제132회 컴퓨터시스템응용기술사 해설집

2024.01.27

국가기술자격 기술사 시험문제

기술사 제 132 회 제 2 교시 (시험시간: 100 분)

분야	정보통신	자격종목	컴퓨터시스템응용기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 10 점)

1. 컴퓨터 시스템은 내부/외부에서 발생하는 각종 event 에 대처하기 위해, 다양한 방식으로 인터럽트(interrupt)체계를 구현하고 있다. 이와 관련하여 아래 사항을 설명하시오.

가. Polling 방식

나. Daisy-Chain 방식

다. Vector Interrupt 방식

2. 사물인터넷은 일상생활에서 AI 와 융합되어 지능형 IoT 로 진화하고 있다. 이와 관련하여 아래 사항을 설명하시오.

가. AIoT(Artificial Intelligence of Things) 개념

나. AIoT 의 보안 취약점

다. AIoT 디바이스 보안기술 3 가지

3. 인터넷 제어 메시지 프로토콜(ICMP, Internet Control Message Protocol)과 인터넷 그룹관리 프로토콜(IGMP, Internet Group Management Protocol)을 비교하여 설명하시오.

4. 이동형 로봇의 대인 충돌 안전성 평가 방법(정보통신단체표준, TTAK,KO-10.1223)에 대하여 아래 사항을 설명하시오.

가. 충돌, 시험에서의 충격 속도 측정방법

나. 충돌 시험용 인체모형(더미, dummy)

다. 인체모형 측정 데이터

5. 정보시스템 마스터플랜(ISMP, Information System Master Plan)에 대하여 아래사항을. 설명하시오.

가. ISMP 와 EA(Enterprise Architecture), ISP(Information System Planning)에 대하여설명하고, 상호 비교

나. 투입공수에 의한 사업대가 산정방식을 적용한 ISMP 수립비 산정 절차, 주요내용, 산출물

6. 개방형 무선 접속망 Open RAN(Open Radio Access Network)은 서로 다른 장비 간 상호 연동을 가능하게 하는 기술이다. 이와 관련하여 아래 사항을 설명하시오.

가. Open RAN 의 개념

나. Open RAN 의 구성요소

다. RAN 과 Open RAN 의 비교

01	인터럽트(Interrupt)		
문제	컴퓨터 시스템은 내부/외부에서 발생하는 각종 event에 대처하기 위해, 다양한 방식으로 인터럽트(interrupt)체계를 구현하고 있다. 이와 관련하여 아래 사항을 설명하시오. 가. Polling 방식 나. Daisy-Chain 방식 다. Vector Interrupt 방식		
도메인	CA/OS	난이도	중(상/중/하)
키워드	SW방법(Polling), HW방법(Vector Interrupt), HW 직렬우순순위(Daisy-Chain)		
출제배경	운영체제의 기본인 인터럽트 방식에 대한 상세 분류 가능 여부 확인		
참고문헌	ITPE 기술사회 https://m.blog.naver.com/syunjae21/222065512231		
해설자	전일 기술사(제 114회 정보관리기술사 / nikki6@naver.com)		

I. 운영체제에서의 인터럽트 개념

개념	- 프로그램 실행 중 하드웨어 입출력 또는 예외 상황 처리를 위해 CPU의 현재 처리를 중단시키고 해당 동작을 수행하도록 하는 시스템 동작	
특징	- 원천 다양성	- 인터럽트가 발생 원천이 다양하여 종류 구분 필요
	- 마스크 비트	- CPU 코어의 인터럽트 마스크 비트에 따라 수행 여부 결정

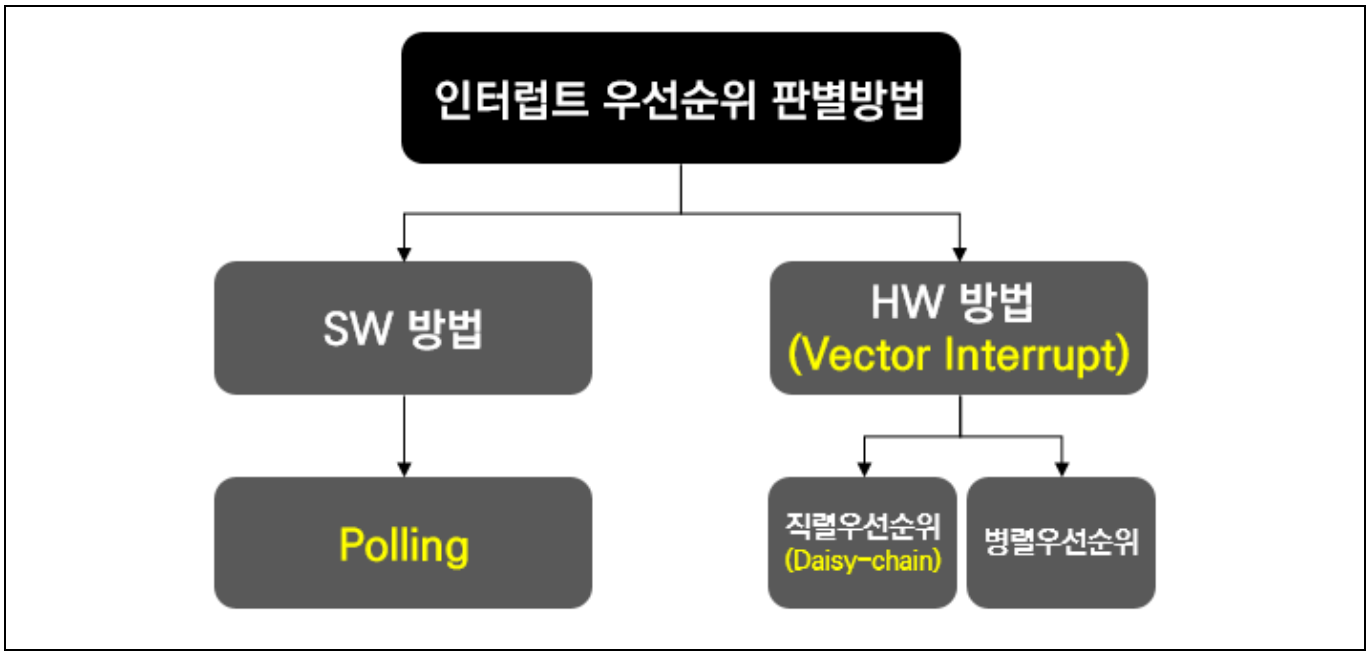
II. 운영체제에서의 인터럽트 종류

구분	종류	설명	
인터럽트 신호 요청	- 단일 회선(Polled)	- 모든 인터럽트 장치가 하나의 회선을 사용, 장치 판별 필요	
	- 고유 회선(Vector)	- 장치마다 고유한 인터럽트 회선을 보유, 장치 판별 불필요	
우선순위 판별 (단일 회선인 경우)	- S/W 방식	- 폴링(Polling)	- 프로그램을 통해 장치 Flag를 통해 우선순위 검사
	- H/W 방식	- Daisy Chain	- 우선순위 높은 장치를 물리적으로 상위에 배치
		- 병렬(Parallel) 우선순위 방식	- 장치 별 Mask Register Bit 설정하여 판별
ISR(Interrupt Service Routine) 호출	- 절대 주소	- 정해진 주소 값 내에 ISR 코드가 존재	
	- 인터럽트 벡터 테이블	- 인터럽트 벡터 테이블에 주소 값을 얻어서 호출	

- 이외에 인터럽트 우선순위에 따른 종류 구분 가능

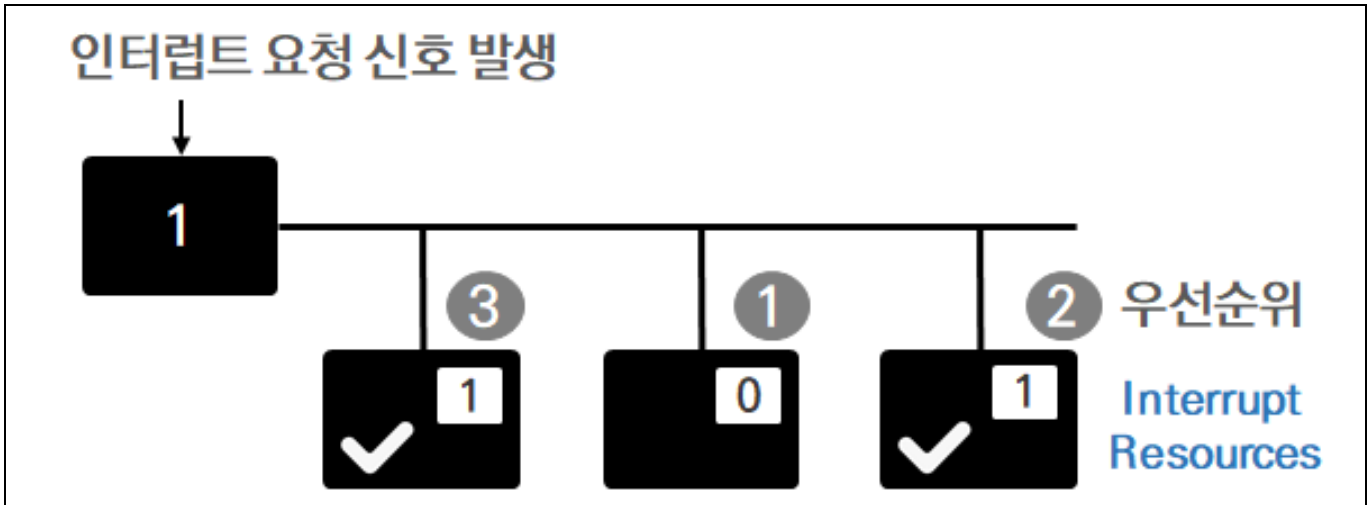
III. SW 방법에 의한 우선순위 판별, Polling 방식 상세 설명

