1980호
2021.01.20.
ISSN 1225-6447

Weekly ICT Trends

주간기술동향



IITP 정보통신기획평가원

- 「주간기술동향」은 **과학기술정보통신부** 「ICT 동향분석 및 정책지원」 과제의 일환으로 정보통신기획평가원(IITP)에서 발간하고 있습니다.
- 「주간기술동향」은 인터넷(http://www.itfind.or.kr)을 통해 서비스를 이용할 수 있으며, 본 고의 내용은 필자의 주관적인 의견으로 IITP의 공식적인 입장이 아님을 밝힙니다.
- 정보통신기획평가원의 「주간기술동향」 저작물은 공공누리 "출처표시-상업적 이용금지" 조건에 따라 이용할 수 있습니다. 즉, 공공누리의 제2유형에 따라 상업적 이용은 금지하나, "별도의 이용 허락"을 받은 경우에는 가능하오니 이용하실 때 공공누리 출처표시 지침을 참조하시기 바랍니다.
  (http://www.kogl.or.kr/info/license.do 참고)

  예시) "본 저작물은 'OOO(기관명)'에서 'OO년' 작성하여 공공누리 제O유형으로 개방한 '저작물명(작성자:OOO)'을 이용하였으며, 해당 저작물은 'OOO(기관명), OOO(홈페이지 주소)'에서 무료로 다운받으실 수 있습니다."



Weekly ICT Trends
주간기술동향
1980호
ISSN 1225-6447

기획시리즈 2

스마트제조 및 산업제어시스템 융합보안 동향

[최윤성/고려대 융합보안대학원]

Ⅰ. OT/ICS 보안의 필요성
Ⅱ. ICS 보안사고 사례
Ⅲ. ICS 보안위협 대응방안
Ⅳ. 결론 및 시사점

ICT 신기술 15

무인기의 안전한 운영을 위한 보안 기술

[왕기철·이병선·김성창/한국전자통신연구원]

Ⅰ. 서론
Ⅱ. 무인기 시스템 및 보안 취약점
Ⅲ. 무인기 시스템에 대한 공격 및 대응 방안
Ⅳ. 결론

ICT R&D 동향 27

초저전력 뉴럴 스파이크 프로세서 SoC

[이재진/한국전자통신연구원]

초고속 직렬 통신 인터페이스 IP

[정덕균/서울대학교]

chapter 1

스마트제조 및 산업제어시스템 융합보안 동향

최윤성 ‖ 고려대 융합보안대학원 교수

산업제어시스템(ICS)은 그동안 외부 접근이 차단된 폐쇄적인 환경과 특정 회사의 기술로 구축되어, 대중적인 사이버 공격이 통하지 않는다는 이유로 보안에 소홀하였다. 최근 ICT 융합에 따른 스마트화로 시스템의 외부 연결이 늘어나고 있어, 단 한 번의 공격 성공으로 연속적인 피해가 발생할 수 있는 보안 위협에 점차 노출되고 있다. 과거 스턱스넷(Stuxnet, 2010), 블랙에너지 & 킬디스크(BlackEnergy & KillDisk, 2015), 인더스트로이어(Industroyer, 2016) 같은 ICS 악성코드가 국가 핵심 기반 시설을 노리는 정치적 목적의 사이버 테러리즘이었다면, 최근 유행하는 ICS 랜섬웨어 로커고가(LockerGoga, 2019), 에칸스(Ekans, 2020)는 데이터를 암호화하여 협박하는 수준을 넘어, 금전적 이득을 극대화하기 위해 특정 산업과 OT의 가용성을 침해하는 표적 공격을 감행하고 있어, 이에 대한 사전대비가 중요하다.

I. OT/ICS 보안의 필요성

산업제어시스템(Industrial Control System: ICS)은 우리가 잘 아는 기간시설, 예를 들어, 원자력발전소, 철도·항공기·선박, 교통신호 제어 등 다양한 분야에서 활용되고 있다. 또한, 최신 정보통신기술(Information Communication Technology: ICT)과 접목으로 우리 앞에 펼쳐질 스마트 공장, 스마트시티의 기반으로 발전이 기대되고 있다. ICT

* 본 내용은 최윤성 교수(☎ 02-3290-4816, yunseong@korea.ac.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

전문가에게 산업제어시스템은 낯선 분야로 관련 용어들이 다소 생소하게 느껴지겠지만, 살면서 한 번도 이용해보지 않은 사람은 없을 정도로 우리 삶에 밀접한 분야이다.

컴퓨터 분야가 주로 정보기술(IT)을 다루는 데 반해, ICS 분야에서는 이를 운영기술(Operation Technology: OT)이라고 부르며, OT는 산업제어시스템(ICS)의 자동화 및 이를 실행하는데 필요한 모든 시스템 환경을 의미한다. 운영기술은 공장·제조(Factory & Manufacturing) 산업의 특성을 반영하여 지속성, 효율성, 실시간성 등의 향상에 초점을 맞추어 발전해 왔으며, 최근 스마트 제조·혁신의 요구로 과거 "소품종-대량 생산" 위주에서 "다품종-맞춤형 생산" 방식으로 진화하는 시기에 놓여 있다.

OT 환경의 스마트화는 IoT 센서, AI/빅데이터, 5G 등 다양한 ICT 최신 기술과 접목하여 발전하고 있으며, 과거 공장이나 기업 내부에만 머무르던 제조 데이터는 이제 지리적 위치에 영향을 받지 않고 활용되도록 글로벌 IT 시스템 및 클라우드 서비스로 옮겨가고 있다.

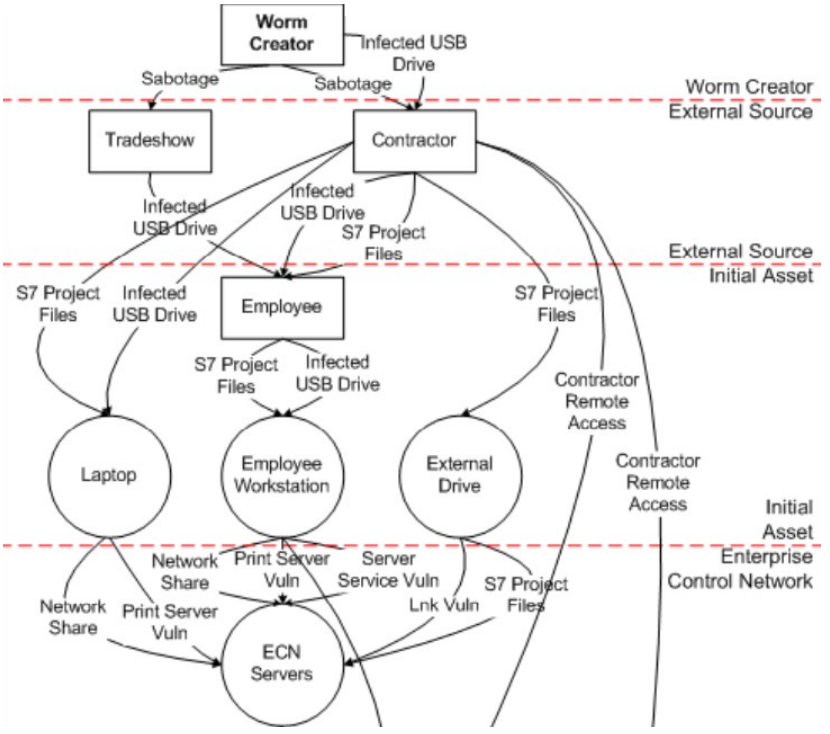
OT 보안의 관점에서 이렇게 새로운 기술과 외부 연결성이 추가되면, 당연히 방어해야 할 공격 접점(Attack Surface)과 보호해야 할 대상 자산(Security Asset)이 늘어난다. 스스로 작업하는 자율협동로봇이나 증강현실(AR) 웨어러블 장치, 산업용 IoT 장비 등이 내부에서 중요한 데이터를 직접 처리하고 무선으로 전송하므로, 기기 자체 및 통신 취약점에 대한 대비가 필요하게 되었다. 제조실행시스템(MES), ERP, CRM 등 IT 경영 시스템과 워크스테이션, 필드 장비 등을 연결하는 경우에도, 연쇄적인 보안 위협에 노출될 수 있으므로, 새로운 시스템의 도입 시에는 항상 보안성이 함께 고려되어야 한다.

하지만 OT 현장의 현실은 IT 보안과는 여러모로 다르며, 당장 어떻게 피해에 대비할 수 있을지, 어디서부터 무엇을 보완해야 할지 쉽게 감이 오지 않는다. 본 고에서는 과거에 발생한 주요 ICS 보안사고 사례를 분석함으로써, 지금 벌어지는 현상을 깊이 있게 이해하고, 우리 앞에 전개될 양상에 대해서도 알아보고자 한다.

Ⅱ. ICS 보안사고 사례

1. ICS 사이버 테러 사례

2010년 이란에서 원자력발전소가 사이버 공격을 당하는 첫 번째 사건이 발생했다.



