

900 MHz 대역 RFID 시스템의 무선 인터페이스  
표준화 동향

황태욱 · 김영수 ·  
박경환\*  
경희대학교 전자정보대학  
전파통신공학,  
\*한국전자통신연구원

요 약

본 고에서는 최근 많은 관심을 갖고 있는 900 MHz UHF 대역을 사용하는 RFID 시스템의 무선 인터페이스 표준에 대해 살펴본다. 900 MHz UHF 대역의 RFID 시스템은 유통, 물류에 사용될 것으로 기대되기 때문에 국제표준화기구인 ISO와 국제 민간 표준화 기구인 EPCglobal에서 무선 인터페이스 표준을 세우고 있다. 특히 2004년부터 이뤄진 EPCglobal의 EPC Class 1 Generation 2 표준은 향후 ISO의 900 MHz 대역 RFID 시스템의 새로운 무선 인터페이스 표준으로 정해질 것으로 기대되고 있어 더욱 관심을 모으고 있다. 이에 본 고에서는 900 MHz 대역 RFID 무선 인터페이스 표준인 ISO/IEC의 ISO 18000-6과 EPCglobal의 EPC Class 1 Generation 1, Generation 2를 중심으로 900 MHz 대역 RFID 시스템의 무선 인터페이스 표준화 동향을 살펴보았다.

I. 서 론

이동 통신과 IT 기술의 발전에 따른 정보 통신 혁명이 우리에게 보다 편리한 세상을 열어주면서 정보 통신 기술에 대한 관심을 더더욱 커져만 가고 있다. 더욱이 최근 유비쿼터스(Ubiquitous)라는 새로운 기술이 소개되면서 많은 사람들의 관심은 유비쿼터스 시대로의 진화로 옮겨지고 있다.

유비쿼터스란 사용자가 네트워크나 컴퓨터를 직

접 접근하지 않고, 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 정보 통신 환경을 말한다. 유비쿼터스 기술의 가장 근본이 되는 기술은 모든 사물을 유일하게 식별할 수 있는 객체 인식 기술이라고 할 수 있다<sup>[1]</sup>. 따라서, 유비쿼터스 환경 구현의 필수 요건은 모든 사물들을 인식하는 것이 필요하며, 사물을 식별할 수 있게 만드는 장치가 필요하다. 이러한 필요 기술을 만족하는 것이 RFID(Radio Frequency Identification)이다. RFID는 리더(Reader 또는 Interrogator)를 통해 접촉하지 않고 태그(Tag)의 정보를 판독하거나 인식하는 기술이다. 태그 내에 있는 초소형 반도체에 사물을 식별할 수 있는 정보를 넣고, 이것을 사물에 붙여 놓으면 리더의 무선 주파수를 이용하여 사물을 판독, 인식, 관리할 수 있게 된다. RFID는 대용량의 데이터를 무선으로 전송할 수 있어 물류, 유통, 전자 지불, 보안 등 우리 사회 전반에 걸쳐서 응용될 것으로 기대된다. 또한, 차세대 유비쿼터스 사회의 핵심 기술이기도 하다<sup>[8]</sup>.

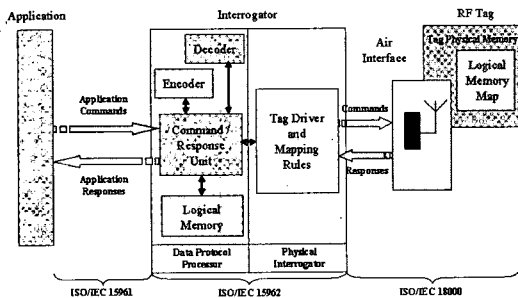
RFID 기술은 1990년대 중반부터 국제표준화기구(ISO)에서 국제 표준화가 논의되기 시작하였다. ISO JTC1/SC17에서 비접촉형 IC 카드의 표준화에 대해 2001년 관련 규격이 모두 제정되었다. RFID 시스템은 전파를 사용해서 리더와 태그간의 통신을 하기 때문에, 국제적인 규격화된 표준없이 개발이 진행된다. 향후 글로벌 관점에서 혼란과 수많은 기준들이 존재하는 문제점이 발생하기 때문에 이를 미연에 방지코자 ISO의 자동 인식 기술 분과인 ISO JTC1/

SC31에서 본격적으로 UHF 대역을 비롯한 실용 주파수별 무선 인터페이스, 데이터 방식 등의 표준화를 거의 마무리하게 되었다. 그 결과 여러 가지 기준들로 존재하던 RFID 기술들이 국제 표준에 맞게 재정비되고 있다. 현재 RFID 관련 국제 표준화 기구는 ISO/IEC JTC1이고 국제 민간단체표준화기구는 EPCglobal 및 uID 센터 등이 있다.

본고는 900 MHz 대역에 대한 RFID 무선 인터페이스 표준을 국제표준화기구인 ISO/IEC의 표준과 EPCglobal에서 제정한 표준 두 가지를 살펴보고, 두 표준의 차이점과 무선 인터페이스 방법 등에 대해서 논하고자 한다. II장과 III장에서는 RFID 시스템의 무선 인터페이스 표준 동향에 대해서 설명하며, IV장에서는 900 MHz 대역의 RFID 무선인터페이스표준 중 ISO/IEC의 표준과 EPCglobal 표준의 무선 인터페이스 절차에 대해서 설명한다. 그리고 V장에서 결론을 맺는다.

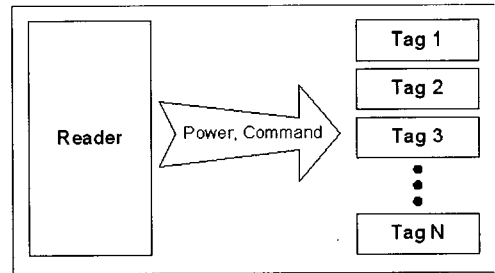
## II. RFID 시스템의 무선 인터페이스

[그림 1]은 ISO/IEC에서 제안한 RFID 시스템 구성을 보여주고 있다. [그림 1]에서 보는 바와 같이 RFID 시스템은 리더(Reader)와 태그(Tag)로 구성되어 있다. RFID 태그는 태그 내부에 독립된 전원의 존재 여부에 따라 능동 태그와 수동 태그로 나뉜다<sup>[4]</sup>.