가. 인터럽트 우선순위 판별 방법



- SW 방법으로는 Polling 방식이, HW 방식으로는 직렬우선순위(Daisy-chain)방식과 병렬우선방식이 존재

나. Polling 방식 상세 설명

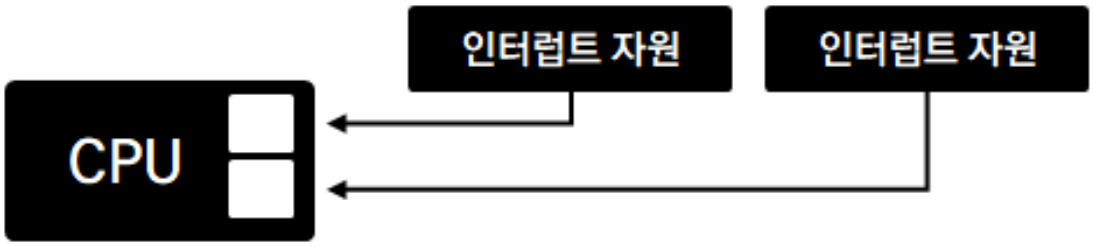


개념		- 프로그램을 통해 각각의 장치 Flag 상태를 검사하여 우선순위가 높은 것부터 차례대로 하나씩 비교한 후 어느 장치에서 인터럽트가 발생했는지 판별하는 방식
특성	장점	- 융통성 존재 - 프로그램 수정 및 우선순위 변경 및 예외처리 쉬움, 비용 저렴
	단점	- 인터럽트 반응속도가 느림

- Polling 방식은 시스템의 리소스를 많이 먹는 부분에 구현 시 시스템 성능 저하의 원인이 되기도 함. 또한 처리에 정확한 타이밍을 요하는 곳에 사용을 할 경우, 이 또한 문제 발생의 원인이 되기도 함

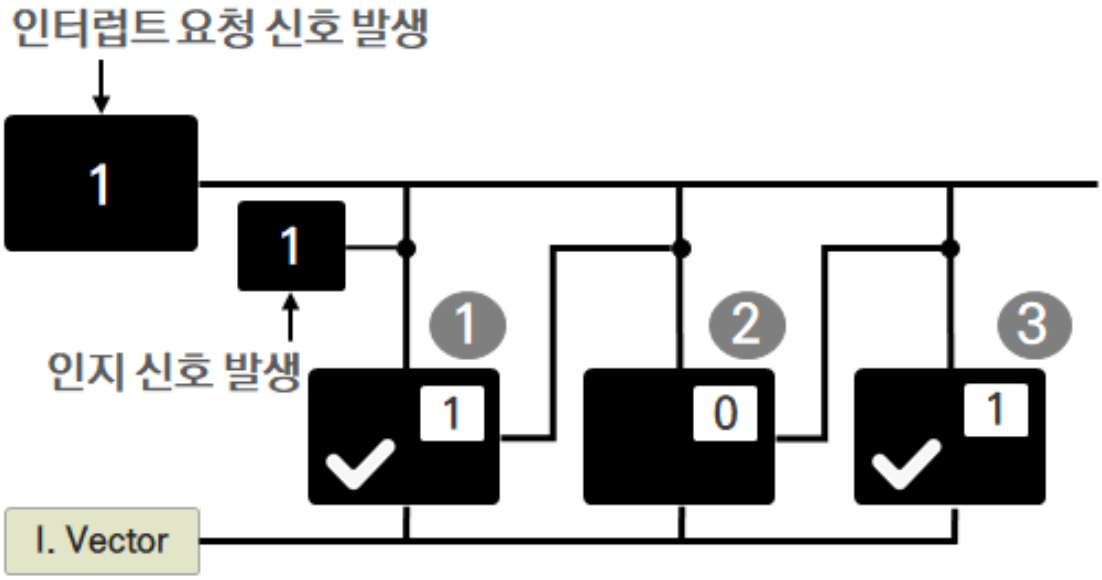
IV. HW 판별, Vector Interrupt 와 Daisy-Chain 방식 상세 설명

가. Vector Interrupt 방식 상세 설명



개념	- CPU에 있는 Interrupt Register의 각 비트에 고유 회선을 연결하는 방식	
특성	장점	- 장치마다 고유한 인터럽트 요청 신호 회선을 가지므로 인터럽트를 요청한 장치 판별 과정이 필요 없음 - 속도 우수
	단점	- SW 방식에 비해 비용 고가 - 변경 및 예외처리 곤란

나. Daisy-Chain 방식 상세 설명



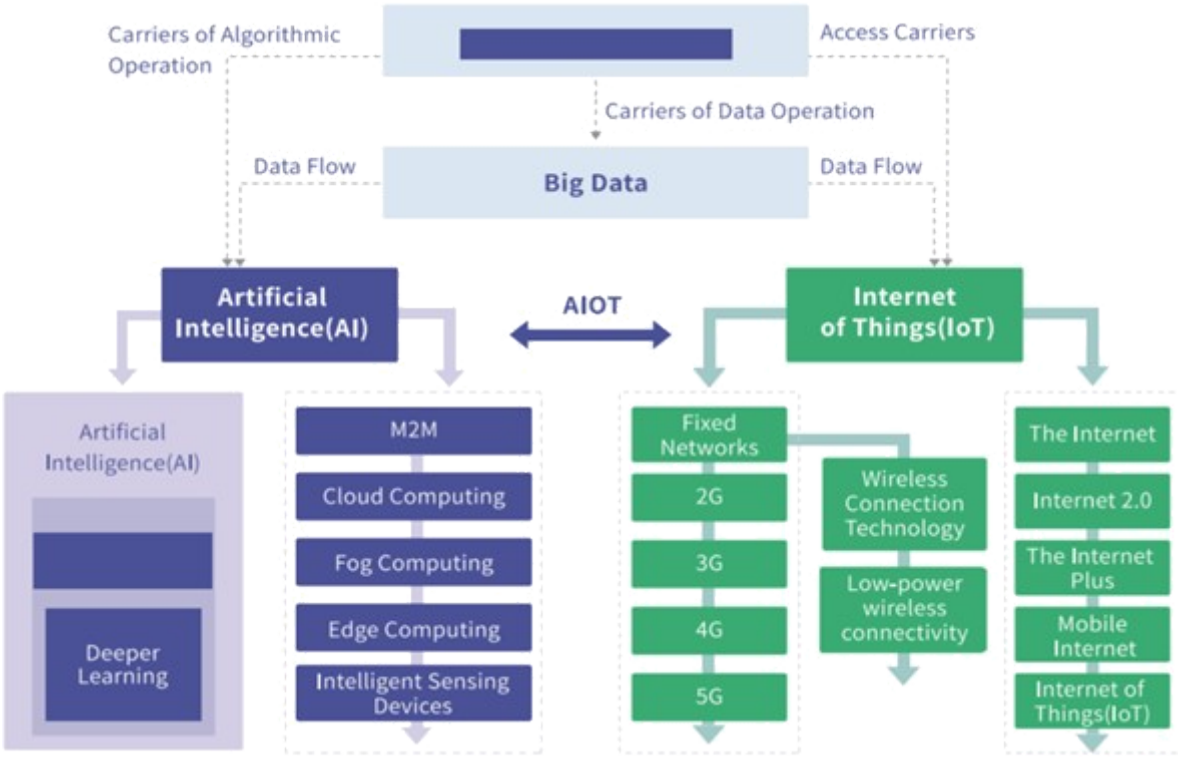
개념	- 인터럽트 요청 장치를 우선순위가 높은 것부터 직렬 회로로 연결한 형태로 CPU 신호를 인지한 최초의 장치만 자신의 장치 번호를 CPU로 보내 장치를 식별하는 방식	
특성	장점	- 신호가 물리적 논리 회로의 속도이므로 반응속도가 빠름
	단점	- 융통성이 없고 수정이나 변경이 곤란 - HW 장비 비용 고가

- 우선순위가 높은 장치를 선두에 위치시키고 나머지를 우선순위에 따라 차례로 연결
- 호스트에 가까운 쪽에 높은 우선권을 두는 경우가 많음

"끝"