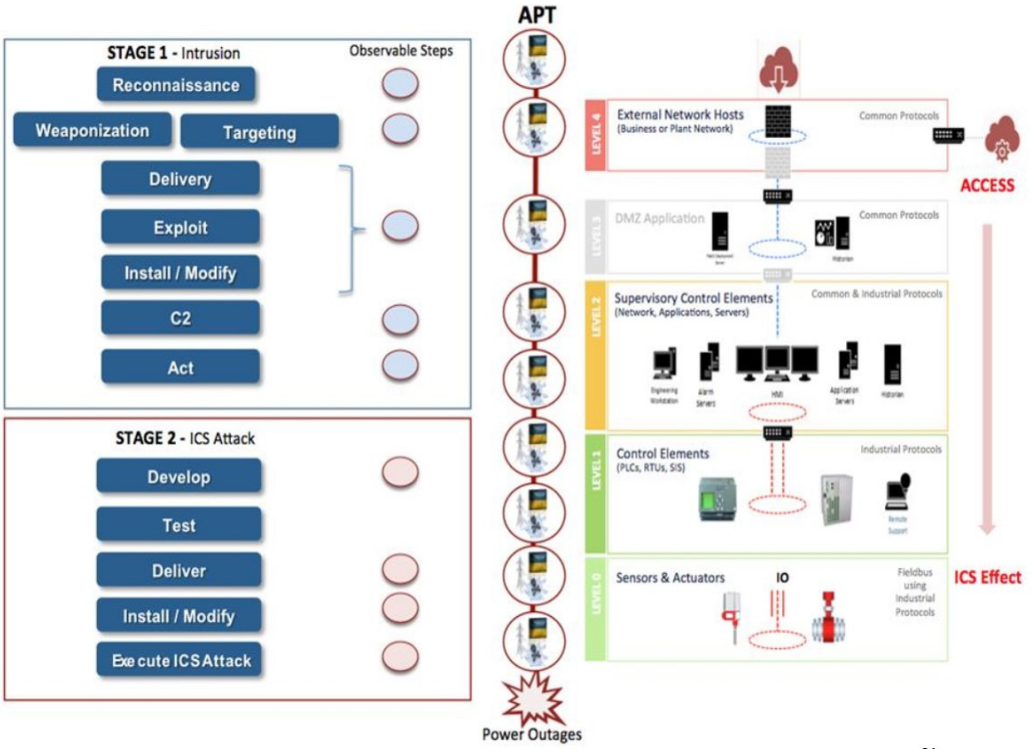
〈자료〉 Eric Byres, "The Future of Critical Infrastructure Security", Byres Security Inc. 2011, p.18.

[그림 1] Stuxnet의 다양한 공격 루트

이란 원전의 공격에 사용된 스턱스넷(Stuxnex) 악성코드는 독일 지멘스사 S7 PLC의[1] STEP 7 소프트웨어를 사용하는 SCADA[2] 시스템 네트워크의 침입을 목표로 개발되었고, 악성코드가 담긴 물리적 USB를 전달하는 사회공학기법(Social Engineering) 공격으로 폐쇄망에 침투하였다([그림 1] 참고). 시스템 제어에 성공한 이후에도 프로세스 데이터 및 로직을 변경하여, 원전 운영자가 이상 징후를 알아차리지 못하도록 하였다.

원전 제어 시스템의 통제권을 획득한 공격자는 1,000여 개에 달하는 고농축 우라늄 원심 분리기에 과부하를 일으켜 사용 불가 상태로 만드는 피해를 주었다. 보안 연구자들은 스턱스넷 악성코드를 원격에서 물리적인 공격이 가능한 무기라는 의미로 "사이버 미사일"이라 명명하였는데, 스턱스넷은 악성코드가 PLC를 어떻게 장악하는지를 전 세계에 보여

1) PLC(Programmable Login Controller): 센서, 모터 등과 프로그램에 의해 순차적인 로직을 처리하는 장치
2) SCADA(Supervisory Control And Data Acquisition): 지리적으로 넓게 분포된 주로 통신, 수도 및 석유/가스 정제, 운송과 같은 산업 플랜트 장비를 모니터링하고 제어하는데 사용되는 시스템으로 ICS는 SCADA를 포함함



〈자료〉 "Analysis of the Cyber Attack on the Ukrainian Power Grid", E-ISAC SANS, 2016. p.5.

[그림 2] ICS 사이버 킬체인과 퍼듀 모델 매핑

준 첫 사례가 되었다.

두 번째 사례는 2015년에 우크라이나의 전력망 시스템을 공격한 사건이다. 이 사건은 발전소로부터 전력을 공급받아, 가정이나 상가, 공장 등에 분배하는 배전망 회사 ICS에 대한 사이버 공격이었다. 총 3곳의 배전 회사 IT 시스템이 사이버 공격을 받아, 결국 변전소와의 전기 연결이 3시간 동안 끊어졌고, 약 225,000 가구가 피해를 보았다. 공격자는 마이크로소프트 오피스 문서를 조작하여 블랙에너지 3(BlackEnergy 3) 악성코드가 포함된 스피어피싱(Spear-phishing) 이메일을 보내 해당 회사의 IT 네트워크를 장악하는 1단계 공격을 수행하였다([그림 2]의 Stage 1 참조).

침투 성공으로 거점을 확보한 공격자는 2단계로 킬디스크(KillDisk) 악성코드를 사용해 핵심 시스템의 마스터 부트 레코드(MBR)를 삭제하여 배전 시스템과 연결 복구를 지연시키고, 흔적이 남지 않도록 관련 로그 기록 또한 삭제하였다. 변전소의 필드 장비를 대상으

로는 맞춤형 악성 펌웨어를 삽입하여 직렬-이더넷(Serial to Ethernet) 변환 장치를 작동 불가능하게 만들고, 무정전 전원공급장치(UPS)를 비활성화하는 등 SCADA 운영에 지장을 주기 위한 다각도의 공격을 수행하였다. 정전 피해가 발생한 이후에도 공격자는 고객이 정전 사실을 회사에 알리는 것을 지연시키기 위해 회사 콜센터에 전화 서비스 거부 공격(DoS)을 수행하여 피해 지속시간이 늘어나도록 하는 치밀함까지 보였다.

우크라이나 전력망 시스템에 대한 사이버 공격은 이것으로 그치지 않았다. 2015년 공격 때 획득한 정보를 바탕으로, 2016년 12월에는 ICS에 대한 직접적인 공격이 가능한 인더스트로이어(Industroyer) 악성코드를 퍼트려 우크라이나의 수도 키예프의 송·변전소를 사이버 공격하여 도시의 약 20%에 한 시간 가량 정전 피해가 발생했다. 인더스트로이어는 특정 업체나 구성에 한정되지 않고, 전력망 및 네트워크 통신에 피해를 줄 수 있으며, 모듈식으로 구성되어 DNP 3 프로토콜 스택 등 추가 탑재가 가능했다. DRAGOS의 분석 결과 IEC 104, 61850, OPC DA Payload 기능 등이 함께 발견되었다[3].

[표 1] ICS 사이버 테러리즘 주요 피해 사례(요약)

대상(발생년도)	악성코드명	폐쇄망 침투 방법	피해 범위
이란 원자력발전소 (2010)	Stuxnet	사회공학 기법 (감염된 USB 드라이브)	원심 분리기 1,000여 개 사용 불가
우크라이나 배전회사 (2015)	BlackEnergy 3 & KillDisk	스피어 피싱 이메일 (MS 오피스 첨부파일)	22만 5,000 가구에 3시간 동안 정전 피해 발생

〈자료〉 고려대 융합보안대학원 자체 작성

2. ICS 랜섬웨어 피해 사례

앞선 두 가지 사례가 사이버 테러리즘 수준의 매우 정교하고, 사회에 큰 영향을 끼친 심각한 공격이라면, 최근 ICS에 대한 공격은 경제적 이익을 목표로 하는 랜섬웨어 공격이 주를 이루고 있다. 랜섬웨어는 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만들고 이를 풀어주는 대가로 금전을 요구하는 악성 프로그램이다.

지난 2018년 8월, 세계 최대 반도체 위탁생산 기업인 대만의 TSMC가 워너크라이(WannaCry) 랜섬웨어에 감염되어 하루 동안 일부 공장의 생산라인 가동이 중단되었고, 이로 인해 약 2,800억 원의 손해를 입은 것으로 알려졌다. 이번 사고는 직원이 새 설비에 소프트웨어를 설치하는 과정에서 사용한 USB가 랜섬웨어를 옮긴 것으로 알려졌지만, 이

작은 실수에 대한 대가로는 피해가 너무나도 컸다.

해커들은 ICS를 대상으로 하는 사이버 공격은 물리적인 피해와 직접적으로 연결되어 있어 심각성이 높다는 점을 노리고 공격하고 있으며, ICS만을 전문적으로 공격하는 랜섬웨어가 나타나고 있다. 2019년에는 세계 최대의 알루미늄 제조사인 놀스크 하이드로(Norsk Hydro)가 랜섬웨어로 인한 피해를 보았다. Norsk Hydro는 세계 곳곳에 지사가 있었는데, 이를 연결하는 글로벌 IT 네트워크 시스템이 로커고가(LockerGoga) 랜섬웨어에 감염된 것이다.