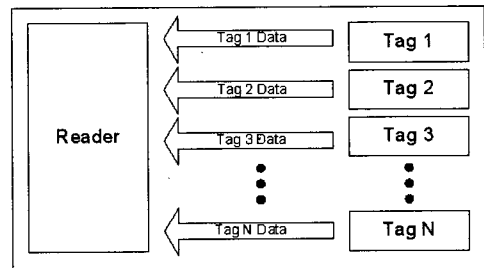


[그림 1] ISO/IEC에서 제안한 RFID 시스템 구성<sup>[4]</sup>

태그 내의 독립된 전원이 존재하고 이 전원을 이용하여 태그가 직접 RF 신호를 송신할 수 있다면 이를 능동 태그라 하고, 독립된 전원이 존재하지 않고 리더로부터 받은 RF 신호를 받아 그 에너지를 이용하여 리더에 데이터를 보내는 태그를 수동 태그라고 한다. 보통 능동 태그가 수동 태그에 비해 인식 거리가 길지만 가격이 비싸고, 태그 내에 존재하는 전원의 수명이 유한하기 때문에 태그 자체의 수명이 유한해지는 단점이 있다. 반면에 수동 태그는 리더로부터 받은 RF 신호의 에너지를 이용하기 때문에 인식 거리가 짧은 반면에 가격이 싸고, 반영구적으로 사용할 수 있는 장점이 있다. 따라서, 물류, 유통 등에 사용될 것으로 기대되는 RFID 시스템은 가격이 비교적 싸고, 반영구적으로 사용할 수 있는 수동 태그에 대한 연구와 개발에 초점이 맞춰지고 있다. 수동 태그 RFID 시스템에서 리더가 태그를 인식



(a) 리더 → 태그



(b) 태그 → 리더

[그림 2] 리더와 태그간의 통신

하는 과정은 [그림 2]와 같이 이뤄진다. 리더는 리더 자신의 RF 신호가 미치는 범위 내의 모든 태그에게 요청(Request) 명령을 브로드캐스트(Broadcast) 한다. 요청 명령을 받은 태그들은 리더에게 데이터를 전송하게 된다. 이때, 여러 개의 태그가 리더에 응답하게 되고, 태그와 태그 사이에 데이터 충돌이 발생할 수 있다. 이러한 태그 데이터 충돌을 회피할 수 있는 충돌 회피 알고리즘을 통해 리더는 온전한 태그 데이터를 수신하게 된다. 이와 같이 무선을 이용해 리더가 태그를 인식하기 위한 전반적인 과정을 무선 인터페이스라고 한다. 이러한 무선 인터페이스에서 사용되는 RF 주파수 대역이 여러 가지로 존재하는데 ISO/IEC에서는 현재 5개의 주파수 대역에 대해서 표준안이 논의되거나 결정되었고, EPCglobal에서는 2개의 주파수 대역에 대해서 표준안이 결정되었다<sup>[7]</sup>.

### 2-1 ISO/IEC의 RFID 무선 인터페이스 표준

ISO/IEC의 RFID 무선 인터페이스 표준은 SG3에서 다루고 있다. SG3는 리더와 태그간의 무선 주파수 통신 방식의 표준을 정의한다. <표 1>은 ISO/IEC JTC1의 국제 표준 분류를 보여주고 있다. <표 1>에

서 SG3가 RFID 무선 인터페이스 표준과 관련된 부분이다. 무선 인터페이스의 ISO/IEC 18000 시리즈에서 135 kHz 이하는 가축 관리, 13.56 MHz는 도서 관리, 2.45 GHz는 소형 무선 응용 분야에서 실제적인 활용이 이뤄지고 있다. UHF 대역 860~960 MHz는 세계적 유통 물류 관련 기관인 EAN/UCC의 글로벌 태그 프로젝트, EPCglobal의 EPC 프로젝트 등에 적용되고 있다. UHF 대역 433 MHz는 다른 무선 인터페이스와는 달리 능동형 태그 방식으로 항만의 컨테이너에 적용 예정에 있다.

각 무선 인터페이스 작업별 표준화는 지난 2004년 9월에 2.45 GHz 대역과 433 MHz 대역의 능동 태그 방식, 135 kHz 이하 대역과 13.56 MHz 대역, 900 MHz 대역에 대한 무선 인터페이스 국제 표준이 차례로 제정되었고, 5.8 GHz 대역은 위원회 단계에서 부결되어 철회되었다. 아울러, 지난 2005년 1월에 열린 JTC1/SC31 RFID 무선 인터페이스 국제 표준화 회의에서 ISO/IEC 18000-6(UHF 무선 인터페이스)의 개정 방향과 EPC Class 1 Generation 2 기반의 ISO Draft 작업 방향이 논의되었다. 차세대 UHF 시스템 ISO 18000-6c의 국제 표준화 계획이 확정되었다<sup>[7]</sup>.

<표 1> ISO/IEC RFID 국제표준 분류<sup>[4]</sup>

그룹	그룹명	ISO/IEC	작업명	비고
SG1	Data Syntax	15961	Tag Commands	데이터 프로토콜
SG2	Tag 식별	15962	Data Syntax	
SG3	Air Interface	15963	RFID Tag ID	태그 식별
		18000-1	Generic Parameters	파라미터 규정
		18000-2	below 135 kHz	가축 관리
		18000-3	13.56 MHz	도서 관리
		18000-4	2.45 GHz	Traceability
		18000-5	5.8 GHz	ITS, 부결
		18000-6	UHF 860~960 MHz	유통, 물류
		18000-7	UHF 433 MHz(Active)	컨테이너
SG4	ARP	TR18001	Application 요구사항	적용 조건 조사

이러한 여러 무선 인터페이스 표준 중에 최근 가장 관심을 모으고 있는 것은 900 MHz 대역의 주파수를 사용하는 표준이다. 900 MHz 대역은 주파수 특성이 다른 대역에 비해 우수하고, 인식 거리가 비교적 긴 장점을 갖고 있다. 특히, ISO/IEC의 분류에 의하면 900 MHz 대역의 RFID 시스템은 유통, 물류에 사용될 예정이어서 RFID 시스템의 도입을 가장 반기고 있는 유통, 물류 업계의 관심이 모아지고 있고, 정부의 정책적 지원에 의해 900 MHz 대역 표준인 ISO 18000-6 표준이 많은 관심을 모으고 있다. ISO 18000-6 표준은 Type A와 B 두 가지가 존재한다. 이에 대한 자세한 무선 인터페이스 표준은 다음 장에서 설명한다.