02	AIoT(Artificial Intelligence of Things)		
문제	사물인터넷은 일상생활에서 AI와 융합되어 지능형 IoT로 진화하고 있다. 이와 관련하여 아래 사항을 설명하시오. 가. AIoT(Artificial Intelligence of Things) 개념 나. AIoT의 보안 취약점 다. AIoT 디바이스 보안기술 3가지		
도메인	디지털서비스	난이도	중 (상/중/하)
키워드	네트워크, 하드웨어, 시스템, 소프트웨어, DB 보안 취약점, SW 보안 플랫폼, H/W 보안, RISC-V 오픈소스 하드웨어 기반 보안		
출제배경	AIoT 기존 출제 문제의 심화 반복 출제		
참고문헌	지능형 IoT 사회의 보안이슈 분석(김호원, 민경식, 박진상 공저, 한국인터넷진흥원, 2022.VOL 5)		
해설자	단합반멘토 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I.디지털 대전환의 핵심 촉매제. AIoT(Artificial Intelligence of Things) 개념



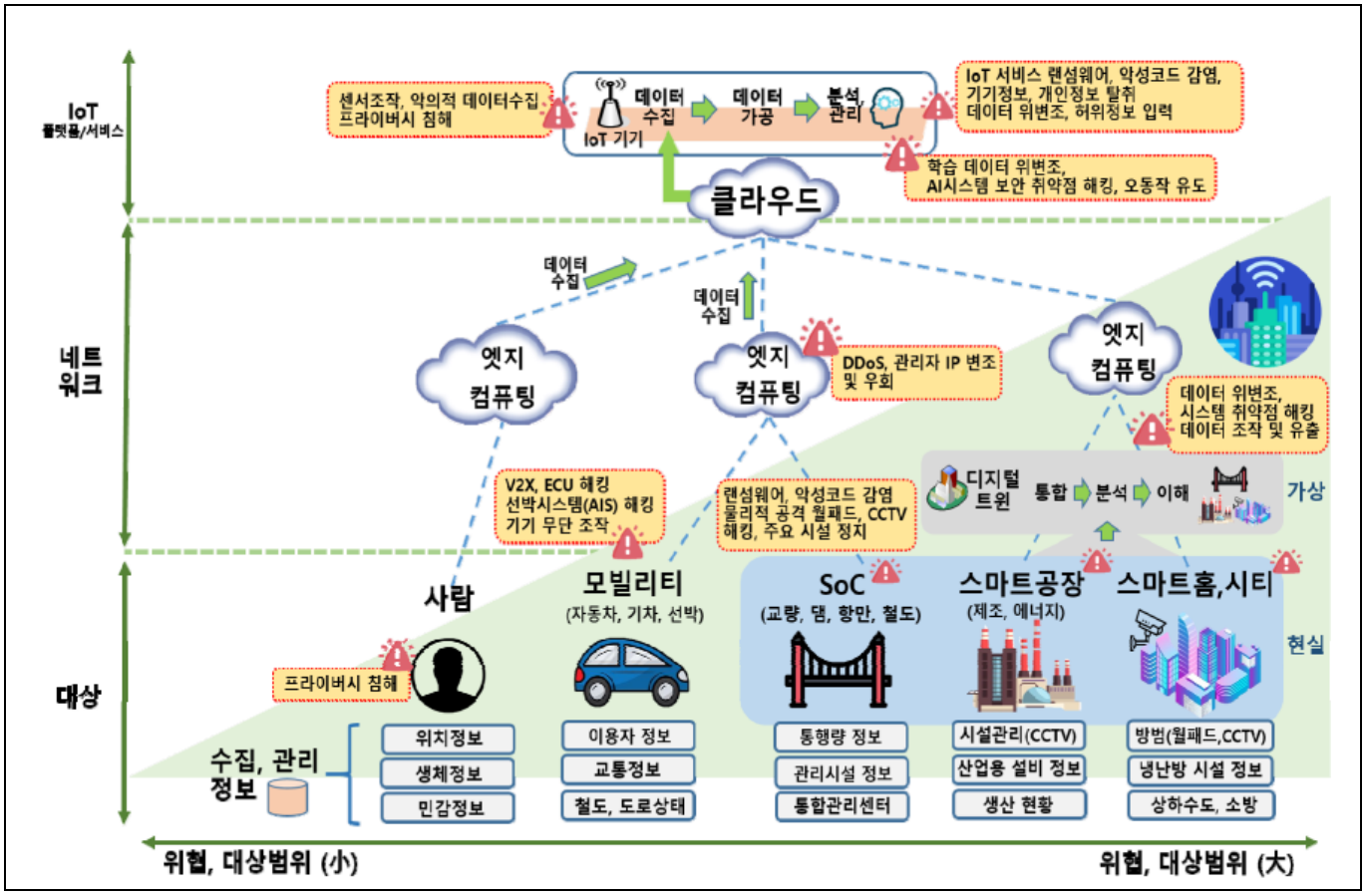
정의	- AI(Artificial)과 IoT(Internet of Things)의 합성어로 AI의 지능성과 IoT의 연결성을 융합하여 IoT의 기능을 확장하여 AI에는 다양한 데이터를 IoT에는 지능화를 제공하는 사물지능융합 기술.	
AIoT의 지능화 발전 단계	Standalone Intelligence	- 독립형 장치는 사용자의 명령을 정확하게 인식, 이해하고 올바른 결정을 내리고 실행하며 피드백을 제공 - 장치 사이에는 활성 연결이 없으며 사용자는 두 장치 간의 상호 작용에 대한 지침을 제공

	Interconnected Intelligence	- '하나의 클라우드/중앙 콘솔, 다중 터미널/센서' 모드를 사용하여 상호 연결된 제품 매트릭스 - 독립형 인텔리전스의 "island dilemma"를 극복하고 인텔리전스 현장 경험을 지속적으로 업그레이드 및 최적화 수행
	Active Intelligence	- 인텔리전스 시스템은 사용자 행동 선호도, 사용자 이미지, 환경 및 기타 유형의 정보에 따라 서비스를 제공할 준비가 되어 있으며 자동 학습, 자기 적응 및 자동 서비스 개선이 가능하며 사용자의 지침 없이 사용자가 필요로 하는 서비스를 능동적으로 제공

- AIoT 확대에 따른 다양한 보안이슈가 발생하고 있으며, 그 중 디바이스 관련 이슈의 해결의 어려움에 따라 그에 대한 해결방안 필요

II. AIoT의 보안 취약점

가. AIoT 보안 취약점 구조도



나. AIoT 보안 취약점

구분	대상	보안위협		
		네트워크	하드웨어, 시스템	소프트웨어, DB
사람	개인화 기기	- DoS·DDoS 공격을 통한 외부 통신 차단	- 펌웨어, 보안 패치 업데이트 취약점으로 인한 제어권 상실, 오작동	- 악성코드 감염, 위치정보, 생체정보, 민감정보 등 유출

모빌리티	자동차	- IoT 데이터 송수신 과정에서 데이터 유출 및 변조, 탈취 등 - NW, 통신 프로토콜 취약점에 따른 보안 위협 발생		- 자동차 ECU 해킹을 통한 무단 조작 - 차량 위치, 이동 정보 등 유출
SoC	교량		- 시설 관리시스템 무단 침입을 통한 시설 관리 불가, 장애 등 발생	- 시설 제어 SW 무단 침입, 악성코드 감염 등을 통한 장애 발생
스마트 공장	제조설비		- 생산시스템 관리 및 인증 취약점으로 인한 설비 제어권 상실, 오작동	- 생산 SW 위변조를 통한 오동작 - 내부시설 내 주요 정보 무단 유출
스마트 시티	월패드, 디지털 도어락, CCTV, 화재감지 센서 등		- 월패드, CCTV 시스템 제어권 상실에 따른 모니터링, 시설관리 등 불가 - 시설관리 시스템 악성코드 감염을 통한 설비 관리 중단	- 월패드, CCTV 시스템 제어권 상실에 따른 모니터링, 시설관리 등 불가 - 시설관리 시스템 악성코드 감염을 통한 설비 관리 중단 - IoT 기기 단순 암호 설정, 악성코드 감염을 통한 사생활, 개인정보 유출, 통제권 상실 - 빌딩 제어·관리 SW 관리 소홀, 보안 패치 미적용 등으로 인한 취약점 노출

- AIoT 보안 취약점을 대응하기 위해 SW, HW와 RISC-V 오픈 소스 하드웨어 기반으로 대응 가능

III. AIoT 디바이스 보안기술 3가지

구분	구현 방법	특징	보안 기술	설명
S/W 플랫폼 보안	- AP 칩을 통해 보안 구현	- 프로세서와 주변 장치, 저장장치를 대상으로 보안 서비스를 제공	- TEE (Trusted Execution Environment)	- 메인 프로세서 내 별도의 독립된 보안 영역이 제공되는 안전한 실행 환경이며, 응용 프로그램의 무결성 및 정보의 기밀성을 제공할 수 있는 프로세서
			- ARM TrustZone	- Secure World와 Normal World로 나뉘며, 실행 영역에서 REE(Rich Execution Environment)와 TEE(Trusted Execution Environment)