LockerGoga는 공장 시스템의 데이터를 사용할 수 없도록 암호화하였고, 이 때문에 알루미늄 공장의 운영을 수동 모드로 전환하였지만 알루미늄 원재료를 뜨거운 열로 녹여 가공하는 작업의 특성상 생산 및 운영 차질은 불가피했다. 결국, 이 회사는 75만 달러(약 900억 원)에 이르는 피해를 보게 되었고, 이 사고로 전 세계 알루미늄 생산량이 감소하여 알루미늄 가격이 상승하는 결과까지 초래하였다. LockerGoga는 Norsk Hydro 공격 이전에도 프랑스의 엔지니어링 기업을 공격한 바 있으며, 이후 미국 화학 기업의 침해 사고 컴퓨터에서도 발견되었다[4].

2017년부터 전 세계적으로 대유행한 WannaCry 랜섬웨어의 경우, 소수의 PC 감염에서 시작하여 이후 무차별적인 확산을 한다면, LockerGoga는 시스템에 먼저 침투한 이후 내부 정보를 활용하여 배포하는 방식으로 변했다. 기존 랜섬웨어는 외부 원격 서비스(Remote Service)를 이용하거나, 원격 파일 복사(Remote File Copy) 기능을 통해 전파(Propagation) 되었지만, 최근 랜섬웨어는 기본 자격증명(Default Credentials) 또는 유효 계정(Valid Accounts)을 탈취하여 전파 권한을 획득하는 방식으로 바뀐 것이다. NorCert의[3] 조사 결과를 보면 LockerGoga는 일반적인 악성코드와 다르게 네트워크 통신을 하지 않아, 전통적인 C2, DNS를 이용하는 수법도 사용하지 않았고, 침투에 성공한 후 내부 Windows Active Directory의 정보를 활용하여 확산하였다[5].

2020년에는 일본의 자동차업체 혼다(Honda)의 공장이 사이버 공격으로 멈춰섰다. 지난 6월, 사이버 공격을 받은 사내 네트워크 시스템이 장애를 일으킨 것이다. 이로 인해 미국과 인도, 브라질, 터키 등 전 세계 공장 여러 곳의 생산라인 관리시스템이 마비되었고, 일본 공장에서는 완성차 출하가 중단되었다.

3) NorCert(Norway Computer Emergency Response Team): 노르웨이 국가 컴퓨터 비상 대응팀

VirusTotal의 연구원은 에칸스(Ekans)[4] 악성코드 샘플에서 혼다의 내부 네트워크로 추정되는 도메인 주소 'mds.honda.com'을 발견했다. Ekans는 소스코드에 포함된 DNS와 IP 주소가 서로 일치하는 경우에만 데이터 암호화를 하도록 구성되어 있어, Ekans가 특정 기업과 조직을 대상으로 공격한다는 것을 보여준다.

Kaspersky ICS CERT 데이터에 따르면 Ekans의 공격 대상에는 혼다 이외에도 전력회사인 Enel Group, 독일의 자동차부품 회사, 의료장비 회사 등이 포함되어 있었다. 또한, 일본, 중국, 유럽의 다른 시스템에서도 Ekans 유사 샘플이 발견되었으며, 혼다 외 다른 완성차 제조업체와 부품제조 회사도 공격받았을 것으로 추측했다[6].

```
taskkill /im proficy administrator.exe /f
taskkill /im ntevl.exe /f
taskkill /im prproficymgr.exe /f
taskkill /im prrds.exe /f
taskkill /im prrouter.exe /f
taskkill /im prconfigmgr.exe /f
taskkill /im prgateway.exe /f
taskkill /im premailengine.exe /f
taskkill /im pralarmmgr.exe /f
taskkill /im prftpengine.exe /f
taskkill /im prcalculationmgr.exe /f
taskkill /im prprintserver.exe /f
taskkill /im prdatabasemgr.exe /f
taskkill /im preventmgr.exe /f
taskkill /im prreader.exe /f
taskkill /im prwriter.exe /f
taskkill /im prsummarymgr.exe /f
taskkill /im prstubber.exe /f
taskkill /im prschedulemgr.exe /f
taskkill /im cdm.exe /f
taskkill /im musnotificationux.exe /f
taskkill /im npmdagent.exe /f
taskkill /im client64.exe /f
taskkill /im keysvc.exe /f
taskkill /im server_eventlog.exe /f
taskkill /im proficyserver.exe /f
taskkill /im server_runtime.exe /f
taskkill /im config_api_service.exe /f
taskkill /im fnplicensingservice.exe /f
taskkill /im workflowresttest.exe /f
taskkill /im proficyclient.exe4 /f
```

[LockerGoga]

```
0x600dec: proficy administrator.exe
0x5f224e: ntevl.exe
0x5fa55a: prproficymgr.exe
0x5f200e: prrds.exe
0x5f6642: prrouter.exe
0x5f9ec6: prconfigmgr.exe
0x5f8552: prgateway.exe
0x5fb5b1: premailengine.exe
0x5f905c: pralarmmgr.exe
0x5f9dc7: prftpengine.exe
0x5fd66e: prcalculationmgr.exe
0x5fb617: prprintserver.exe
0x5fb4b2: prdatabasemgr.exe
0x5f91ac: preventmgr.exe
0x5f7356: prreader.exe
0x5f6756: prwriter.exe
0x5faf2a: prsummarymgr.exe
0x5f7d25: prstubber.exe
0x5fb7c0: prschedulemgr.exe
0x5f119e: cdm.exe
0x5fe4d4: musnotificationux.exe
0x5f8287: npmdagent.exe
0x5f76da: client64.exe
0x5f310e: keysvc.exe
0x5fca0b: server_eventlog.exe
0x5fb5c2: proficyserver.exe
0x5fbfbf: server_runtime.exe
0x5feaaa: config_api_service.exe
0x5fff0e: fnplicensingservice.exe
0x5fd592: workflowresttest.exe
0x5fb0fa: proficyclient.exe
```

[Ekans]

〈자료〉 "Ransomware Against the Machine", FireEye Threat Research, Feb. 2020, p.4.

[그림 3] LockerGoga와 Ekans에서 발견된 OT 관련 프로세스 리스트

4) Ekans 랜섬웨어는 스펠링을 거꾸로 읽은 Snake 또는 SnakeHose로도 불린다.

LockerGoga와 Ekans의 공통점은 ICS를 표적으로 삼아 맞춤형 공격을 한다는 것이다. 이 두 개의 랜섬웨어에서 제너럴 일렉트릭(General Electric)사의 데이터 히스토리 관리시스템인 프로피시(Proficy) 프로세스가 동일하게 확인되었다([그림 3] 참고). 특히, 이들 악성코드는 공격 전에 OT 관련 소프트웨어 프로세스를 종료하고, ICS에서 사용하는 파일을 암호화하여 공격 성공률을 높였다. Ekans는 1,000개 이상의 OT 프로세스 Kill List를 보유하고 있으며, 동종 랜섬웨어인 MegaCortex 및 Maze에서도 유사한 OT 프로세스 리스트가 관찰되었다,

[표 2] ICS 랜섬웨어 주요 피해 사례(요약)

대상 (관련업종)	악성코드명	피해액	추가 공격 사례
2018년 대만 TSMC (반도체 생산 공장)	WannaCry	약 2,800억	르노(자동차), 보잉(항공) 등 불특정 다수 기업
2019년 노르웨이 Norsk Hydro (알루미늄 생산 공장)	LockerGoga	약 900억	프랑스 엔지니어링 기업, 미국 화학기업 2곳 등
2020년 일본 Honda (자동차 공장)	Ekans (Snakehose)	미상 (생산 중단)	Enel그룹(전력), Fresenius(헬스케어), 독일 자동차부품 및 의료기기 회사 등 표적 공격

〈자료〉 고려대 융합보안대학원 자체 작성

III. ICS 보안위협 대응방안

이처럼 공장 시스템이 랜섬웨어에 감염되면 데이터 가시성에 문제가 발생하고, 이후 제조 공정의 가용성 훼손으로 이어져, 결국 생산 차질과 금전적 손해로 이어진다.

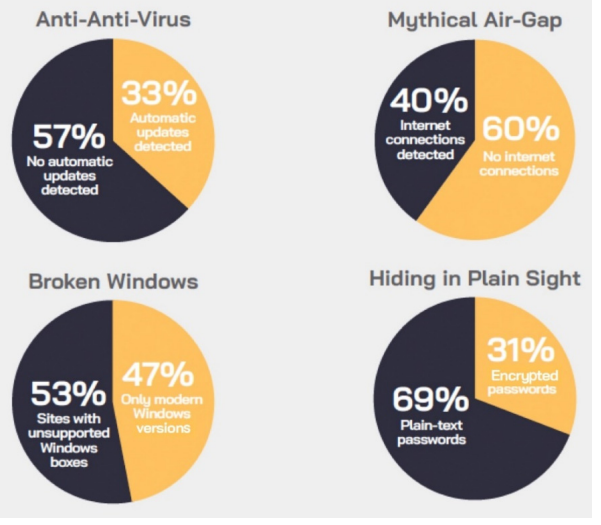
랜섬웨어 감염과 같은 침해 사고는 해당 기업에서 의도적으로 보도하지 않는 이상 피해 사실이 외부에 알려지기 어렵지만, 과거 IT 기업들이 보안 사고로 겪어 왔던 여러 가지 문제들이 현재의 OT 영역에서 발생하고 있다는 사실에 주목해야 한다. 일부 기업은 대외 신뢰도 하락을 이유로 대부분 피해 사실을 숨기려 하지만, 랜섬웨어 조직들은 이점을 다시 악용하여 공격을 통해 획득한 데이터를 다크웹(DarkWeb) 같은 블랙 마켓에 유통하고, 이를 2차 협박 수단으로 활용하고 있다.