## 2-2 EPCglobal의 RFID 무선 인터페이스

민간 표준단체인 EPCglobal의 RFID 무선 인터페이스 표준은 13.56 MHz 대역과 900 MHz 대역에 대해서 정하고 있다. <표 2>는 EPCglobal의 RFID 표준을 보여주고 있다. EPCglobal 2~EPCglobal 5까지가 RFID의 무선 인터페이스 표준이다.

ISO/IEC의 ISO 18000-6과 대응되는 EPCglobal의

900 MHz 대역 표준은 <표 2>에서 EPCglobal 2와 4, 5이다. EPCglobal 2는 900 MHz 대역에 대한 EPCglobal 표준 중 Class 0에 대한 규정이며, EPCglobal 4는 EPC Class 1 Generation 1(이하 EPC C1 Gen.1), EPCglobal 5는 EPC Class 1 Generation 2(이하 EPC C1 Gen.2)에 대한 규정이다. EPC Class 0는 오로지 읽을 수만 있는 RFID 태그의 IC 칩을 사용했을 경우의 표준이며, Class 1은 한 번 쓸 수 있고 그 다음부터는 읽을 수만 있는 태그 칩을 사용하는 경우의 표준이다. Class 1은 다시 Generation 1과 Generation 2로 나뉘는데 Generation 2는 Generation 1의 수정 버전이라고 보면 된다. EPC C1 Gen.2가 나오게 된 배경은 EPCglobal이 900 MHz 대역의 RFID 표준을 Generation 1에서는 Class 0와 Class 1 두 가지 무선 인터페이스 프로토콜을 갖게됨으로써 멀티 프로토콜 리더가 아니면 두 종류의 태그를 인식할 수 없는 문제가 존재했기 때문이다. 따라서, 하나의 900 MHz 대역으로 표준을 통합하는 과정에서 한 번 쓰고 여러 번 읽을 수 있는 Class 1으로 통합하여 수정 버전을 내놓게 된 것이다.

본 고에서는 다음 장에서 EPC C1 Gen.1과 EPC

<표 2> EPCglobal 표준화 분류<sup>15)</sup>

표준 순번	표준 이름
EPCglobal 1	EPC Tag Data Specification
EPCglobal 2	900 MHz Radio Frequency(RF) Identification Tag Specification(Class 0)-Candidate recommendation
EPCglobal 3	13.56 MHz ISM Band Class 1 Radio Frequency(RF) Identification Tag Interface Specification(Class 1)
EPCglobal 4	860~930 MHz Class 1 Radio Frequency(RF) Identification Tag Radio Frequency & Logical Communication Interface Specification(Class 1 Version 1)
EPCglobal 5	Radio Frequency Identity Protocols-Generation 2 Identity Tag(Class 1): Protocol for Communication at 860~960 MHz(Generation 2)
EPCglobal 6	Reader Protocol
EPCglobal 7	Savant Specification
EPCglobal 8	Physical Markup Language(PML) Core Specification, XML SCHEMA and Instance Files
EPCglobal 9	Object Name Service(ONS) Specification V1.0

C1 Gen.2에 대해서 자세히 설명한다.

### III. ISO 18000-6

ISO/IEC의 900 MHz 대역 표준인 ISO 18000-6은 Type A와 Type B 두 가지가 존재한다. 이 절에서는 ISO 18000-6의 RFID 무선 인터페이스 표준에 대해서 설명한다.

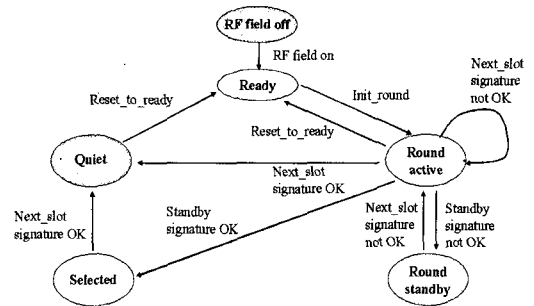
#### 3-1 ISO 18000-6 Type A

ISO 18000-6 Type A는 860~960 MHz 대역을 이용하며, 충돌 회피 방법은 ALOHA 알고리즘을 사용한다. 변조 방법으로는 AM(Amplitude Modulation)을 사용한다. 데이터 코딩은 리더에서 태그로 전송될 때는 PIE(Pulse Interval Encoding)를 사용하며, 태그에서 리더로 전송될 때는 FM0를 사용한다. <표 3>은 리더와 태그 간 통신에 대해서 요약하여 보여주고 있다<sup>[1]</sup>.

[그림 3]은 ISO 18000-6 Type A의 태그 State 블록도를 보여주고 있다<sup>[1]</sup>. [그림 3]에서 보면 리더의 명령에 따라 태그가 이동할 수 있는 State와 리더가 태그를 어떤 과정(명령)을 통해 인식하는지를 확인할 수 있다.

<표 3> ISO 18000-6 Type A 주요 파라미터

분류	내용
동작 주파수	860~960 MHz
리더→태그 코딩 방법	PIE(Pulse Interval Encoding)
태그→리더 코딩 방법	FM0
변조방법	AM(Amplitude Modulation)
전송 속도	33 또는 40 kbps
충돌 회피 알고리즘	ALOHA
태그 고유 Bit 수	64 bits
에러 체크 방법	16 bits CRC
태그 인식 개수	최대 256개 Tags



[그림 3] ISO 18000-6 Type A 태그 State 블록도<sup>[1]</sup>

먼저, 리더는 태그에 최초의 명령을 송신하기 전에 채널이 비어 있는지를 확인하는 단계를 거친다. 이 시간을 Taq(Type A Quiet Time)이라고 하며, 적어도 300 ms 이상의 Taq이 유지되어야 리더는 채널이 비어 있다고 판단하고 태그에게 명령을 전송할 수 있다. 이 시간 동안 리더는 계속해서 RF Field를 태그에 보내게 되고, RF Field OFF 상태에 있었던 태그들은 동작할 수 있는 충분한 에너지를 리더의 RF Field로부터 공급받음으로서 Ready State로 이동해 동작 준비 상태에 접어들게 된다. 만약, 일정 시간 이상 RF Field를 받지 못했거나 에너지가 미약한 경우, 태그는 동작 상태가 되지 않아 리더의 어떤 명령에도 응답하지 않는다.