				로 분리
			- Intel SGX	- 특정 애플리케이션 코드 및 데이터를 메모리 내에 격리하는 하드웨어 기반 메모리 암호화를 제공
H/W 보안	- 별도의 하드웨어 모듈을 추가	- 기존 보안 기능을 제공하지 않는 IoT 디바이스에도 보안을 적용 가능	- TPM(Trusted Platform Module)	- 암호키, 패스워드, 디지털 인증서 등을 안전하게 저장하는 보안 모듈로, 식별·인증, Secure Boot 기능 뿐 아니라 플랫폼 무결성 검증, 디스크 암호화 등 다양한 환경에 적용
			- SE(Secure Element)	- 애플리케이션을 안전하게 호스팅하고 암호화 데이터를 저장할 수 있고 변조 방지가 적용된 칩
RISC-V 오픈 소스 하드웨어 기반 보안	- RISC-V 활용 (RISC 기반 개방형 명령어 집합 (ISA))	- 개발자가 원하는 방향대로 성능에 맞게 기능을 구현 가능	- RISC-V MultiZone	- MultiZone은 RISC-V ISA를 지원하는 TEE(Trusted Execution Environment) 구조이며 TEE는 통상적으로 Normal World와 Secure World로 구분하여 Secure World에 대해 높은 권한을 요구하여 동작
			- RISC-V 메모리 격리	- 응용 프로그램 간 메모리 격리 기술(Memory Isolation)을 구현 가능
			- RISC-V 하드웨어 기반 메모리 무결성	- RISC-V의 칩셋으로 명령어가 들어가기 전 하드웨어 암호 모듈 추가를 통해, 메모리 무결성을 보장 가능

- AIoT는 보안 취약점을 대응과 함께 다양한 방안을 통해 발전이 가능

IV. . AIoT의 발전을 위한 주요 방안

측면	주요 방안	설명
정책 관점 (Political)	- 융합형 인력 양성	- 복합 임무 사물인터넷 플랫폼 관련 핵심 원천 기술 개발 위한 다양한 지식을 보유한 융합형 인력 양성 지원
	- 자율형 IoT 기술 개발 지원	- 미래 인구 감소, 재난 등을 대비해 인간을 대신할 수 있는 자율형 IoT 기술 개발 지원
	- IoT 중소기업 지원	- 유망한 기술을 지니고 있으나 자본 규모가 적은 IoT 중소기업의 진흥을 위한 지원
	- 실시간 데이터 활용 규제 완화	- 초기 시장 형성 및 활성화를 위한 실시간 상황 데이터 활용 규제 완화
기술적 관점 (Technical)	- 자율형 협업 사물인터넷 플랫폼	- 최적제어 기반 능동 자율형 협업 사물인터넷 플랫폼 기술 개발
	- 5G와 6G 기술 개발	- 차세대 네트워크를 위한 5G 응용기술 개발 및 6G 핵심

	및 선점	기술 선정
	- 개방형 플랫폼 구축	- 개방형 협업 사물인터넷 플랫폼과 서비스 프레임워크 인프라 구축
사회적 관점 (Social)	- 협업 생태계 조성	- 사물 인터넷 협업 생태계 조성
	- 데이터 생태계 조성	- 수집 데이터 공개 및 공동 이용 가능한 생태계 조성

"끝"

03	ICMP, IGMP		
문제	인터넷 제어 메시지 프로토콜(ICMP, Internet Control Message Protocol)과 인터넷 그룹관리 프로토콜(IGMP, Internet Group Management Protocol)을 비교하여 설명하시오.		
도메인	네트워크	난이도	중(상/중/하)
키워드	오류보고 메시지, 질의 메시지, 멀티캐스트, 그룹방식		
출제배경	네트워크 프로토콜 기본 개념 확인		
참고문헌	ITPE 기술사회 자료		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

I. 인터넷 제어 메시지 프로토콜 ICMP의 개요

가. ICMP(Internet Control Message Protocol)의 역할

- 신뢰성이 없고 비연결형 데이터 그램 전달 제공, 오류제어와 지원 매커니즘이 없는 IP 프로토콜의 문제점을 보완하기 위해 설계

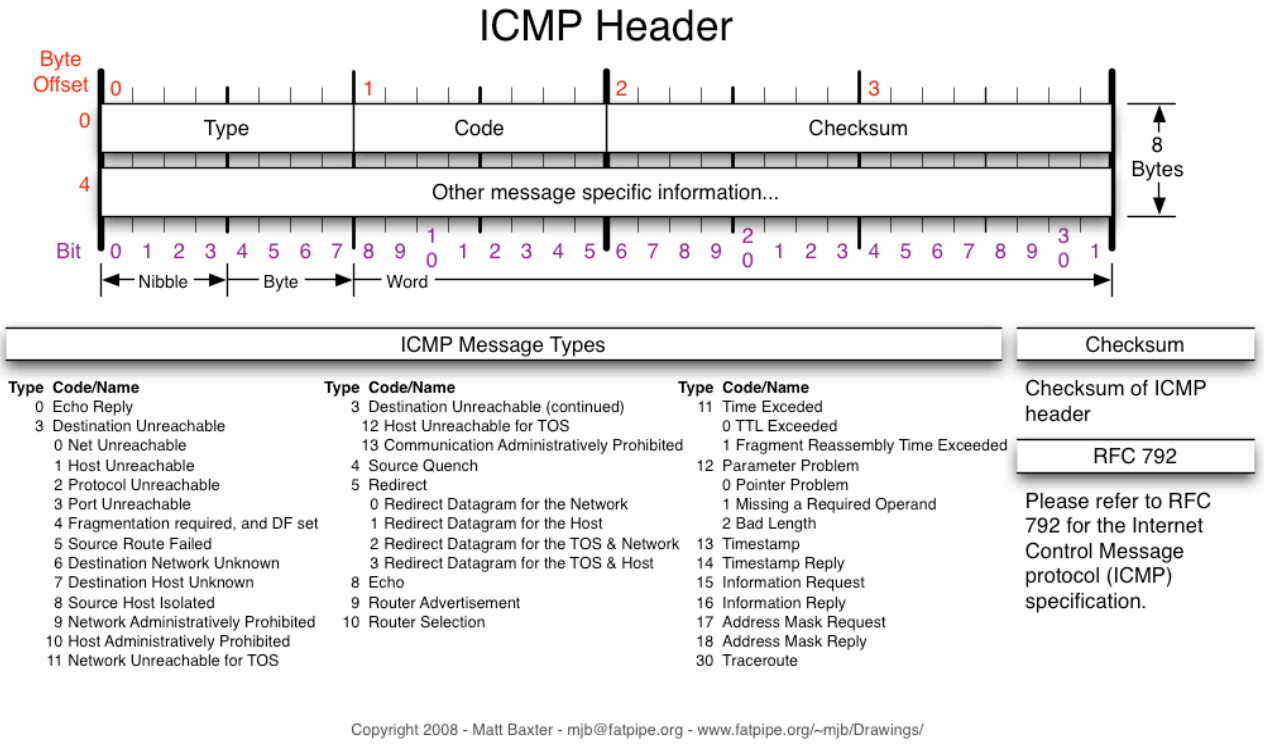
나. ICMP 메시지 유형

- ICMP 메시지는 오류보고(Error reporting) 메시지와 질의(query)메시지로 나뉨
- 오류 보고 메시지 : 라우터나 (목적지)호스트가 IP 패킷을 처리하는 도중 발견되는 문제를 보고
- 질의 메시지 : 쌍으로 발생되는데 호스트나 네트워크 관리자가 라우터나 다른 호스트로부터 특정 정보를 획득하기 위해 사용

Category	Type	Message
Error-reporting Message	3	- Destination unreachable (목적지 도달못함)
	4	- Source quench (혼잡발생)
	11	- Time exceeded (요청시간 만료)
	12	- Parameter problem (헤더 문제)
	5	- Redirection (라우팅 경로 재지정)
Query Message	8 or 0	- Echo request or reply
	13 or 14	- Timestamp request and reply
	17 or 18	- Address mark request and reply
	10 or 9	- Router solicitation and advertisement

II. ICMP 의 헤더 및 동작

가. ICMP 의 헤더 구조



Copyright 2008 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawings/

나. 오류 보고 메시지 및 질의 메시지

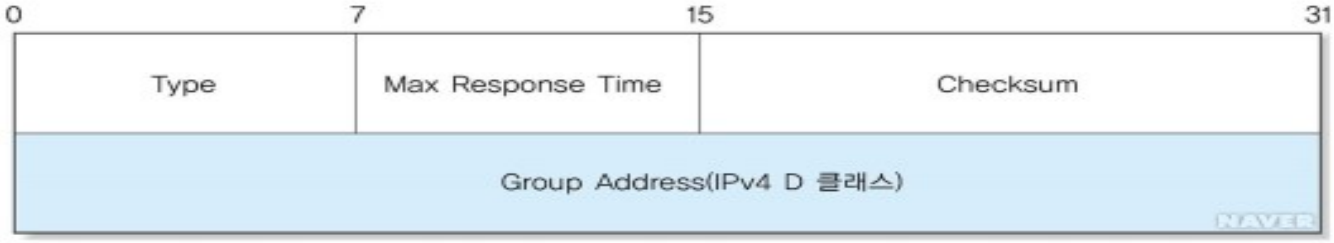
구분	메시지	내용
오류 보고 메시지	Destination unreachable	- 라우터가 데이터그램을 라우팅할 수 없을 때 - 호스트가 데이터그램을 배달 할 수 없을 때
	Source quench	- 발신지 억제. 라우터나 목적지 호스트에서 혼잡으로 인해 데이터 그램이 폐기
	Time exceeded	- 라우터가 time to live 0인 데이터그램 받을 시
	Parameter problem	- 데이터그램의 헤더 부분에 불명료한 점이 있음
	Redirection	- 데이터그램을 재지정시
질의 메시지	Echo request or reply	- 고장진단. 두 시스템이 서로 통신할 수 있는지 확인
	Timestamp request and reply	- IP데이터그램의 왕복 시간 결정 위한 time stamp 요청 및 응답
	Address mark request and reply	- 네트워크 주소와 서브넷 주소 식별 위한 주소 마스크 요청 및 응답
	Router solicitation and advertisement	- 라우터 주소 확인과 라우터 정상 동작 여부 확인