국내 보안 기업인 NSHC는 랜섬웨어 해커 조직을 추적하고, 이들이 지금까지 600여 곳의 피해기업으로부터 훔친 각종 데이터를 다크웹에 공개했다고 언론 보도했다. 해당

조직은 훔친 데이터 중 일부만 먼저 공개하고, 이후 더 많은 파일을 유출하겠다고 협박하여 피해 기업으로부터 금전적인 이득을 취하고 있다. 또한, 해당 기업의 데이터가 유출된 사실을 언론사에 전달해 피해기업에 더 큰 비용을 지급하도록 압박하는 것으로 드러났다. 정보통신서비스 사업자의 경우에는, 개인정보 유출, 해킹 등 침해 사고 발생 시 한국인터넷진흥원(KISA) 같은 전문기관에 신속히 신고하고 공동으로 대응하게 되어 있다.

그렇다면 OT 기업이 랜섬웨어로부터 피해를 막으려면 어디서부터 대비해야 하는가에 대해 살펴보자. 랜섬웨어는 기본적으로 데이터를 인질로 보상을 요구하기 때문에, 접근제어나 이메일 필터 등 대비가 필요하고, 기술적 조치가 불가능하다면 주기적인 백업도 좋은 방안이다. 재해복구시스템을 별도로 구축하고, 사고로부터 얼마나 빨리 시스템을 정상화할 수 있는가를 나타내는 시스템 복원력(Resilience)을 높일 수 있다면 손실을 최소화할 수 있다.

또한, 스마트폰, IoT 기기 등 엔드포인트가 늘어나고, 누구나 작업에 USB를 사용하며, 스마트폰 테더링으로 어디서든 외부와 연결하는 현실을 고려하면, 폐쇄망이라고 해서 모두 안전할 것이라는 장담은 금물이다. Shodan.io 같은 인터넷 스캐닝 서비스를 이용하면 외부에 노출된 시스템을 몇 번의 클릭만으로 찾아낼 수 있기 때문에, 개개인의 보안 인식 강화와 더불어 조직 차원의 철저한 연결 관리도 필요하다.



〈자료〉 "GLOBAL ICS & IIOT RISK REPORT", CyberX, 2019, p.2.

[그림 4] GLOBAL IOT/ICS RISK

하지만 OT 현장의 보안 현실은 아직 해야 할 일이 많다. 2019년 미국 CyberX의 조사에 따르면, 조사의 50% 이상이 바이러스 백신이나 보안 업데이트를 하지 않고 있으며, 인터넷과 분리된 OT 네트워크를 사용 중이나, 조사의 40%에서 인터넷 연결이 탐지되었다. 시스템 비밀번호를 암호화하지 않고, 평문으로 보관하는 경우는 69%나 되었다([그림 4] 참고).

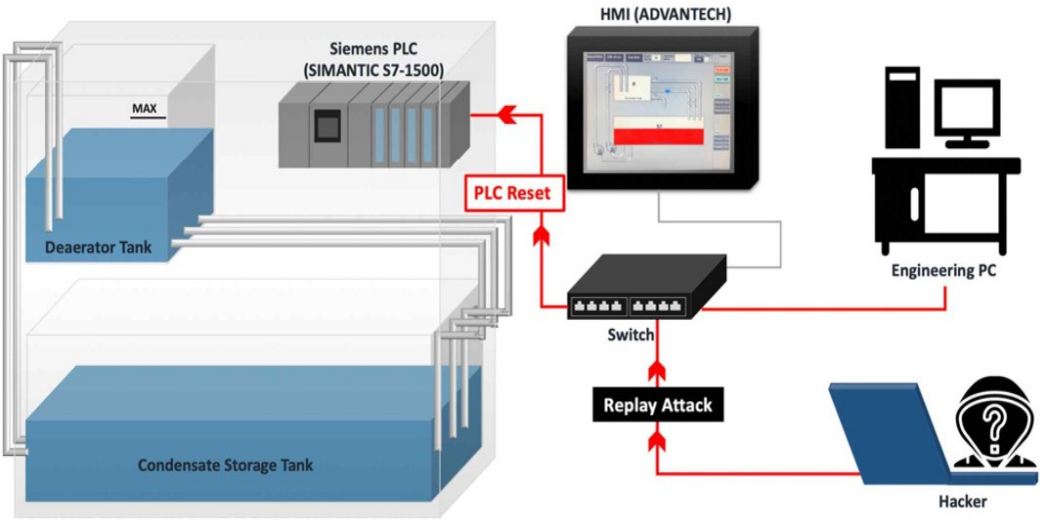
OT 보안의 중요성에는 누구나 공감하지만, 이처럼 IT와는 다른 OT만의 특성 때문에 보안을 적용하기가 쉽지 않은 측면도 있다. 최우선으로 OT는 시스템의 고(高)가용성, 즉 중단되지 않고 지속해서 운영되는 것이 매우 중요하다. 따라서 시스템을 일시 중단시켜야 하는 업데이트나 보안 패치를 적용하기가 어렵다. 또한, 도입된 장비의 생명주기가 길어 한 번 설치된 장비는 별다른 수정 없이 수십 년간 운영되기도 하고, 심지어 운영 중간에 장비 제조업체가 사라지는 예도 있다. 보안성보다 생산성이 중시되는 특성 때문에, 기존 시스템에 영향을 덜 주면서도 보안을 강화할 수 있는 즉, OT에 특화된 보안 기술의 연구개발이 중요하다([그림 5] 참고).

ICS 통신 프로토콜은 공장 자동화가 이루어진 오랜 시간 동안 내부 공정의 장비들이 효율적으로, 그리고 실시간 통신하는 것을 목표로 발전해 왔다. 그에 따라 특별한 보안 기능을 탑재하지 않고 벤더(Vendor) 자체적인 프로토콜을 개발하거나 여러 개의 산업표

Security Topic	Office IT Systems	IACS Systems
Antivirus	Widely used and easily updated	complicated and often impossible to implement
Life Cycle	3-5 Years	5-20 Years
Awareness	Good	Not good
Patch Management	Often	Rare, approval from Plant manufacturers
Change Management	Regular and scheduled	Rare
Evaluation of log files	Established practice	Unusual practice
Time Dependency	Delays Accepted	Critical
Availability	Not always available, failures accepted	24*7
IT Security Awareness	Good	Poor
Security tests	Widespread	Rare and problematic
Testing environment	Available	Rarely available

〈자료〉 "Whitepaper Industrial Security based on IEC 62443", TUV NORD GROUP, Version 1.0, p.4.

[그림 5] Office IT와 OT(IACS) 보안의 차이점



〈자료〉 "0-DAY RESEARCH TARGETING ICS/SCADA SYSTEM BY RED ALERT", NSHC Security, 2020, p.23.

[그림 6] Siemens PLC 프로토콜 취약점 개요도

준이 혼재되어 활용되고 있다. OPC-UA와 같이 일부 보안 기능을 포함하고 상호운용성을 보장하는 프로토콜도 있으나 OT 환경의 특성상 적용이 활성화되기까지는 시간이 필요하다. 최근에는 각 Fieldbus 직렬통신 및 산업용 이더넷 프로토콜에 보안 기능을 추가하고. ICS 상의 이상 징후를 진단하기 위한 연구도 활발히 진행 중이며, 블랙박스(Black-box) 테스팅과 같이 대상 기기 정보가 없이도 분석이 가능한 기술은 OT 환경에 적합하다.

블랙박스 테스팅이란 기기에 대한 정보나 소스코드 없이 오로지 입력값과 결과값만으로 분석하는 방법으로, 대상의 내부를 들여다보며 분석하는 화이트박스 테스팅과 구별된다. "퍼즈 테스팅(Fuzz Testing) 또는 퍼징(Fuzzing)"이라 불리는 분석 기술이 대표적이며, 대상에 순차적인 입력값을 전송하여 비정상적인 응답이나 충돌을 유발하고, 이를 통해 알려지지 않은 에러, 버그 그리고 새로운 취약점을 탐지할 수 있다. 그리고 Fuzzing과 같은 분석 기술을 기반으로 검사를 자동화하는 것은 분석 결과의 품질을 고르게 유지하고 다양한 기기를 효율적으로 검증할 수 있기에 중요하다.

