가 PUF 회로의 전기적 특성을 변화시켜 공격을 차단한다. 칩DNA PUF 기술은 프로세스, 전압, 온도, 노후화에 대해 뛰어난 안정성을 제공한다.

칩DNA는 미국 국립표준기술연구소(NIST) 무작위 테스트 세트의 PUF 출력 평가를 통과했다. 맥심 DS28E38 보안 인증장치는 칩DNA PUF 기술을 적용한 맥심의 첫 번째 보안 IC다. DS28E38은 맥심 칩DNA 기술을 탑재해 침투형 공격에 영향을 받지 않는다. 이는 칩DNA 기반의 루트 암호 키가 메모리나 다른 안정 상태(static state)에 위치하지 않기 때문이다.

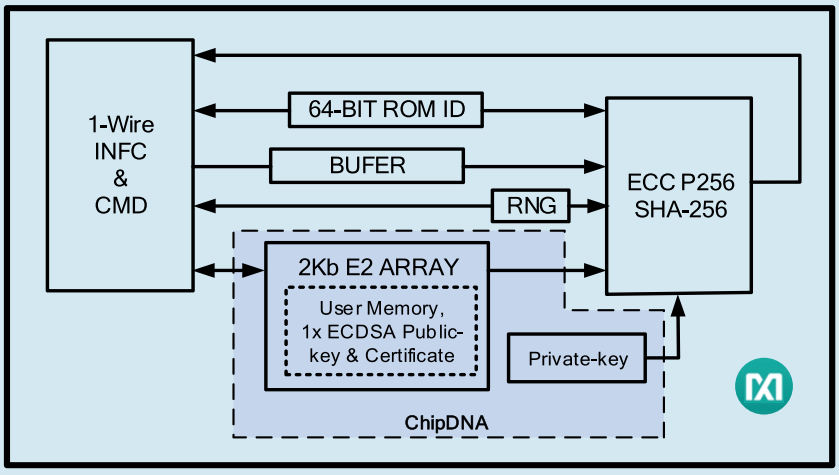


그림 2. 칩DNA PUF 기술을 적용한 DS28E38 딥커버 보안 IC의 블록 다이어그램

맥심 PUF 회로는 기본적인 MOSFET 반도체 디바이스에서 자연스럽게 발생하는 랜덤 아날로그 특성을 기반으로 암호 키를 생성한다. 이 회로는 필요할 때 디바이스 고유 키를 생성하고, 사용되지 않을 경우 고유 키는 바로 사라진다. DS28E38은 물리적 침투형 공격을 받으면 회로의 민감한 전기적 특성이 변해 추가적인 보안 침해를 막아준다. 이 밖에도 보안 IC 키가 암호 연산에 직접 사용돼 키 관리가 단순해지거나 또는 관리할 필요조차 없어진다.