III. 인터넷 그룹관리 프로토콜 IGMP개요

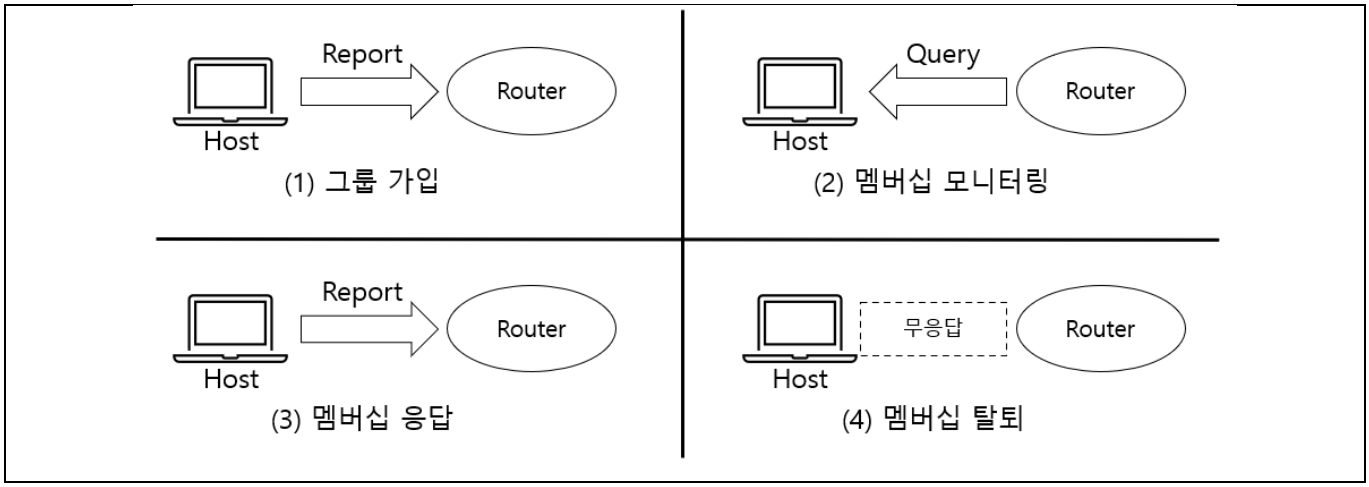
가. IGMP (Internet Group Management Protocol)의 정의

- 다수의 호스트를 논리적 단위 하나로 관리하기 위해 호스트와 라우터 사이에 그룹 멤버 정보를 교환하여 그룹 생성, 제거, 전송 호스트의 그룹 참가, 탈퇴 등 멀티캐스트 그룹의 소속원을 관리하는 프로토콜

(IP 멀티캐스트 그룹-특정 멀티캐스트 주소를 가진 IP 패킷을 주고받을 수 있는 호스트나 라우터 집단)



나. IGMP 그룹방식



- 그룹 가입 및 탈퇴는 Report와 Query 메시지로 확인 가능

다. IGMP의 그룹방식 상세설명

이용방식	항 목		설 명
Addressing 방식	개념		- D Class IP 주소를 통해 각각의 멀티캐스트 그룹 정의
	IP 범위		- 224.0.0.0 ~ 239.255.255.255 범위에서 동적으로 할당되어 사용되고, 수신자 그룹을 지정하여 사용
IGMP Protocol 이용방식	개념		멀티캐스트 그룹에 대한 가입 및 탈퇴 기능을 제공하는 프로토콜
	동작 방식	그룹 가입	가입하고자 하는 그룹에 대해 요청. 호스트는 한번만 전송
		멤버십 모니터링	라우터가 주기적으로 멤버십 유지 확인 메시지 전송
		멤버십 응답	호스트는 멤버십 유지 위해 멤버십 보고 메시지 전송
		멤버십 탈퇴	멤버십 탈퇴시 응답하지 않거나, 탈퇴 메시지 전송
	메시지 유형	Report	호스트에서 라우터로 그룹가입, 멤버십유지 응답 메시지
		Query	라우터에서 호스트로 보내는 모니터링 위한 메시지

- IPv6에서는 IGMP와 유사한 MLD(Multicast Listener Discovery) 사용

"끝"

04	이동형 로봇의 대인 충돌 안전성 평가 방법		
문제	이동형 로봇의 대인 충돌 안전성 평가 방법(정보통신단체표준, TTAK,KO-10.1223)에 대하여 아래 사항을 설명하시오. 가. 충돌, 시험에서의 충격 속도 측정방법 나. 충돌 시험용 인체모형(더미, dummy) 다. 인체모형 측정 데이터		
도메인	디지털서비스	난이도	상(상/중/하)
키워드	TTAK,KO-10.1223, 이동 로봇, 충격, 대인 충돌, 구속 충돌, 비구속 충돌, 더미		
출제배경	이동형 로봇의 주행 간 대인 충돌과 관련한 안전성 평가 방법 규정 표준		
참고문헌	정보통신단체 표준, TTAK,KO-10.1223		
해설자	BP반 김찬일 기술사(제 130회 정보관리기술사 / s2carey@naver.com)		

I. 충돌, 시험에서의 충격 속도 측정 방법

가. 측정 요구사항:

- 충격 속도의 측정은 로봇과 더미의 충돌이 발생하는 시점으로부터 0.2초 이전에 이루어져야 하며, 측정 데이터의 정확도는 ±1 % 이내가 되어야 한다.

나. 측정 방법의 제안

제안	내용
로봇의 바퀴에 의해 작동하는 평판 시스템	- 로봇의 바퀴와 연결된 금속판을 통해 트리거 신호 발생 시간 차를 측정하여 속도 계산
주어진 거리를 가는 데 필요한 시간을 측정하는 방식	- 로봇이 특정 거리를 이동하는 데 걸리는 시간을 측정하여 속도 산출.
영상 기록을 이용한 속도 측정 방식	- 초당 500~2000 프레임의 이미지를 처리하여 로봇의 속도를 측정하는 방식

II. 충돌 시험용 인체모형(더미, dummy)

- 충돌 시험에서 사용되는 인체모형은 로봇 사용 환경과 시나리오를 고려하여 하나 또는 그 이상의 모델을 적용한다. 자동차의 정면 또는 측면 충돌 시험에 사용하는 규격 모델의 사용을 권장한다.

항목	내용
인체 모형 선택	- 로봇 사용 환경과 시나리오에 맞게 하나 이상의 인체모형을 적용하며, 자동차 충돌 시험에 사용되는 규격 모델 사용을 권장
인체 모형의 조립 및 준비	- 모든 신체 부위가 완전히 조립되어야 하며, 시험 중 가속도 변화와 흉부 변위를 측정하기 위한 트랜스듀서를 포함
트랜스 듀서 요구사항	- 직교 감도는 모든 방향에서 5% 미만이어야 합니다. - 계측 채널은 연 1회 이상 표준 장치를 사용하여 교정해야 합니다.

	- 계측 채널의 오차는 1%를 넘지 않아야 합니다.
인체모형의 복장	- 계측 장치가 설치된 더미는 신축성 있는 짧은 소매 상의와 무릎 길이의 바지를 착용

- 계측 장치가 설치된 더미는 몸에 꼭 맞는 면으로 된 신축성이 있는 짧은 소매와 무릎 길 이의 바지를 착용해야 한다

III. 인체모형의 측정 데이터

- 충돌시험을 통해 계측된 인체모형의 측정 데이터는 <표 7-1>에 따라 기록한다. 측정할 값은 시료의 제한사항에 따라 전체 또는 일부를 선택하여 결정할 수 있다. 측정 데이터는 필터링과 디지털화를 통해 후처리 할 수 있으며, 이 경우 트랜스듀서의 감도와 계측 채널의 성능이 고려됨.