네트워크 프로토콜 Fuzzing을 통한 보안 취약점 발견 사례를 보면, 2019년 우리나라(한국원자력연구원과 NSHC)와 이스라엘 텔아비브 대학 연구팀이 각각 독일 지멘스사 PLC에서 사용 중인 S7 통신 프로토콜의 취약점을 Fuzzing 기술로 밝혀냈다. S7 프로토

콜이 보안에 취약했던 이유는 지멘스 PLC와 통신하는 포털 사이트가 한 방향으로만 인증 기능을 제공했기 때문인데, 엔지니어링 PC와 PLC의 중간에 위치한 공격자의 리플레이(Replay) 공격에 대한 취약성이 밝혀진 것이다([그림 6] 참고). 이를 분석한 연구팀은 해당 보안 취약점이 보완되도록 조치하고 연구결과를 외부에 공개한 바 있다.

Ⅳ. 결론 및 시사점

우리는 OT/ICS를 노리는 많은 사이버 공격이 시도되고 있으며, 물리적인 피해가 함께 발생할 수 있어 더욱 주의가 필요하다는 사실을 알았다. 현재 IT 보안 전문가는 OT 용어와 기술에 익숙하지 않고, OT 영역에서는 사이버 보안에 대한 인식이 미흡한 상황이지만, OT 보안의 중요성을 고려해 볼 때 각자 영역의 간극을 좁혀 나갈 필요가 있다. “보안은 제품 하나가 아니라, 전체 프로세스(Security is a process, not a product)”라는 ‘Bruce Schneier’의 말처럼, 설계 단계에서부터 대비하지 않는다면, OT 보안은 사상누각(沙上樓閣)일 수밖에 없다[11].

그동안 ICS 공격에 성공한 해커들은 과거의 템플릿을 참조하며, 2차 공격을 위한 첩보를 수행하고 맞춤형 공격으로 진화하고 있으므로, 관련 보안 기술의 신속한 연구 개발을 통해 대응해야 한다. 비단 OT 분야뿐만 아니라, 의료 IT와 같은 융합 산업도 비슷한 상황으로, 민감한 개인정보를 담고 있는 데이터를 암호화하지 않고 저장하거나 사용자 인증, 접근제어가 부실한 시스템 사례가 보고되고 있어 염려스럽다[12].

향후에는 국제적인 표준화가 진행되는 ISA/IEC 62443 같은 산업제어시스템에 대한 보안 요구사항과 국내 KS 표준 등 구체적인 제도가 마련되면, 본격적으로 OT 보안에 대한 지침이 마련될 것으로 판단한다. 2020년 1월, 데이터 3법의 강화된 개정안이 국회를 통과하였다. 따라서 개인정보 관리자는 데이터 유출 방지에도 더욱 신경을 써야 할 것이다.

[참고문헌]

[1] Eric Byres, “The Future of Critical Infrastructure Security,” Byres Security Inc. 2011, p.18.
[2] “Analysis of the Cyber Attack on the Ukrainian Power Grid,” E-ISAC SANS, 2016, p.5.

[3] “CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations,” DRAGOS, 2017, p.12.
[4] TechCrunch.com, “Aluminum manufacturing giant Norsk Hydro shut down by ransomware,” 2019. 3. 19.
[5] SecurityBoulevard.com, “The Norsk Hydro ransomware attack: An in-depth look,” 2019. 3. 20.
[6] “Targeted attacks on industrial companies using Snake ransomware,” Kaspersky ICS CERT, June 2020, p.1.
[7] “Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT,” FireEye Threat Research, 2020, p.3.
[8] CyberX-labs.com, “New CyberX Global ICS & IIoT Risk Report: ICS Networks Are Soft Targets,” 2018. 10. 30.
[9] “Whitepaper Industrial Security based on IEC 62443,” TUV NORD GROUP, Version 1.0, p.4.
[10] “0-DAY RESEARCH TARGETING ICS/SCADA SYSTEM BY RED ALERT,” NSHC Security, 2020, p.23.
[11] Schneier on Security, “The Process of Security,” 2000. 4.
[12] “Confidential patient data freely accessible on the internet,” Greenbone, 2019, p.3.

chapter 2

무인기의 안전한 운영을 위한 보안 기술

왕기철 ‖ 한국전자통신연구원 책임연구원
이병선 ‖ 한국전자통신연구원 실장
김성창 ‖ 한국전자통신연구원 실장

I. 서론

드론이라 불리는 무인기(Unmanned Aerial Vehicle)는 파일럿 없이 자율적으로 비행하거나 파일럿이 원격으로 조종하여 비행하면서 탑재된 임무장비를 통해 임무를 수행하는 비행체를 의미한다. 원래 무인기는 군에서 감시정찰, 관심지역의 조사 및 촬영, 정밀 타격 등의 용도로 사용되어 왔다. 최근에는 무인 배달, 3차원 공간지도 작성, 임무장비를 이용한 과학 조사 활동, 정밀 농임업, 정밀 수산업, 재난 예측 및 대응 등과 같은 다양한 민간 응용들에 활용되고 있다.

무인기들을 일반공역에 진입시켜 다양한 응용에 활용하기 위해서는 다음과 같은 핵심기술들이 성숙되어야 한다. 먼저, 통신 및 보안기술로, 이는 무인기와 조종기 및 무인기 간에 데이터를 신뢰성 있게 교환하기 위한 기술이다. 탐지 및 인식 기술은 무인기가 가진 센서를 통해 무인기의 외부 환경을 인식하는 기술을 의미한다. 자율비행 기술은 무인기의 임무

* 본 내용은 왕기철 책임연구원(☎ 062-970-6531, gcwang@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
** 본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 5G 드론 시스템 및 원격운영시스템 개발사업의 연구결과임(NRF-2020M3C1C2A01080836).

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락

를 수행하기 위한 비행경로 계획을 세워 비행하되 실시간으로 바뀌는 환경을 인식하여 비행경로를 동적으로 변경하는 기술이다. 무인기의 비행시간을 증대시킬 수 있는 무인기 동력원의 기술 개발 또한 매우 중요하다. 안티 드론 기술은 보호 구역에 난입하는 무인기를 실시간으로 인식하고 추적하여 파괴적 혹은 비파괴적으로 대응하는 기술이다. 비행제어 기술은 숙련된 조종사의 조종 행위를 모사하는 고난이도 비행 모사와 외부 환경 변화에 강인하게 대응하는 적응형 제어 기술이다. 자율 착륙 기술은 무인기가 탑재된 센서에 기반하여 착륙 지점을 자율적으로 선정하고 자율무인차량, 자율무인선박 등에 안전하게 착륙하는 기술이다[1]. [표 1]은 위에서 언급한 핵심 기술들을 표로 정리한 것이다.

[표 1] 무인기의 활용을 위한 핵심 기술

분류	설명
통신 및 보안 기술	무인기와 조종기 및 무인기 간에 데이터를 안전하고 신뢰성 있게 교환
탐지 및 인식 기술	센서를 통해 무인기의 외부 환경을 인식
자율비행 기술	비행경로 계획을 세워 비행하되 실시간으로 바뀌는 환경을 인식하여 비행경로를 동적으로 변경
동력원 기술	무인기에 적합하면서 임무 수행 시간을 증대시킬 수 있는 동력원
안티 드론 기술	보호 구역에 난입하는 무인기를 실시간으로 인식하고 추적하여 파괴적 혹은 비파괴적으로 대응
비행제어 기술	숙련된 조종사의 조종 행위를 모사하는 고난이도 비행 모사와 외부 환경 변화에 강인한 적응형 제어
자율착륙 기술	탑재된 센서에 기반하여 착륙 지점을 자율적으로 선정하고 자율무인차량, 자율무인선박 등에 안전하게 착륙

〈자료〉 한국전자통신연구원 자체 작성

본 고에서는 위에서 언급한 다양한 무인기 핵심 기술들 중에서 무인기 운영의 신뢰성과 안전성을 담보하는 보안 기술을 다룬다. 먼저 무인기 시스템의 구성 요소들을 살펴보고, 무인기 시스템의 구성 요소에 따른 보안 취약점을 소개한다. 다음으로 식별된 무인기의 보안 취약점을 이용한 공격 방법들을 자세히 설명한다. 마지막으로 앞에서 설명한 공격 방법들에 대한 알려진 대응 방안들을 제시한다.

II. 무인기 시스템 및 보안 취약점

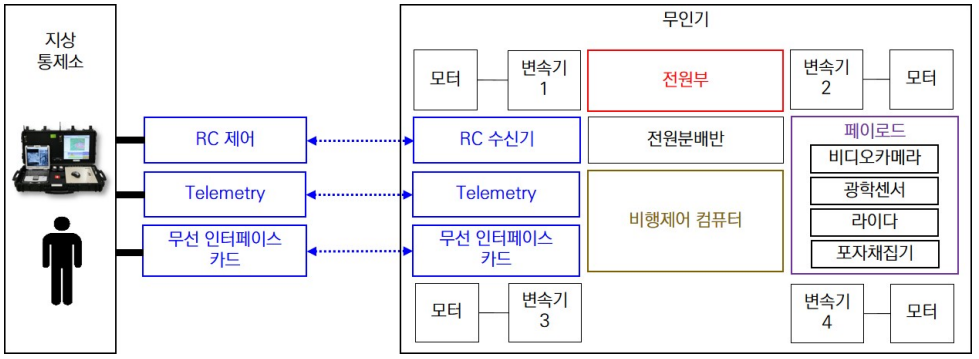
1. 무인기 시스템

일반적으로 무인기 시스템은 무인기 기체, 무인기를 제어하고 그 상태를 감시하는 지상통제소, 그리고 무인기 기체와 지상통제소 간의 데이터 통신 링크로 구성된다[2].