리더로부터 충분한 RF Field를 받아 동작 상태가 된 태그들은 이제 리더의 명령을 수행할 준비가 된다. 리더는 Ready State에 있는 태그들에게 Init\_round 명령을 내리게 되고, 이 명령을 받은 태그들은 태그 인식 과정을 수행하는 Round Active State로 이동하게 된다. Round Active State에 있는 태그들은 충돌 회피 알고리즘에 의해 충돌 해결 과정을 수행한다. ISO 18000-6 Type A에서는 충돌 회피 알고리즘으로 ALOHA 방법을 사용한다. init\_round 명령 내에 포함된 round 값과 태그 내의 RNG(Random Number Generator)를 이용하여 Round 내에서 자신이 사용할 Slot을 선택하게 된다. 이제 리더는 Round Active

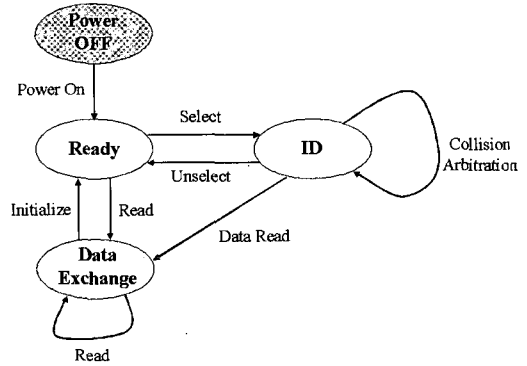
State에 있는 태그들 중 Round 내의 하나의 Slot을 선택하게 되고, 해당 Slot에 오직 하나의 태그만 할당 되었다면, 리더는 해당 Slot의 태그의 메모리에 있는 데이터 또는 SUID(태그 고유번호) 읽기 또는 쓰기를 위해 선택된 태그를 Selected State로 이동시킨다. 이때 선택되지 않은 태그들은 선택된 태그가 읽기/쓰기가 끝날 때까지 Round Active State에서 선택한 자신의 Round와 Slot 값을 유지하면서 Round Standby State에서 대기하였다가, 선택된 태그의 읽기/쓰기가 끝나면 다시 Round Active State로 이동하여 리더의 선택을 기다리게 된다. Selected State에서 선택된 태그는 읽기/쓰기 과정이 끝난 다음 Quiet State로 이동한다. Quiet State로 이동한 태그들은 리더에게 자신의 데이터를 성공적으로 보내어 통신이 끝난 태그들이 모여있는 State이다. 이 상태의 태그들은 현재나 이후의 Round에서 더 이상 인식할 필요가 없는 태그이므로 Reset\_to\_ready 명령에 의해 초기화될 때를 제외하고는 리더의 어떤 명령에도 응답하지 않는다<sup>[1]</sup>.

### 3-2 ISO 18000-6 Type B

<표 4>는 ISO 18000-6 Type B에서 리더와 태그간의 통신 방식을 보여주고 있다<sup>[1]</sup>. ISO 18000-6 Type B는 리더에서 태그로의 전송에서는 Manchester 코딩

<표 4> ISO 18000-6 Type B 주요 파라미터

분류	내용
동작 주파수	860~960 MHz
리더→태그 코딩 방법	Manchester
태그→리더 코딩 방법	FM0
변조방법	AM(Amplitude Modulation)
전송 속도	8 또는 40 kbps
충돌 회피 알고리즘	Binary Tree
태그 고유 Bit 수	64 bits
에러 체크 방법	CRC-16
태그 인식 개수	최대 2 <sup>256</sup> 개 Tags



[그림 4] ISO 18000-6 Type B 태그 State 블록도<sup>[1]</sup>

방법으로 데이터를 코딩하며, 태그에서 리더로의 전송에서는 FM0로 코딩한다. 변조 방법은 ISO 18000-6 Type A와 마찬가지로 AM으로 변조한다. 충돌 회피 방법은 이진 트리(Binary Tree) 방법을 사용한다.

[그림 4]는 ISO 18000-6 Type B의 태그 State 블록도를 보여주고 있다<sup>[1]</sup>. [그림 4]에서 보면 리더의 명령에 따라 태그가 이동할 수 있는 State와 리더가 태그를 어떤 과정과 명령을 통해 인식하는지를 확인할 수 있다.

리더의 인식 범위 내에 있는 모든 태그가 리더로부터 동작에 필요한 에너지를 공급받으면 POWER-OFF State에서 Ready State로 이동한다. Ready State는 리더로부터 태그의 기능을 구동하기 위해 필요한 에너지를 받은 State로 리더의 명령에 응답할 수 있는 State이다. 또한, 태그를 인식한 후 필요한 읽기나 쓰기 과정을 거친 후 대기하는 State이기도 하다. Ready State에 있는 태그들이 리더로부터 Group\_Select 명령을 수신하게 되고, Group\_Select 명령을 제대로 수신한 태그들은 자신의 COUNT 값을 0으로 초기화하고 ID State로 이동하게 된다. ID State에서 COUNT 값을 0으로 초기화한 태그들은 태그 내의 메모리에서 UID 값을 읽어 리더에게 전송한다. 이때, COUNT 값이 0인 태그가 2개 이상이어서 리더의 Select 명령에 2개 이상의 태그가 응답한다면 리더는

Fail 명령을 태그에게 보내게 된다. Fail 명령을 수신한 태그들 중에 COUNT 값이 0이 아니거나 랜덤 변수가 1인 태그들은 COUNT 값을 1만큼 증가시킨다. 만약 Fail 명령을 수신한 태그들 중에 COUNT 값이 0인 태그는 태그 내의 RNG를 통해 COUNT 값을 그대로 유지하면서 랜덤 변수를 생성한다. 이때 새롭게 생성한 랜덤 변수가 0인 태그들은 다시 리더에게 데이터를 전송하게 된다. 이 과정이 ISO 18000-6 Type B의 충돌 회피 과정이다. 이러한 과정을 리더에 응답하는 태그가 하나만 남을 때까지 반복하게 된다. 하나의 태그가 선택되면 리더는 선택된 태그에게 Success 명령을 보내게 되고, Success 명령을 수신한 태그는 자신의 COUNT 값을 1만큼 감소시킨다. 이때, 이 태그는 리더와 통신을 할 수 있는 태그로 선택되었기 때문에 리더는 이 태그에게 DATA\_READ 명령을 보내게 되고, 이 태그는 ID State에서 Data Exchange State로 이동하게 된다. Data Exchange State로 이동한 태그는 리더로부터 Read 명령을 받게 되면 태그 메모리의 데이터를 리더로 전송하게 된다. 전송이 성공적으로 끝나면 리더는 태그에게 Initialize 명령을 보내고, 이 명령을 수신한 태그는 Ready State로 이동하게 된다<sup>[1]</sup>.