<표 7-1> 측정 데이터

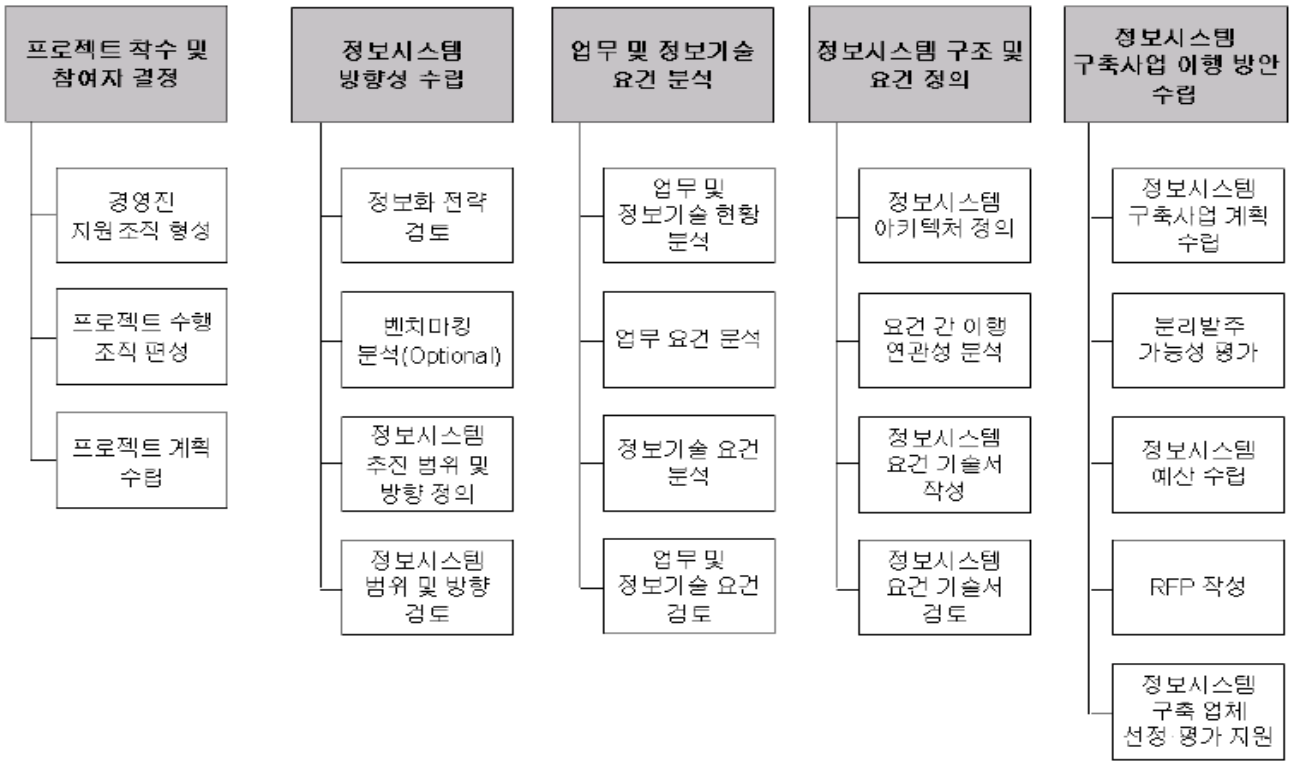
측정할 값	방향
머리	
– 무게중심 가속도	X, Y, Z축
상부 목	
– 힘	X, Y, Z축
– 모멘트	X, Y, Z축
흉부	
– 흉부 편향	X축
대퇴골	
– 힘(오른쪽과 왼쪽)	Z축
경골	
– 힘	X, Z축
– 상부 모멘트	X, Y축
– 하부 모멘트	X, Y축
무릎	
– 이동하는 무릎 관절의 변위	X축
골반	
– 가속도	X,Y, Z측

"끝"

05	ISMP		
문제	정보시스템 마스터 플랜(ISMP, Information System Plan)에 대하여 아래사항을 설명하시오. 가. ISMP와 EA(Enterprise Architecture), ISP(Information System Planning)에 대하여 각각 설명하고, 상호 비교 나. 투입 공수에 의한 사업대가 산정방식을 적용한 ISMP 수립비 산정 절차, 주요내용, 산출물		
도메인	IT경영전략	난이도	중(상/중/하)
키워드	SW 개발 사업, ISMP 세부 절차, EA 구성요소,		
출제배경	IT 전략 수립의 기본인 ISMP, EA, ISP에 대한 지식 이해 확인		
참고문헌	ITPE 기술사회 자료집		
해설자	정상반 정상 기술사(제 124회 정보관리기술사 / itpe_peak@naver.com)		

I. 정보 전략의 수립, ISMP, EA, ISP 설명

가. ISMP의 설명

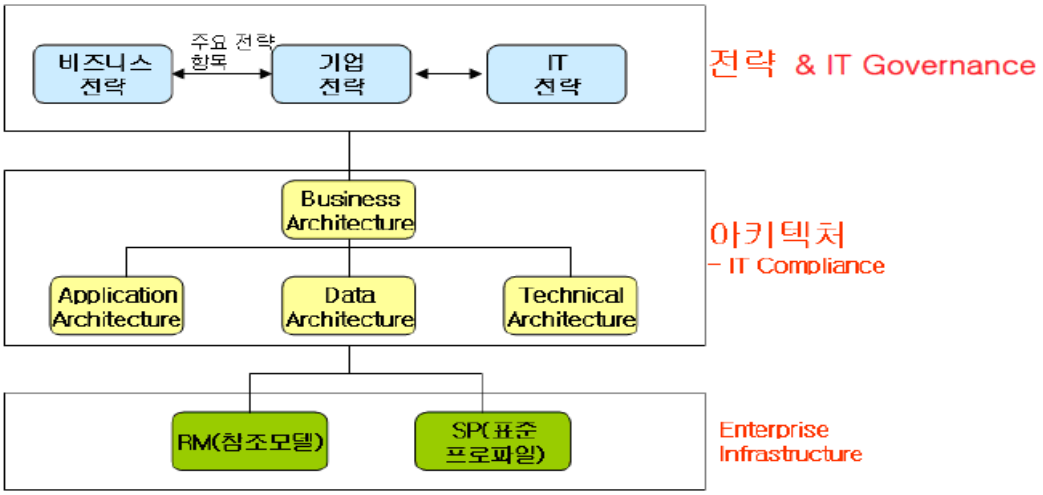


개념	특정 SW 개발 사업에 대한 상세 분석과 제안요청서(RFP)를 마련하기 위해 기능점수 도출 가능 수준까지 요건을 기술하여 구축전략 및 이행 전략 수립하는 활동	
목적	ISP 수행범위 한계점 해결	- 실제 구축될 시스템이 제공할 서비스의 내용, 기능, 기술적 요구사항 등 ISP 수행 범위의 한계를 해결
	부적절 발주 관행 해결	- RFP는 마스터플랜 수립 후 SI기업의 도움을 받아 작성하는 것으로 인식

		- RFP 작성시 ISP 내용을 거의 참고하지 않는 관행 해결
	요구사항 명확화	- 비즈니스적 기능/비기능 요구사항과 기술적 요구사항, 프로젝트 지원 요구사항 상세화 통한 RFP 작성 및 구축 사업계획 수립

- 정보시스템에 대한 요구사항을 상세화하여 사업 규모 및 예산의 객관화된 산정과 함께 불합리한 과업 변경을 최소화

나. EA의 설명

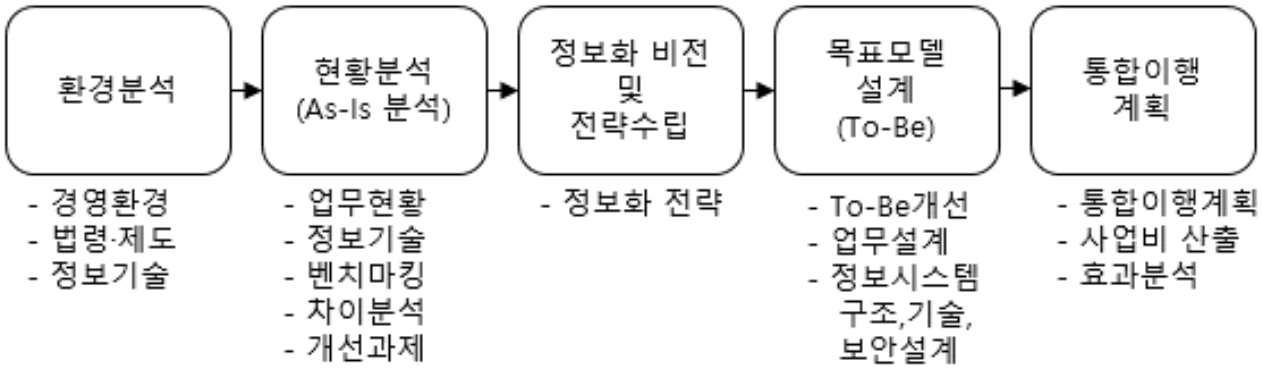


개념	기관에서 정보화를 체계적으로 추진하기 위해 업무, 데이터, 응용 서비스, 정보 기술 등 정보화 구성요소 및 이들 간의 상호 관계를 미리 정해 놓은 정보화 종합 설계도	
구성요소	IT Governance	- 실제 구축될 시스템이 제공할 서비스의 내용, 기능, 기술적 요구사항 등 ISP 수행 범위의 한계를 해결
	Business Architecture	- RFP는 마스터플랜 수립 후 SI기업의 도움을 받아 작성하는 것으로 인식 - RFP 작성시 ISP 내용을 거의 참고하지 않는 관행 해결
	Application Architecture	- 비즈니스적 기능/비기능 요구사항과 기술적 요구사항, 프로젝트 지원 요구사항 상세화 통한 RFP 작성 및 구축 사업계획 수립
	Data Architecture	-기업의 업무수행에 필요한 데이터의 구조를 체계적으로 정의 -전사의 데이터 영역을 분류하며, 업무데이터와 메타 데이터를 구분하거나 업무 데이터는 운영계 데이터, 정보계 데이터 등으로 구분
	Technical Architecture	-비즈니스, 데이터, 애플리케이션 아키텍처에서 정의된 요건을 지원하는 전사의 기술 인프라 체계를 정의
	Security Architecture	-보안정책, 보안원칙, 보안 프레임워크 -보안 참조모델, 보안 아키텍처 패턴 -보안 설계 모델, 보안 구현 모델
	RM	-참조모델(Reference Model) -아키텍처를 위한 기업 내/외부 사례, 표준 참조