무인기 기체는 무인기의 두뇌인 비행제어 컴퓨터(Flight Control Computer: FCC), 각 부품에 전원을 공급하는 전원부, 전원을 각 부품에 분배하는 분배반, 그리고 지상통제소와 통신을 수행하는 통신부, 무인기를 비행하게 하는 구동부, 무인기의 임무 수행을 위한 페이로드(payload)로 구성된다. 비행제어 컴퓨터는 무인기의 자세를 측정하는 자세 및 방위기준시스템(Attitude and Heading Reference System: AHRS), 위치를 측정하는 GNSS(Global Navigation Satellite System) 수신기, 고도를 측정하는 고도계(Barometer/Altimeter) 센서 등으로 구성된다. 비행제어 컴퓨터는 지상통제소로부터 전달받은 조종 명령어 혹은 자동비행경로를 위치 및 자세 추정값과 비교하고, 그 차이를 모터의 회전속도로 바꿔서 구동부에 전달한다. 구동부는 비행제어 컴퓨터로부터 받은 신호에 따라 모터를 회전시키는 작업을 수행하며, 이를 위해 모터, 프로펠러, 변속기(Electronic Speed Controller: ESC)를 가진다. 통신부는 지상통제소의 조종기로부터 조종 명령어를 수신하는 RC(Remote Control) 수신기, 무인기의 위치, 자세, 속도, 전원 잔량 정보를 지상으로 송신하는 텔레메트리(telemetry) 송신기, 직접 혹은 네트워크형 통신을 수행하기 위한 인터페이스 카드 등으로 구성된다. 페이로드는 다양한 영상 센서들, 라이다(lidar), 합성개구 레이더(Synthetic Aperture Radar: SAR), 포자채집기, 가스분석기, 농약살포기 그리고 이들의 흔들림을 방지하기 위한 짐벌장치 등으로 구성된다.

지상통제소는 무인기를 원거리에서 조종하기 위한 원격 조종기, 무인기로부터 수신된 텔레메트리 정보를 수신하기 위한 텔레메트리 수신기, 무인기로부터 직접 혹은 네트워크형 통신을 통해 데이터를 수신하기 위한 인터페이스 카드와 데이터를 처리하고 시각적으로 표현하기 위한 정보처리 및 도식장치로 구성된다.

통신 링크는 무인기와 지상통제소 사이에서 데이터를 전달하기 위한 통로로서 조종 신호를 전달하기 위한 통신은 2.4GHz와 같은 ISM(Industrial Scientific and Medical)



〈자료〉 한국전자통신연구원 자체 작성

[그림 1] 무인기 시스템의 구성

대역을 주로 사용한다. 무인기의 위치, 자세, 속도, 전원 잔량 정보를 수신하기 위한 텔레메트리 통신은 433MHz나 900MHz 대역을 사용하며, 직접 통신 혹은 네트워크형 통신은 WiFi, LTE, 5G 등의 기술이 사용된다. [그림 1]은 무인기 시스템의 구성요소를 도식화한다.

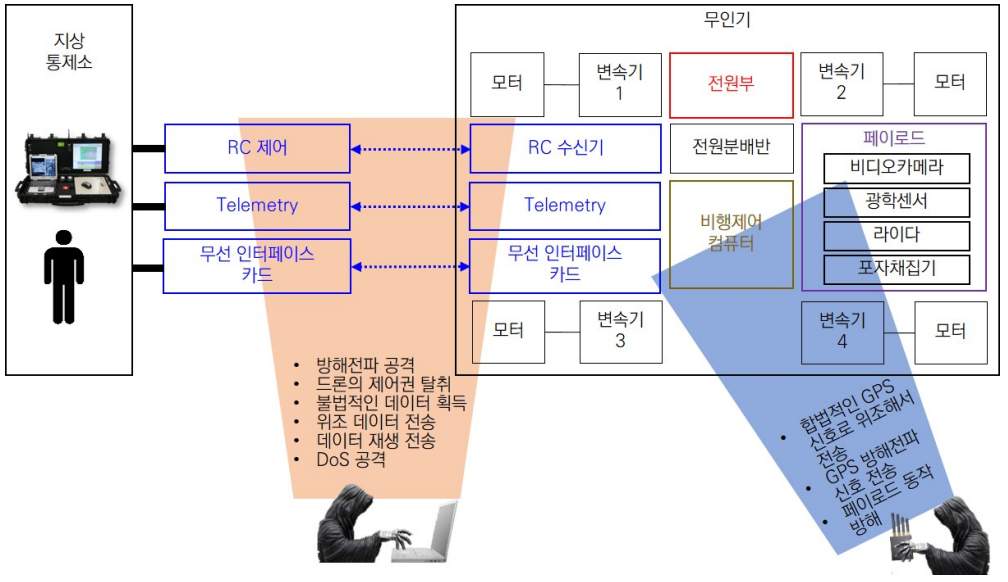
2. 무인기 시스템의 보안 취약점

무인기 시스템이 처한 보안 위협은 무인기와 지상통제소 간의 통신에 가해지는 보안 위협, 무인기의 비행제어 컴퓨터 내에 있는 센서들에 가해지는 보안 위협, 그리고 무인기의 페이로드에 가해지는 보안 위협으로 나눌 수 있다.

첫 번째, 무인기와 지상통제소 간의 통신은 공격자의 방해 전파에 의해 아예 신호 전송이 어려워지거나 신호 전송이 가능하더라도 제어권 분실, 도청, 전송 데이터 위조, 데이터 전송 부인, DoS(Denial of Service) 공격과 같은 보안 위협이 존재한다.

두 번째, 무인기의 비행제어 컴퓨터 내에 존재하는 자이로스코프, 가속도계, 전자 나침반, 고도계 등은 무인기의 3축 각속도 및 가속도, 진북 정보, 자세 정보, 고도 정보 그리고 이들을 보조하기 위한 정보를 제공하는데, 이 정보들이 오염되는 경우에는 무인기의 구동에 오동작이 발생하여 정상적인 비행이 어렵다.

세 번째, GNSS 수신기는 인공위성으로부터 발사된 전파를 수신하여 무인기의 위치를 결정하는데, 이 수신기의 동작을 방해하는 간섭 신호 혹은 위조 신호를 전송하여 무인기에



〈자료〉 한국전자통신연구원 자체 작성

[그림 2] 무인기 시스템의 보안 위협

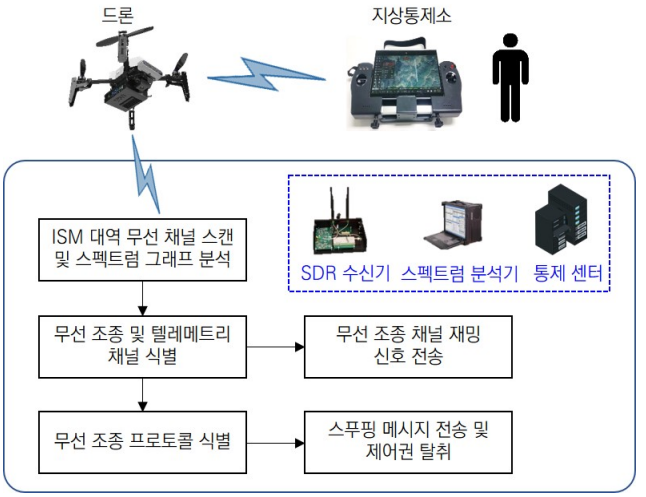
게 할당된 비행경로를 이탈할 수 있는 보안 위협이 존재한다.

네 번째, 무인기는 자신의 임무를 수행하기 위해서 비디오카메라, 광학 센서, 라이다, 포자채집기, 농약살포기 등의 장비들을 싣고 비행하는데, 이 장비들이 오작동 혹은 파손되는 경우에는 임무 수행이 불가능하게 된다. [그림 2]는 무인기 시스템의 보안 위협을 보여준다.