#### IV. EPC Class 1

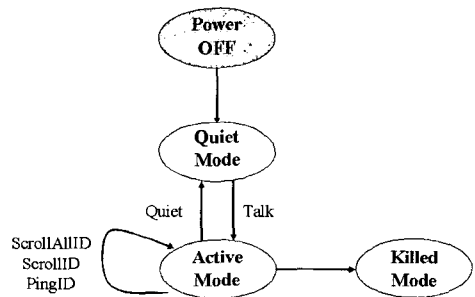
민간표준단체인 EPCglobal의 900 MHz 대역 무선 인터페이스 표준은 Class 0와 Class 1이 존재하며, Class 1은 다시 Generation 1과 Generation 2로 나뉜다. 본 고에서는 EPC Class 1 Generation 1과 EPC Class 1 Generation 2에 대해서 다루겠다.

EPC Class 1에서 사용되는 태그의 ID는 EPC code를 사용하며 일반적으로 64 또는 96 비트가 사용된다<sup>[3][4]</sup>.

##### 4-1 EPC Class 1 Generation 1

<표 5> EPC C1 Gen.1의 주요 파라미터

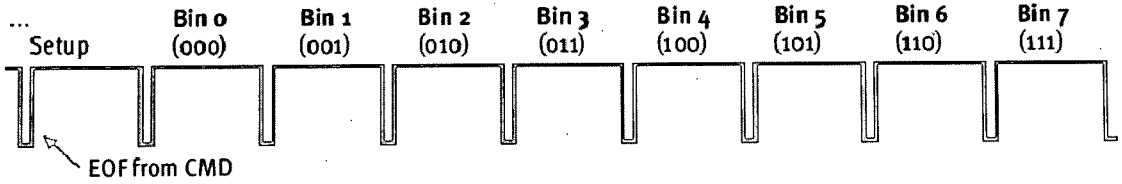
분류	내용
동작 주파수	860~900 MHz
리더→태그 코딩 방법	PWM(Pulse Width Mod.)
태그→리더 코딩 방법	PIM(Pulse Interval Mod.)
변조방법	ASK
전송 속도	70 또는 140 kbps
충돌 회피 알고리즘	Bin Slot을 이용한 Binary Tree
태그 고유 Bit 수	64 또는 96 bits(EPC Code)
에러 체크 방법	CRC-16
태그 인식 개수	규정되지 않음



[그림 5] EPC C1 Gen.1의 태그 State 블록도<sup>[3]</sup>

<표 5>는 EPC C1 Gen.1의 리더와 태그간의 통신 규격을 보여주고 있다. 충돌 회피 알고리즘은 Bin slot을 이용한 Binary Tree 알고리즘을 이용한다<sup>[3]</sup>.

[그림 5]는 EPC C1 Gen.1 태그의 State 블록도를 보여주고 있다. 리더의 인식 범위 내에 있는 모든 태그에게 리더는 CW(Continuous Wave) 신호를 보내게 되고, 태그는 이 신호에 의해 충분한 에너지를 받게 되면 Power-OFF State에서 Quiet State로 이동하게 된다. Quiet State에 있는 태그들은 리더로부터 Talk 명령을 수신하고, Talk 명령 내의 [PTR]이 가리키는 위치의 [VALUE] 값과 일치하는 태그는 Active State로 이동하게 된다. [PTR]은 태그를 인식하는 사용되는 데이터 위치를 가리키는 포인터이며, [VALUE]는 태



[그림 6] Ping ID 명령에 의해 할당받는 BIN slot<sup>[3]</sup>

그를 인식할 때 사용되는 데이터 값이다. 반대로 Active State에서 리더가 태그에게 Quiet 명령을 송신하고, Quiet 명령을 수신한 태그들 중 Quiet 명령 내의 [PTR]이 가리키는 위치의 [VALUE] 값과 일치하는 태그는 Quiet State로 이동한다.

Active State의 태그는 PingID 명령을 사용하여 태그를 인식한다. PingID를 받은 태그들은 자신의 태그 ID 중 최상위 3 bit와 일치하는 Bin Slot을 할당받는다. [그림 6]은 Ping ID를 받은 태그들이 할당받는 BIN Slot을 보여주고 있다<sup>[3]</sup>.

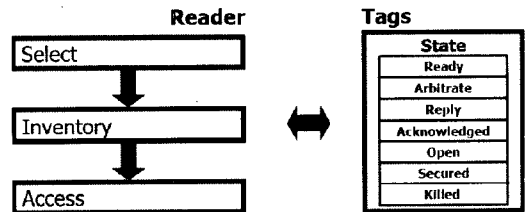
즉, 태그 ID 최상위 bit가 “001”이라면, 그 태그는 Bin 1을 할당받는다. 하나의 Bin Slot에 두 개 이상의 태그가 응답하면 충돌이 발생한 것으로 판단하고, 리더는 PingID 명령을 이용하여 충돌이 발생한 태그의 그 다음 3 bit를 다시 전송할 것을 요구한다. 충돌이 발생한 태그는 최상위 3 bit 다음의 3 bit를 다시 리더에게 전송하는 것을 충돌이 나지 않을 때까지 반복하여 충돌을 회피하게 된다. 이렇게 리더는 Ping-ID 명령을 통해 태그를 인식한 후 ScrollID 명령을 사용하여 인식된 태그를 Quiet State로 이동시킨다. 만약, Active State에서 리더의 Kill 명령을 받은 태그가 있다면, 그 태그는 Killed State로 이동하고 리더의 명령에 응답하지 않는 inactive 상태가 된다<sup>[2]</sup>.