	SP	-Standard Profile -각 RM에 대한 Profile(지침) 제공 표준 -구성영역(서비스/기술/세부기술

- 기업의 전략과 아키텍처, 인프라의 전사적 아키텍처 프레임워크 통합 모델

다. ISP의 설명

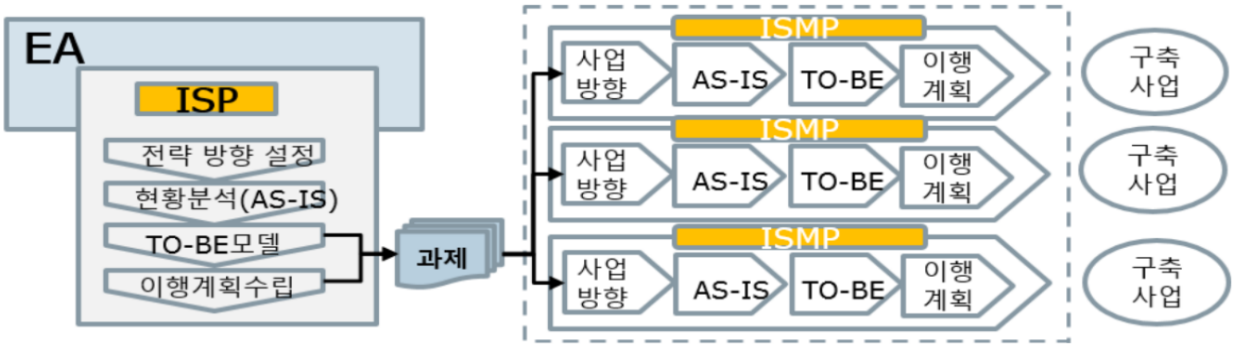


개념	조직의 중장기 마스터 플랜을 지원하기 위한 정보시스템을 계획하고 전략을 수립하는 활동	
수행 내용	환경 분석	- 경영 현황 분석, 법령·제도 분석, 정보기술(IT) 환경분석
	현황 분석 (AS-IS 분석)	- 정보기술(IT) 환경분석, 정보시스템 분석, 벤치마킹, 차이 분석, 이슈통합 및 개선과제 도출
	정보화 비전 및 전략 수립	- 환경분석과 현황분석 결과를 연계하여 정보화 비전, 목표, 단계별 실행 전략 등을 수립
	목표모델설계(TO-BE 모델)	- 개선과제 상세화, 업무프로세스 설계, 정보시스템 구조설계, 데이터 구조설계, 기술 및 보안 구조 설계
	통합 이행계획	- 정보시스템 구축 계획 수립, 총 사업비 산출, 효과 분석

- ISP수립 시 기본적인 단계이고 개별방법론에 따라 순서 및 세부내용은 탄력적으로 조정 가능

II. ISMP, EA, ISP의 상호 비교

가. ISMP, EA, ISP의 개념 관계 비교



나. ISMP, EA, ISP의 개념 상세비교

구분	ISMP	EA/ITA	ISP
개념	특정 사업 분석과 RFP 마련을 위해 업무 및 정보기술에 대한 현황,요구사항을 상세히 기술하며, 구축 전략 및 이행 계획을 수립하는 활동	조직에 사용되는 정보 기술을 활용한 아키텍처와 시스템들을 총괄한 것으로 업무 및 관리 프로세스와 정보기술 간의 관계를 표현한 청사진	조직의 경영 목표 전략을 효과적으로 지원하기 위한 정보화 전략 및 비전을 정의하고 IT사업(과제) 도출 및 road-map을 수립하는 활동
목적	특정 정보시스템의 기능적, 기술적 요구사항 상세화	비즈니스와 정보기술 간의 유연한 융합	경영전략과 정보화 전략 연계 및 새로운 정보기술 반영
범위	단위프로젝트 또는 단위 프로젝트의 묶음	비즈니스, 데이터, 어플리케이션, 기술 아키텍처	전사, 서비스 또는 부서 대상 정보화전략
주요활동	정보시스템 구축 범위 및 방향 수립 정보시스템에 대한 기능적, 기술적 요건도출 정보시스템 구조 및 요건 상세기술 정보시스템 구축사업 이행계획수립 정보시스템 예산 산정 및 업체 선정/평가 지원	기업 내/외부 환경분석 EA 목적 및 방향정의 EA 프레임워크 정의 참조모델 정의 EA 원칙 수립 현행 아키텍처 정보 구축 목표 아키텍처 구축 EA 관리 체계 정의	경영환경 분석 최신 정보기술 동향분석 업무분석 정보시스템 구조 분석 정보전략 및 정보관리 체계 수립 미래업무 프로세스 및 정보시스템 구조 설계 To-Be 로드맵 수립
주요 산출물	RFP 정보시스템 예산	EA 비전, 원칙 참조모델(BRM, SRM, DRM, TRM) AS-IS/TO-BE 아키텍처 (비즈니스, 데이터, 어플리케이션, 기술) EA 거버넌스	경영환경 분석 및 정보기술동향 분석 보고서 업무 및 정보시스템 분석 보고서 IT비전 및 전략 이행과제 및 로드맵

- EA/ITA 목표 아키텍처 구조 이행 기반으로 세부사업 구조인 ISMP 도출 진행

III. 정보시스템 마스터플랜(ISMP) 수립비 산정절차, 주요내용, 산출물

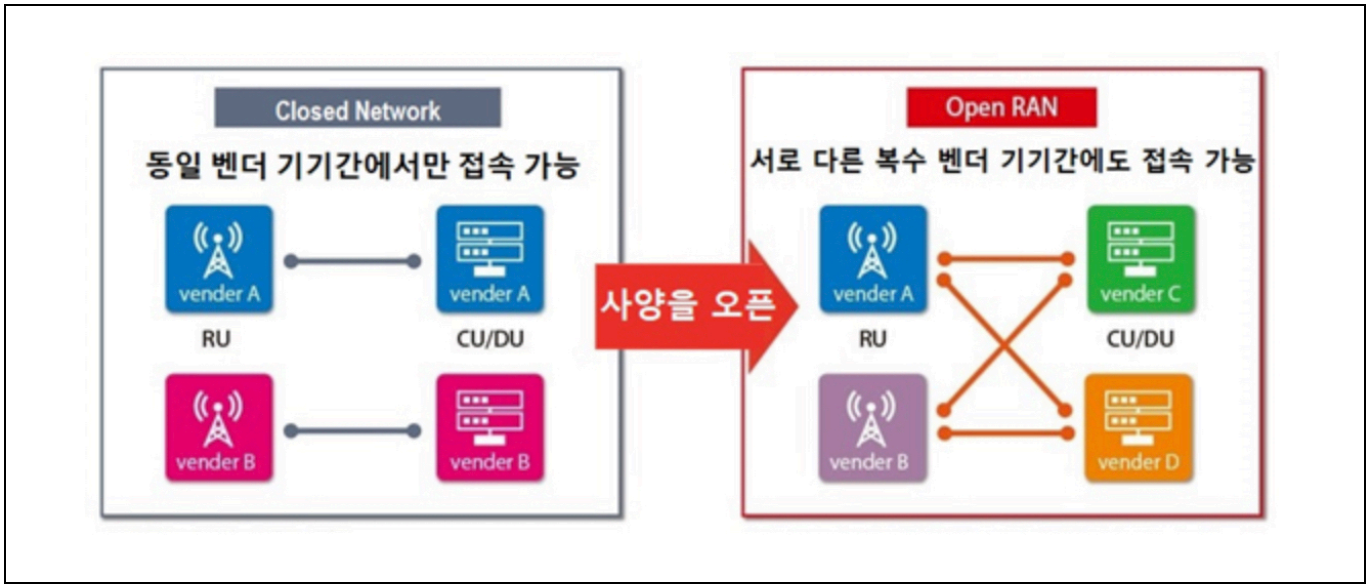
절차	주요내용	산출물
1. 사전준비	○ 컨설팅의 대상 업무 범위를 확정하고, 업무별 요구사항을 결정한다.	컨설팅 대상 업무 요구사항
2. 투입공수 산정	○ 컨설팅의 업무특성을 고려하여 투입직무를 결정한다. ○ 업무범위와 요구사항을 고려하여 필요한 직무별 투입인력의 수와 기간을 결정한다.	IT직무별 투입공수
3. 직접인건비 계산	○ 컨설팅을 수행할 인력의 직접인건비를 계산한다. - 직접인건비 = 직무별 투입공수 × 소프트웨어 기술자 평균임금	직접인건비
4. 제경비 및 기술료 계산	○ 컨설팅 업무를 수행할 인력의 제경비와 기술료를 계산한다. - 제경비 계산 = 직접인건비 × 144~154% - 기술료 계산 = (직접인건비 + 제경비) × 20~40%	제경비 기술료
5. 직접경비 계산	○ 컨설팅 업무에 필요한 직접경비를 계산한다.	직접경비
6. ISMP 컨설팅 대가 산정	○ 컨설팅 대가를 산정한다. - 컨설팅 대가 = 직접인건비 + 제경비 + 기술료 + 직접경비	컨설팅 대가