III. 무인기 시스템에 대한 공격 및 대응 방안

1. 무인기 시스템에 대한 공격

무인기와 지상통제소 간의 통신은 무인기와 지상통제소가 일대일로 직접 통신하는 방법과 5G와 같은 지상의 이동 통신망을 이용하여 일대다로 통신하는 방법으로 나뉜다. 일대일로 직접 통신하는 방법에서 공격자는 무인기 조종 신호에 강한 간섭을 발생시켜 출발지로의 복귀를 유도하거나 위조된 무인기 조종 신호를 전송하여 자신이 원하는 곳으로 무인

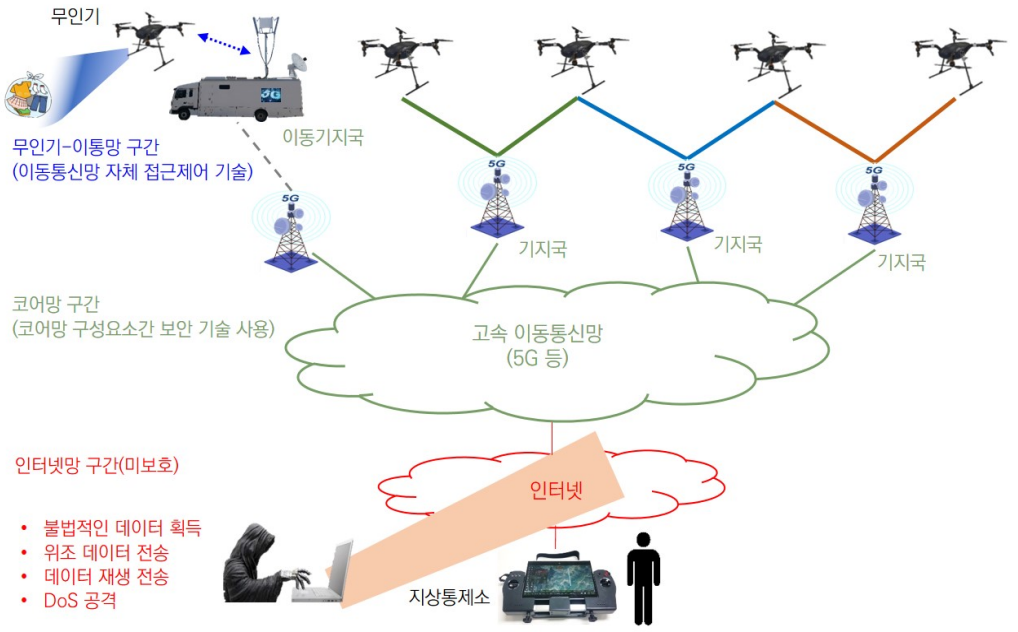


〈자료〉 한국전자통신연구원 자체 작성

[그림 3] 무인기-지상통제소 간 직접 통신에서의 공격

기를 이동시킬 수도 있다. 대부분의 무인기 조종 신호는 433MHz, 2.4GHz, 5GHz와 같은 ISM 대역에서 동작하고, 이 대역에서 동작하는 무인기 조종 프로토콜들은 잘 알려져 있기 때문에, 공격자들이 이러한 공격들을 쉽게 감행할 수 있다[3]. 즉, 공격자는 ISM 대역에서 방송되는 신호를 스캔하여 스펙트럼 그래프를 분석하고 무인기의 조종 채널과 텔레메트리 채널을 식별한다. 이후에 공격자는 식별된 채널에 강한 재밍(jamming) 신호를 전송하고, 무인기는 더 이상 지상통제소와 통신이 불가하므로 출발지로 복귀하게 된다. 또한, 공격자가 무인기의 조종 채널을 분석하여 어떤 조종 프로토콜이 사용되는지 파악하면, 프로토콜의 조종 메시지를 위조하여 무인기의 조종 제어권을 불법으로 획득할 수 있다[3]. [그림 3]은 무인기와 지상통제소 간의 직접 통신을 사용하는 경우의 통신 링크 공격을 보여준다.

지상통제소가 여러 무인기를 동시에 운용하는 경우에는 5G와 같은 고속의 지상 이동통신 네트워크를 사용하는데, 이 통신 방법은 무인기와 지상통제소 사이에 [그림 4]와 같이 세 개의 통신 구간으로 구성된다. 첫째, 무인기-이동통신망 구간은 이동통신망 사업자가 단말의 이동통신망 접근을 제어하는 자체 프로토콜에 의해 보호가 된다. 다음으로, 이동통신망의 코어망 구간은 코어망의 구성 요소들 간에 IPSec(IP Security)과 같은 종단 보안 프로토콜을 적용하여 보호가 가능하다[4]. 마지막으로, 네트워크형 통신의 경우에 지상통제소는 인터넷과 같은 공용망을 통해 이동통신망에 연결되고, 결국은 무인기와 연결되는

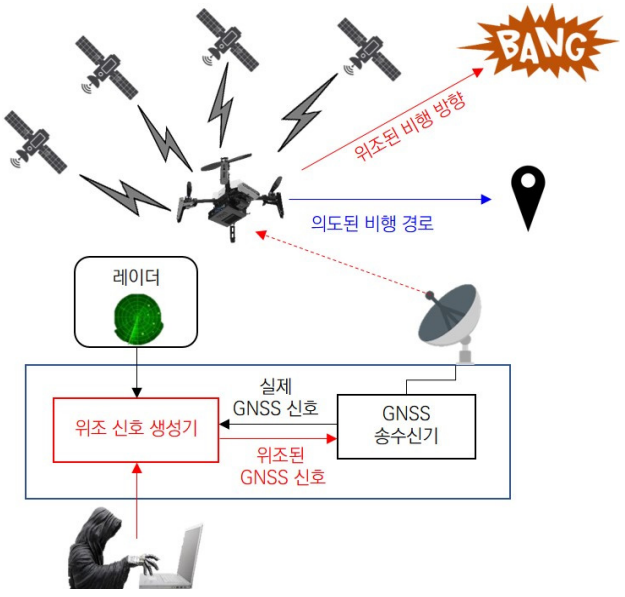


〈자료〉 한국전자통신연구원 자체 작성

[그림 4] 네트워크형 통신 방식에서의 공격

구조를 가진다. 공용망에서 무인기와 지상통제소 간에 통신 보호장치가 없으면, 공격자는 무인기와 지상통제소 간의 통신 내용을 불법으로 도청하여 위조된 데이터의 전송, 세션 탈취, 서비스 거부 공격 등을 수행할 수 있다.

공격자에게 있어서 무인기 자체도 좋은 공격 대상이 되는데, 특히 비행제어 컴퓨터와 모터 변속기(ESC) 등이 주요한 공격 목표가 된다. 비행제어 컴퓨터의 자이로스코프는 무인기의 3축 각속도를 측정하는데, MEMS(Micro-Electro-Mechanical Systems) 기반의 취약한 각속도계는 소음에 의해 오동작하며 정상적인 비행이 불가한 문제를 발생시킨다[5]. 또한, GNSS 수신기는 4개의 위성으로부터 수신된 신호의 거리 측정을 통해 수신기(무인기)의 위치를 측정하는데, 공격자는 같은 주파수 대역의 강력한 재밍 신호를 전송하여 무인기의 GNSS 신호 수신을 막을 수 있다. [그림 5]에서처럼, 공격자는 위조된 GNSS 신호를 발생시켜 무인기가 잘못된 방향으로 비행하게 할 수있다[6],[7]. 임의의 악의적인 공격자는 EMP(Electromagnetic Pulse) 신호 혹은 마이크로파를 비행 중인 무인기에 발사하여 무인기의 비행제어 컴퓨터의 전자회로를 교란시킬 수 있다. 이 경우에 무인기는



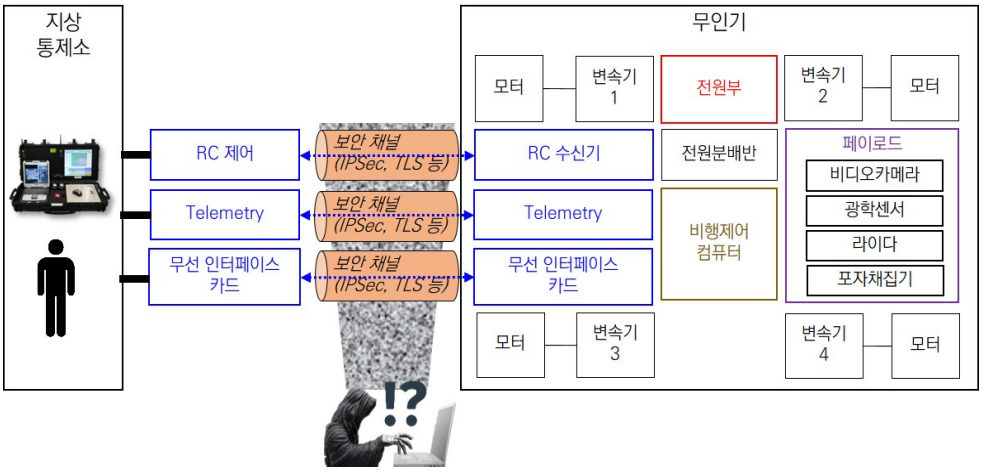
〈자료〉 한국전자통신연구원 자체 작성

[그림 5] 무인기의 GNSS 스푸핑 공격

정상비행을 수행할 수 없으며, 심지어 일부 전자회로가 파괴되어 추락할 수 있다.