#### 4-2 EPC Class 1 Generation 2

EPC C1 Gen.2는 EPC C1 Gen.1의 단점을 보완하고, ISO 18000-6과의 통합을 고려한 업데이트 버전이라고 할 수 있다. 최근 ISO/IEC는 900 MHz 대역의

<표 6> EPC C1 Gen.2의 주요 파라미터

분류		내용
동작 주파수		860~960 MHz
리더→태그	코딩 방법	PIE
	변조 방법	SSB-ASK, DSB-ASK, PR-ASK
	전송 속도	40/80/160 kbps
태그→리더	코딩 방법	FM0 또는 Miller-Modulated Subcarrier
	변조 방법	ASK 또는 PSK
	전송 속도	5~640 kbps
충돌 회피 알고리즘		Slot Counter를 이용한 Binary Tree
태그 고유 Bit 수		64 또는 96 bits(EPC Code)
에러 체크 방법		CRC-16
태그 인식 개수		규정되지 않음



[그림 7] 리더와 태그간의 명령 흐름 및 태그 state<sup>[3]</sup>

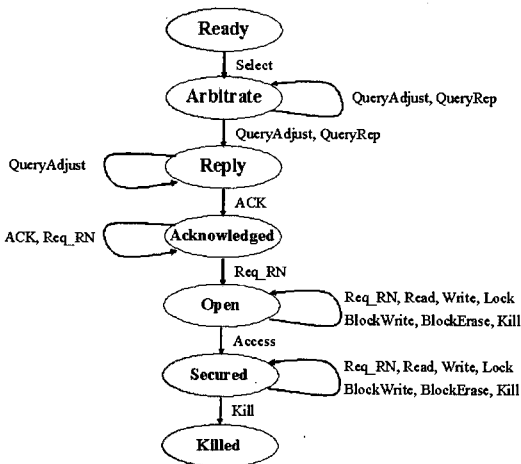
RFID 무선 인터페이스 표준인 ISO 18000-6의 수정 작업을 하면서 EPC C1 Gen.2를 ISO 18000-6 Type C로 새롭게 받아들이 것을 결정 한 바 있다. 따라서, 앞으로의 900 MHz 대역의 RFID 시스템은 EPC C1 Gen.2 표준을 따를 것으로 여겨지며, 앞으로 대두될



모바일 RFID 역시 이 표준을 따라갈 것으로 기대된다.

〈표 6〉은 EPC C1 Gen.2의 리더와 태그간의 통신 규격을 보여주고 있다. 충돌 회피 알고리즘은 Slot Counter를 이진 트리 방법을 사용하며, 변조는 리더에서 태그로 전송될 때는 ASK를 사용한다. 태그에서 리더로 전송될 때는 ASK 외에 PSK도 사용 가능하다. 데이터 코딩은 리더에서 태그로 전송될 때는 PIE 코딩을 사용하며, 태그에서 리더로 전송될 때는 ISO 18000-6와 같은 FM0나 Miller-Modulated sub-carrier 방법을 사용한다. 태그의 정보를 담고 있는 코드의 포맷은 EPC C1 Gen.1과 마찬가지로 EPC 포맷을 사용한다.

EPC C1 Gen.2는 [그림 7]에서의 단계를 거치면서 리더와 태그가 통신한다<sup>[3]</sup>. 먼저 리더는 Select 명령을 태그에 내리며 Select 명령을 받은 태그들은 자신이 속할 Inventory(일종의 그룹)를 선택받고, 동작을 준비하게 된다. 다시 리더는 태그에 Inventory 명령들을 내려보내 태그를 인식하게 되고 Access 명령들을 통해 태그의 데이터를 읽기 또는 쓰기를 수행하게 된다. 이때 태그는 [그림 8]에서처럼 7개의 State 중에 있게 된다<sup>[3]</sup>.



[그림 8] EPC C1 Gen.2의 태그 State 블록도<sup>[3]</sup>

리더는 태그에게 일정 시간 동안 CW 신호를 보내게 되고, 동작에 필요한 최소한의 에너지를 리더로부터 받은 태그들은 동작 준비 상태에 접어든다. 이 상태가 Ready State이다. 동작 준비 상태에 있는 태그들에게 리더는 Select 명령을 내리게 된다. 이 Select 명령 내에는 리더의 인식 범위 내에 있는 태그들 중에 특정 태그들이 세션 S0부터 S3 중에 한 세션을 선택받고, Inventory Flag 중에 어떤 Inventory Flag를 선택할지를 결정하는 명령이 포함되어 있다. 이 Inventory Flag에 의해 특정 태그들은 S0부터 S3까지 4개의 세션 중에 하나를 선택하게 된다. 리더의 Select 명령에 의해 선택된 태그의 Inventory Flag는 다시 A 그룹과 B 그룹으로 나뉘게 된다. 이제 특정 리더는 세션 S0부터 S3까지 중 한 세션에서 Inventory Flag A 그룹 또는 B 그룹 중에 한 그룹에 존재하는 태그들과 통신하게 되고, 통신이 끝난 태그는 세션 내의 다른 그룹으로 이동시키게 된다. 예를 들어, 어떤 리더가 Select 명령을 통해 인식 범위 내에 있는 태그들 중 EPC 코드의 8번째부터 15번째의 코드가 00110010인 태그들은 세션 S1의 Inventory Flag를 A로 설정하라고 명령을 내린다. 그럼 리더의 인식 범위 내에 있는 태그들 중 EPC 코드의 8번째부터 15번째의 코드가 00110010인 태그들은 세션 S1의 Inventory Flag를 A로 바꾸게 된다. 이후 이 태그들은, 만약 리더로부터의 Query 명령이 세션 S1, Inventory Flag=A 조건을 포함하면, 이때부터 Inventory Round에 참여하게 되며 리더와 통신할 수 있게 된다. 리더와 통신이 끝나고 나면, 세션 S1의 Inventory Flag를 B로 바꾸고 해당 Inventory Round에서 제외된다. 이와 같이 리더가 세션 S1의 Inventory Flag=A인 태그들과 모두 통신을 하고, 태그들이 모두 세션 S1의 Inventory Flag가 B 값으로 바뀌게 되면 더 이상 통신할 것이 없는 상태가 되는데 이 상태를 한 번의 Inventory round가 끝났다고 표현한다. 한 번의 Inventory Round가 끝나면 다시 리더는 리더의 인식범위

내에 있는 태그들 중에 특정 태그들의 Inventory Flag 와 그룹을 결정하고 통신하는 새로운 Inventory Round를 수행하게 된다.

Inventory Flag에 상관없이 항상 리더와 통신할 수 있도록 결정되는 태그들도 있는데 바로 Selected Flag이다. 만약 태그가 Selected Flag로 결정되면 이 태그들은 리더가 접근하는 Inventory Flag에 상관없이 리더의 명령에 응답할 수 있게 된다.