- 최근 2023년 개정버전으로 제경비율 4% 상향된 144~154%로 변경

"끝"

06	OPEN RAN		
문제	6. 개방형 무선 접속망 Open RAN(Open Radio Access Network)은 서로 다른 장비 간 상호 연동을 가능하게 하는 기술이다. 이와 관련하여 아래 사항을 설명하시오. 가. Open RAN의 개념 나. Oepn RAN의 구성요소 다. RAN과 Open RAN의 비교		
도메인	네트워크	난이도	중 (상/중/하)
키워드	벤더 종속성 제거, O-CU, O-DU, O-RU, O-CP, O-UP		
출제배경	네트워크 벤더 종속성 제거를 통한 O-RAN 생태계 조성 및 5G 기반 기술 활용		
참고문헌	ITPE 기술사회 자료집		
해설자	정상반 정상 기술사(제 124회 정보관리기술사 / itpe_peak@naver.com)		

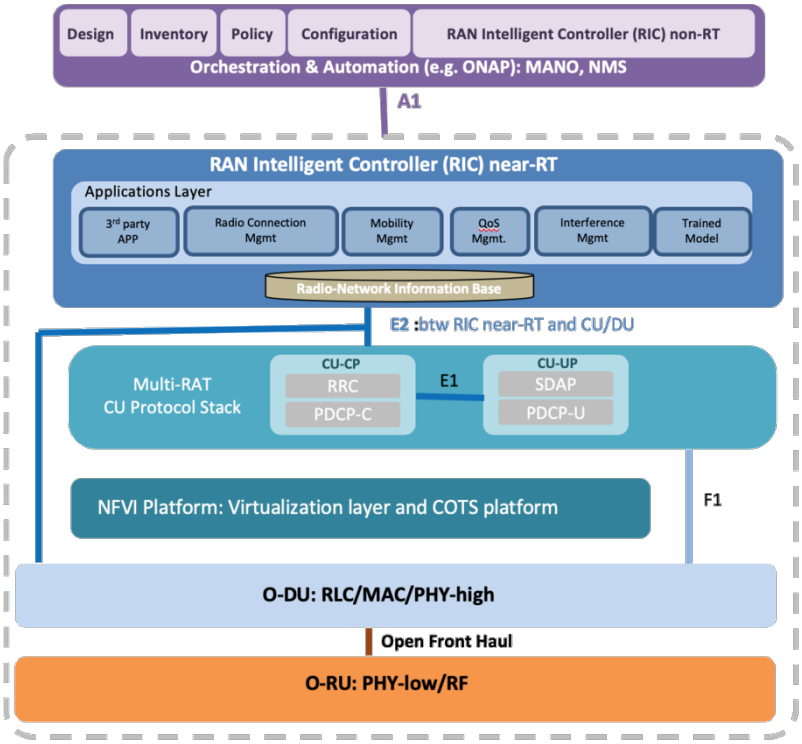
I. 네트워크의 벤더 종속성 탈피 O-RAN의 등장배경



- 네트워크 기술 발달에 따른 장비들의 일부 업체의 종속성을 탈피하고 네트워크 구축 효율성을 확장하기 위해 개방형 아키텍처 구축 대두

II. Open RAN의 개념 및 구성요소

가. Open RAN의 개념



- 네트워크 장비 운용에 필요한 RAN 구간에 가상화 기술을 적용하여 Hardware와 Software를 분리하기 위한 Apache 2.0 License의 개방형 아키텍처

나. Open RAN의 구성요소

구성 요소	기반 기술	설명
RIC (RAN Intelligent Controller)	- RIC near-RT(Realtime) - RIC non-RT(Realtime)	- 데이터 수집과 분석을 기반으로 RAN 요소(element)와 자원을 제어하고 최적화를 수행
O-CU (O-RAN Centralized Unit)	- RRC (Radio Resource Control) - SDAP (Service Data Adaption Protocol) - PDCP (Packet Data Convergence Protocol)	- RRC 및 PDCP 계층을 실행하는 중앙 집중식 장치 - CU Control Plane과 CU User Plane로 구성 - 미드홀(Midhaul) 인터페이스를 통해 여러 O-DU 작동을 제어
O-DU (O-RAN Distributed Unit)	- RLC (Radio Link Control) - MAC (Media Access Control) - High PHY	- O-RU 근처에 위치해서 RLC(Radio Link Control), MAC(Media Access Control) 및 PHY 계층 일부를 실행하는 분산 장치
O-RU (O-RAN Radio Unit)	- Digital Front End (DFE) - RF Front End (RF FE) - Low PHY - Beamforming	- 안테나(Antenna) 근처에 위치하거나 혹은 통합 - 안테나(Antenna)에서 송수신되는 무선 신호를 프론트 홀(Fronthaul)을 통해 O-DU(Distributed Unit)로 전송할 수 있는 디지털 신호로 변환

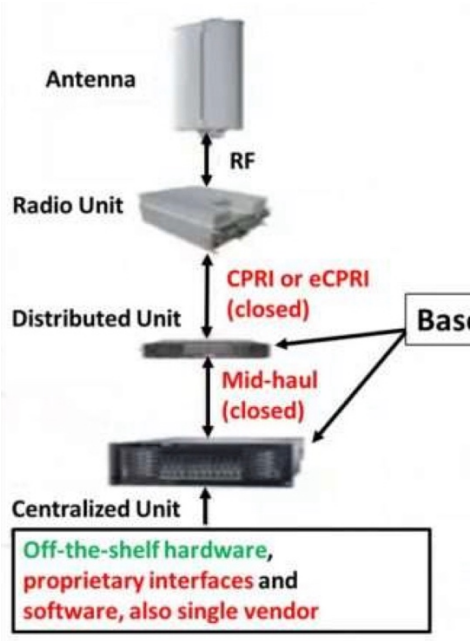
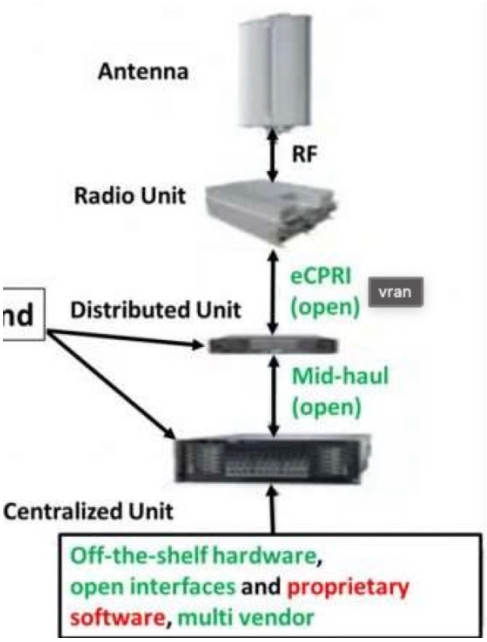
III. RAN과 Open RAN의 비교

가. RAN과 Open RAN의 개념 비교

RAN	O-RAN
- 원격으로 제어되는 머신 등의 기기를 무선 링크를 통해 네트워크의 다른 부분으로 연결하는 안테나, 무선장치, 컨트롤러를 갖춘 기지국으로 구성된 무선 통신 기술	- 가상화, 마이크로서비스, 컨테이너 기반의 기술의 사용과 개방형 인터페이스를 하용한 통신 서비스 공급업체 네트워크 내에서 사용되는 RAN 기술

- 기존 RAN의 종속성과 구축 효율성을 위해 O-RAN 으로 개선

나. RAN과 Open RAN의 상세 비교

구분	RAN(Traditional RAN)	O-RAN(Open RAN)
개념도		
공급	- 단일 벤더(Single Vendor)	- 다중 벤더(Multiple Vendors)
플랫폼	- 공급 업체에 종속되어 시장 출시 기간이 길며, 고비용	- Software Defined - 개방형 White-Box 하드웨어
모듈성	- 제어(Control)와 데이터 및 고유 Interface가 통합되어 구성	- 제어(Control)와 데이터 및 Open API가 모두 분리
애플리케이션 및 네트워크 적응성	- 사전에 프로그래밍 된 고정된 제어 로직과 고정된 네트워크 리소스	- 실제 네트워크 조건에 따라 프로그래밍 가능

- 도입 기업의 세부 특성에 따라 RAN과 O-RAN 고려 적용

"끝"

ITPE 기술사회
제132회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2024년 01월 27일
집 필 강정배PE, 안경환PE, 김찬일PE, 전일PE, 정상PE, 안수현PE
출 판 **ITPE(Information Technology Professional Engineer)**
주 소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층
ITPE 선릉점 서울시 강남구 선릉로 86길 15, 3층 IT교육센터 아이티피이
ITPE 강남점 서울시 강남구 테헤란로 52길 21 파라다이스벤처타워 3층 303호
ITPE 영등포점 서울시 영등포구 당산동2가 하나비즈타워 7층 ITPE
연락처 070-4077-1267 / itpe@itpe.co.kr