2) https://en.wikipedia.org/wiki/Physical_unclonable_function

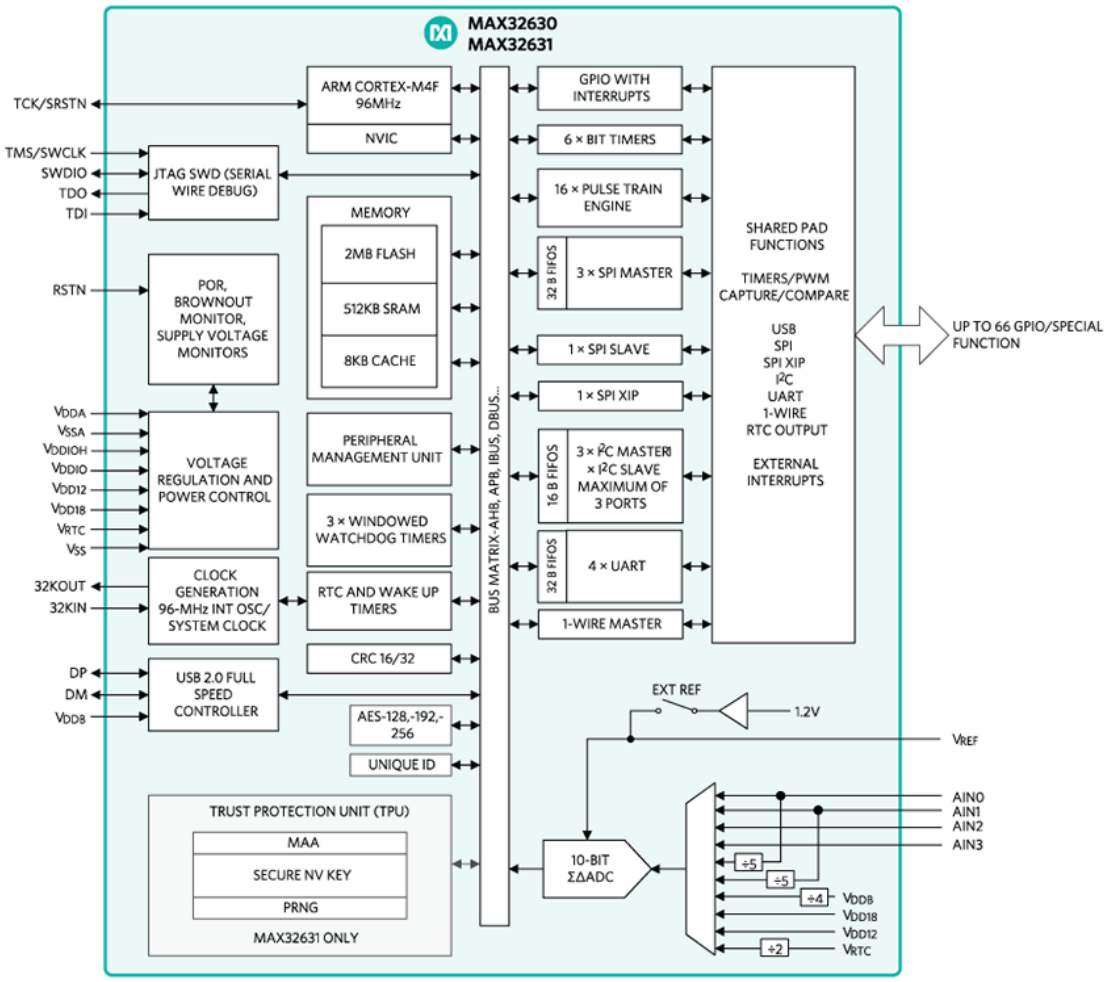


그림 3. 저전력 ARM Cortex-M4 프로세서를 탑재한 고성능 암호화 엔진이 내장된 MAX32631

보안 기능이 강화된 웨어러블용 MCU

개발 초기부터 상대적으로 낮은 비용으로 효과적으로 IoT 노드에 보안을 설계할 수 있는 기술도 있다. 오늘날 저전력 MCU와 컴패니언 프로세서는 보안 기능을 갖추고 있다. 이 보안 기능으로 신용 카드 단말기와 동일한 암호화 툴을 장착한 블루투스 심장 박동 센서를 만들 수 있다. IoT 노드는 ECC (Elliptic-Curve Cryptography) 같은 고급 기술을 이용해 시스템 비밀 키를 위험에 노출시킬 필요 없이 시스템을 광범위하게 구축하도록 한다. 특별한 하드웨어를 이용해 암호화 기술을 구현함으로써 IoT 노드는 소프트웨어를 이용할 때보다 더욱 빠르고 적은 전력 소비로 보안 기능을 수행한다.

보안은 IoT 설계에서 더 이상 선택이 아닌 필수사항이 됐다. 맥심과 같은 많은 반도체 기업들은 IoT 디바이스가 한번 구축되면 더 이상 신경 쓰지 않아도 될 정도로 신뢰도를 높이는 노력을 기울이고 있다.

IoT는 신뢰 가능하고 보이지 않는 상태를 유지해야 한다. 많은 시간과 비용을 들이지 않고도 강력한 보안 설계가 가능하다는 사실은 여러 사례를 통해 이미 증명됐다. 설계 초기 단계부터 보안을 도입하고 하드웨어 기반 보안을 추구함으로써 사이버 범죄에서 자유로운 연결된 세상을 기대해본다.

저자정보

류제필 부장
소속 맥심 인터그레이티드 코리아
주 연구분야 Security & Communications
E-mail JP.Ryu@maximintegrated.com

산업통상자원부 beyond leading technology KIAT KSIA 한국반도체산업협회
SAMSUNG 삼성전자 SK hynix MagnaChip Amkor Technology®
반도체설계교육센터 (IDEC) Homepage. http://www.idec.kr TEL. 042-350-8540 | 본 월간지는 "지능형반도체 전문인력양성사업(2018)"의 일환으로 수행되었습니다.