Ready State에서 리더의 Select 명령에 의해 Inventory Flag를 설정받은 태그들은 리더의 다음 명령을 기다린다. 이제 리더는 Ready State에 있는 태그들에게 Query 명령을 내려보내게 된다. Query 명령 내에는 리더가 어떤 Inventory Flag와 통신을 할지(세션 S0부터 S3 중에 하나), Query 명령에 응답하는 태그들의 데이터 코딩 방법, 파일롯 톤(Pilot tone) 사용 여부, Q 값 등에 대한 정보가 들어있다. 따라서, Query 명령을 받은 태그들은 Query 명령 내의 Inventory Flag 세션 값과 리더의 Select 명령에 의해 부여 받은 세션 값이 같으면 리더의 Query 명령에 응답하는데 그때의 데이터 코딩 방법과 파일롯 톤 사용 여부 등은 Query 명령을 따라 결정하여 응답하게 된다. 이때 리더에게 응답하면서 Query 명령 내의 Q 값(0~15)을 이용하여 태그 내의 RNG를 통해  $0 \sim 2^Q - 1$  사이의 랜덤 변수를 부여받아 Slot 값을 결정하고, 결정된 Slot 값과 함께 리더에게 응답하게 된다. Query 명령 내의 Q 값에 의해 태그 스스로 결정하는 Slot 값은 리더가 인식 범위 내의 다중의 태그 응답에 따른 충돌을 회피하기 위해 사용된다.

이제 리더는 리더의 Query 명령에 의해 응답한 태그들 중에 만약 Slot 값이 0인 태그가 하나라면 그 태그는 리더로부터 새로운 랜덤 변수를 생성하라는 명령인 QueryRep 명령을 받게 되고, 새로운 랜덤 변수 RN16을 부여받고, 리더에게 새로운 RN16을 전송하고 Reply State로 이동한다. 만약, Slot 값이 0인 태그가 여러 개이거나 Slot 값이 0보다 작거나 큰 태그

들은 Arbitrate State로 이동하게 된다. 만약 Slot 값이 0인 태그가 하나뿐이어서 새로운 RN16을 생성하고, Reply State로 이동한 태그는 새롭게 생성한 RN16과 함께 자신의 PC, EPC 코드, CRC-16을 보내게 된다. 리더는 Reply State에서 리더에게 응답한 태그의 정보 중에 먼저 RN16을 판단하여 태그가 Reply State로 이동하면서 보낸 새로운 RN16인지를 판정한 후, CRC-16을 체크하여 에러가 없는지 판단하게 된다. 만약, 태그가 Reply State로 이동하면서 리더에게 보낸 새로운 RN16이 확실하고 CRC-16을 체크한 결과, 에러가 없었다면 리더는 Reply State에 있는 태그에게 RN16 값이 포함된 ACK 명령을 보내고, 해당 태그를 Acknowledged State로 이동시킨다. ACK 명령을 받아 Acknowledged State로 이동한 태그는 자신이 조금 전에 리더에게 응답한 RN16 값과 비교하여 같은 RN16이 포함된 ACK 명령이면 리더에게 자신의 PC, EPC, CRC-16 코드를 보내고, 리더는 태그의 정보를 읽어들인다. 만약, 태그가 Reply State로 이동하면서 리더에게 보낸 새로운 RN16이 아니거나 CRC-16에서 에러가 발생한 것으로 체크된다면 Reply State에 있는 태그는 Arbitrate State로 내려가 다음 리더의 명령을 기다린다. 리더의 ACK 명령을 수신하여 Acknowledged State로 이동한 태그와 리더의 ACK 명령 내의 RN16 값이 일치하지 않는다면, 리더에 일치하지 않았음을 회신하게 된다. 이때 리더는 Access 명령 중에 하나인 Req\_RN을 통하여 새로운 RN16을 생성할 것을 명령하고, 태그는 새로운 RN16을 생성하여 리더에 응답한다. 이제 리더가 새로운 RN16이 포함된 ACK 명령을 다시 보내게 되고, 새롭게 생성한 태그의 RN16과 비교하여 일치하면 리더에게 태그 자신의 PC, EPC, CRC-16을 전송하게 된다.

Ready State에서 리더의 Query 명령에 의해 응답한 태그들 중에 만약 Slot 값이 0이 아닌 태그들이나 Reply State에서 확실하지 않은 RN16이나 CRC-16에 에러가 있어 리더와의 통신에 실패한 태그들은 Ar-

bitrate State로 이동하게 된다. Arbitrate State에 있는 태그들은 Reply State에 있는 태그가 리더와 통신이 끝날 때까지를 기다려 다음의 Round에서 리더와의 통신을 기다리는 State라 할 수 있다. 리더는 Reply State에 있는 태그와 통신이 끝나면 Arbitrate State에 있는 태그들에게 QueryRep나 QueryAdjust 명령을 내려보내 태그가 새로운 Q 값을 설정하여 Slot 값을 새로이 결정하도록 한다. QueryRep 명령은 특정 세션에 있는 모든 태그들의 Q 값을 일괄적으로 하나 감소하도록 하도록 하는 명령이며, QueryAdjust는 특정 세션에 있는 태그들의 Q 값을 그대로 유지하거나 +1 또는 -1 되도록 하는 명령이다. 이 명령에 의해 새로운 Slot 값을 설정한 태그들 중에 만약 Slot=0인 태그가 하나만 있다면, 그 태그는 새로운 RN16 값을 생성하여 Reply State로 이동하게 되고, 그렇지 않은 경우는 Arbitrate State에 있는 태그들에게 다시 Q 값이 설정되도록 하는 과정을 반복한다.

Acknowledged State에서 리더에게 태그 정보(PC, EPC, CRC-16)를 전송한 태그의 메모 내에 특정 코드를 읽거나 쓰기를 위하여 리더는 Access 명령을 통해 Open State로 이동시킨다. Open State에서는 특정 코드를 읽거나 쓸 수 있을 뿐 아니라, 특정 코드 블록(Block)을 쓰거나 지울 수도 있으며, 태그 내의 정보들이 Access 명령에 의해 수정되지 않도록 Lock을 걸어놓을 수도 있다. 이러한 모든 절차는 Open State에서 리더의 Access 명령에 의해 수행된다. Open

State에서 수행되는 절차는 다음과 같다.

Acknowledged State에서 리더에게 태그 메모리 정보를 전송한 태그가 리더의 Access 명령을 수신하고, 수신된 Access 명령 내의 Access Password가 0이었다면 그 태그는 Secured State로 이동하고, 만약 Access Password가 0이 아니었다면 Open State로 이동하게 된다. Open State로 이동한 태그는 리더의 Read 명령에 의해 태그의 특정 메모리 부분을 리더에게 응답할 수 있고, 리더가 Write 명령과 함께 보낸 데이터를 태그의 특정 메모리 부분에 저장할 수도 있다. 또한, 리더의 BlockWrite나 BlockErase 기능을 통해 태그의 메모리 내의 특정 블록을 쓰거나 지울 수도 있다. 만약, 리더로부터 Lock 명령을 수신한다면 Write나 Erase가 되지 않도록 Lock을 걸 수도 있다. 또한, 태그에게 리더가 Kill 명령을 내리면 Kill 명령을 수신한 태그는 리더에게 정확한 Kill 명령인지를 두 번의 확인 작업을 거친 후 Killed State로 이동하게 된다. 다른 명령과는 달리 Kill 명령이 두 번의 확인 작업을 거치는 것은 Kill 명령에 의해 Killed State로 이동한 태그는 리더가 Power-Up을 위한 CW 신호를 보내지 않는 한 Power Down 상태로 있게 되기 때문이다.

Acknowledged State에 있는 태그가 리더의 Access 명령을 수신했을 때, Access Password가 0인 명령을 수신했다면 태그는 Secured State로 이동한다. Secured State 역시 Open State와 마찬가지로 리더가 태그 메모리 내의 일정 부분을 읽거나 쓰기를 할 수

<표 7> 900 MHz 대역 RFID 시스템의 무선 인터페이스 표준 비교

표준	데이터 코딩		Code bit	Data Rate		Security
	리더→태그	태그→리더		리더→태그	태그→리더	
ISO 18000-6 Type A	PIE	FM0	64 bits	8 kbps	40 kbps	none
ISO 18000-6 Type B	Manchester	FM0	64 bits	33 kbps	40 kbps	none
EPC C1 Gen.1	PWM	PIE	64, 96 bits	140 kbps	140 kbps	8 bit Kill
EPC C1 Gen.2	PIE	FM0, Miller	64, 96 bits	40~160 kbps	5~640 kbps	32 bit Kill Access

있고, 메모리 내의 특정 블록을 읽거나 지울 수도 있으며, Write와 Erase를 못하도록 Lock을 걸 수 있는 작업을 수행한다. 또한, Kill 명령에 의해 태그가 더 이상 리더의 명령에 응답하지 않는 상태인 Killed State로 태그를 이동시킨다<sup>[3]</sup>.

## V. 결 론

본 고에서는 유비쿼터스 시대의 핵심 기술인 RFID의 무선 인터페이스에 대한 표준 중에서 900 MHz 대역의 RFID 무선 인터페이스 표준을 ISO/IEC의 ISO 18000-6과 EPC Class 1에 대해서 살펴보았다. 본 고에서 살펴본 RFID 무선 인터페이스는 ISO 18000-6 Type A와 Type B, EPC Class 1 Generation 1, Generation 2 등 4가지의 무선 인터페이스에서 리더와 태그간의 통신에 사용되는 명령들과 절차들을 설명하였다. 본 고에서 살펴본 4가지 무선 인터페이스 프로토콜에 대해서 간략하게 비교한 내용을 <표 7>에 정리하였다.

본 고에서 살펴본 RFID 무선 인터페이스 표준 중 EPC Class 1 Generation 2는 유통, 물류에 사용될 900 MHz 대역의 최신 표준으로 정해질 것이 확실시되고 있다. 더욱이 아직도 미개척지인 모바일 RFID에 EPC Class 1 Generation 2를 기반으로 활용 방안 및 새로운 표준에 대한 연구와 국제 표준화 활동이 필

요할 것이다. 이러한 노력이 앞으로 도래할 유비쿼터스 시대에 우리나라의 IT 강대국 이미지를 UT 강대국으로 이끌어 갈 것으로 기대된다.

## 참 고 문 헌

- [1] ISO/IEC, ISO/IEC JTC 1/SC 31/WG 4 N0722, Nov. 2003.
- [2] Auto-ID Center, *860~930 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation*, 2002.
- [3] EPCglobal, *EPC Radio Frequency Identity Protocols Class 1 Generation 2 UHF RFID Protocol for Communications at 860~960 MHz*, 2004.
- [4] ISO/IEC JTC1, <http://www.jtc1.org/>
- [5] EPCglobal, <http://epcglobalinc.com/>
- [6] RFID Journal, <http://www.rfidjournal.com/>
- [7] 고현봉, 오영철, "RFID 표준화 동향", *Telecommunications Review*, 15(2), pp. 244-255, 2004년 4월.
- [8] 이수련, 이채우, "RFID 시스템의 다중 인식 기술 현황", *한국전자과학회지 전자과기술*, 15(2), pp. 44-53, 2004년 4월.
- [9] 박지만, 박영수, 전성익, "전파식별(RFID) 시스템 기술", *전파진흥*, pp. 84-95, 2004년 4월.

≡ 필자소개 ≡

황 태 욱



2001년 2월: 경희대학교 전파공학과 (공학사)  
2003년 2월: 경희대학교 전파공학과 (공학석사)  
2003년 3월~현재: 경희대학교 전파공학과 박사과정  
[주 관심분야] RFID, SDR, Spectrum Management

management

박 경 환



1991년 2월: 한양대학교 전자공학과 (공학사)  
1993년 2월: 한국과학기술원 전기 및 전자공학과 (공학석사)  
1997년 2월: 한국과학기술원 전기 및 전자공학과 (공학박사)  
1997년 1월~2000년 12월: 테이콤 종합

연구소 선임연구원

2001년 1월~현재: 한국전자통신연구원 선임연구원

[주 관심분야] RFID, RFIC, 무선통신시스템, EM Scattering

김 영 수



1981년 2월: 연세대학교 전자공학과 (공학사)  
1983년 2월: 연세대학교 전자공학과 (공학석사)  
1988년 12월: 미국 Arizona State University 전기 및 컴퓨터공학과 (공학박사)

1985년 5월~1986년 5월: Consultant, Signal-System Technology Inc., U.S.A.

1986년 6월~1988년 12월: Research Associate, Arizona State University

1989년 2월~1992년 8월: ETRI 전파기술부 전파응용연구실 실장

2002년 1월~2003년 2월: Visiting Faculty, MPRG, Virginia Tech., U.S.A.

2004년 12월~현재: TTA RFID/USN 프로젝트 그룹 RFID 무선접속 실무반, 의장

1992년 9월~현재: 경희대학교 전자정보대학 전파통신공학 교수

[주 관심분야] OFDM, RFID, SDR, MIMO System, Smart Antenna