2. 무인기에 대한 공격 대응

본 절에서는 3.1절에서 제시한 무인기를 목표로 하는 공격들에 대한 알려진 대응 방안들을 설명한다. 먼저, 무인기의 통신 링크에 대한 공격들에 방어하기 위해서는 무인기와 지상통제소 간에 IPSec이나 TLS(Transport Layer Security)와 같은 종단 보안 채널을 생성해야 한다. 보안 채널의 형성을 위해서는 통신 모뎀 앞단에 데이터 암복호화 하드웨어를 배치해서 채널 암호화를 수행하는 방법이 있는데, 이 방법은 주로 군용 무인기 시스템에서 주로 사용한다. 다른 방법은 무인기와 지상통제소 사이에 보안 터널을 생성하여 무인기와 지상통제소 간에 교환되는 데이터를 보호하는 방법이다[4]. 이 방법은 무인기가 지상통제소와 지상 이동통신망 및 공용망을 통해 연결될 때 주로 사용하는 방법이다[4]. 무인기와 지상통제소 간에 보안 터널을 생성하는 일반적인 절차는 다음과 같다. 먼저, 무인기와 지상통제소 간에 상호 인증을 수행하고, 상호 인증이 종료되면 암호 통신을 수행하기

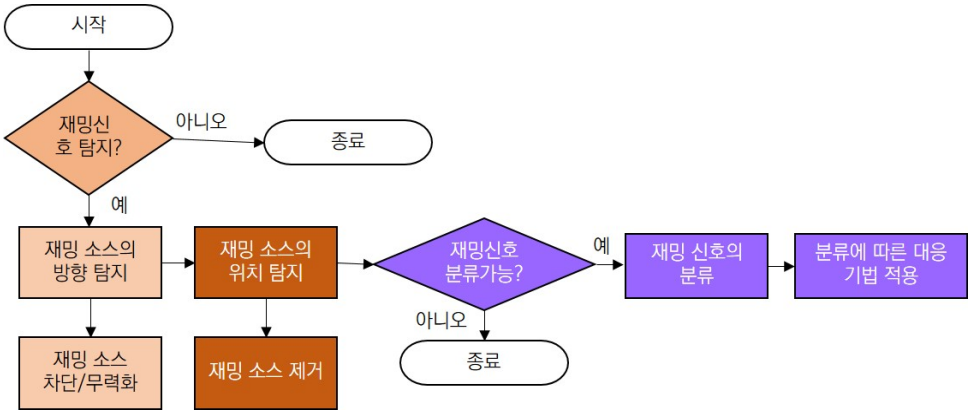


〈자료〉 한국전자통신연구원 자체 작성

[그림 6] 무인기 시스템의 통신 링크 보안

위한 통신키를 설정한다. 이후에 무인기와 지상통제소는 설정된 통신키와 암복호화 알고리즘을 이용하여 상호간 통신의 기밀성, 무결성, 최신성, 부인봉쇄를 보장한다. 무인기와 지상통제소는 상호간 통신의 보안성 강화를 위해서 주기적으로 새로운 키를 수립하여 공유한다. [그림 6]은 무인기 시스템의 통신 링크 보안 방안을 보여준다.

무인기의 GNSS 수신기에 대한 공격 대응은 GNSS 재밍 신호에 대한 대응 방안과 스푸

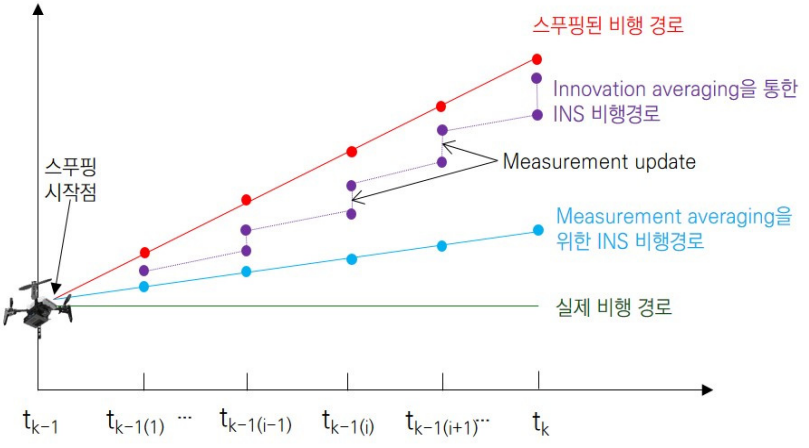


〈자료〉 R. M. Ferre, P. Richter, E. Falletti, A. D. Fuente, "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft," IEEE Communications Surveys and Tutorials, Vol.22, No.1, First quarter 2020, pp.249-291.

[그림 7] GNSS 재밍 공격에 대한 대응

핑(spoofing)된 GNSS 신호에 대한 대응 방안으로 구분된다. GNSS 재밍 공격을 탐지하기 위해서는 재밍 반송파 주파수 및 대역 파라미터들을 이용하여 재밍 신호들을 수학적으로 모델링하고, 이 모델들과 거의 일치하는 신호가 수신되면 GNSS 재밍을 당하고 있음을 인지한다. 이 경우에, 재밍 신호의 방향을 탐지할 수 있고 방해 전파를 송출할 수 있는 장비가 있다면, 해당 방향으로 방해 전파를 전송하여 재밍 신호의 무력화를 시도한다. 만일, GNSS 재밍 신호의 방향을 식별할 수 없다면, 재밍 신호의 분류가 가능한지를 점검한다. GNSS 재밍 신호의 분류가 가능하면, GNSS 수신기의 구성 요소들(전단부, 선행연관부, 후행연관부, 항법부)에 대한 공격 위치에 따른 경감대책을 수립하여 적용한다[8]. [그림 7]은 GNSS 재밍 공격에 대한 대응 방안을 보여준다.

무인기에서 GNSS 스푸핑 탐지 방법은 클록 동기화 신호 기반의 방법과 칼만 필터(Kalman Filter) 기반의 방법으로 나뉜다. 무인기가 정상적인 클록 동기화 신호를 받을 때 가지는 클록의 편이(bias)와 표류(drift)를 모델링하여 시그니처로 저장한 후에, 실제 무인기의 비행에서 이와 유사한 시그니처를 가지는 동기화 신호만 받아들이는 방법이다. 무인기의 이동방향, 이동경로, 이동속도를 유지하는 관성측정장치(Inertial Measurement Unit)는 그 측정값을 관성항법시스템(Inertial Navigation System)에 되먹임시켜 무인기가 할당된 경로를 유지하게 한다. 칼만 필터는 측정값들을 시간을 두고 지속적으로 관찰



〈자료〉 Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System," IEEE Sensors Journal, Vol.19, No.13, Jul. 2019, pp.5167-5178.

[그림 8] Innovation averaging을 이용한 GNSS 스푸핑(spoofing) 탐지

하여 알려지지 않은 값들을 추정하게 되는데, 위치와 속도 오류, 자이로스코프의 편이, 무작위 소음 오류, 가속도계 변이 오류 등을 계산한다. 이러한 칼만 필터에 의한 오류값들을 충분히 긴 시간 동안 보정하였을때, GNSS 스푸핑에 의한 측정값에 근사하게 되어 스푸핑을 탐지할 수 있게 된다. 이 방법을 innovation averaging[9]이라 칭하는데, [그림 8]은 innovation averaging 기반의 GNSS 스푸핑 탐지 방법을 보여 준다. 무인기가 GNSS 스푸핑 공격을 받는 경우에, 여러 개의 GNSS 수신기를 이용하여 의심스런 신호를 배제할 수 있다. 또한, 라이다(lidar)와 같은 센서들을 이용하여 원래의 비행경로로 복귀를 시도할 수 있다. GNSS 스푸핑을 원천적으로 차단하기 위해서는 위성이 GNSS 신호를 보낼 때 개인키로 서명해서 보내고, 무인기는 위성의 공개키로 복호화가 되는 경우에만 GNSS 신호를 받아들이면 된다. 그러나, 이 방법은 군용 위성에서만 적용된다[6].

소음을 통해 무인기의 자이로스코프에 오동작을 유발시키는 공격에 대응하기 위해서는 다음과 같은 방법들을 사용할 수 있다[5]. 첫 번째, 자이로스코프 회로를 보호 차폐물 안에 넣어서 소음으로부터 보호할 수 있다. 다음으로, 추가적인 자이로스코프를 배치하여 공명 주파수에만 반응하도록 함으로써 원래의 자이로스코프 공명 출력을 제거할 수 있다. 또한, 자이로스코프의 감지 전극에 콘덴서를 추가로 배치하여 공명 효과를 감소시킬 수 있다.

IV. 결론

본 고에서는 하늘을 나는 IoT 장치로서 활용 분야를 크게 넓히고 있는 무인기 시스템의 보안 취약점들과 이 취약점들을 이용하여 수행되고 있는 다양한 공격들을 소개하였다. 이이서 앞서 소개된 다양한 공격들에 대응하기 위한 알려진 방법들을 또한 설명하였다. 필요한 시간에 장소를 변경하면서 대량의 데이터를 수집할 수 있는 무인기의 활용을 실생활에 더욱 확장하기 위해서는 무인기 비행의 안전성, 신뢰성, 그리고 수집 데이터의 보안성을 더욱 향상시켜야 한다. 이러한 측면에서, 무인기 시스템의 잠재된 보안 취약점을 선제적으로 파악하고, 이러한 취약점에 기반한 공격들을 효과적으로 방어하기 위한 보안 기술들이 개발되어야 한다.

[참고문헌]

[1] 왕기철, 이병선, 안재영, “무인기 자율비행 기술 동향,” 스마트 트렌드 디바이스 매거진, Vol.36, 2019. 10. 16, pp.18-23.

[2] 김성훈, 김준현, 손호웅, 이강원, “무인비행장치 측량,” 시그마프레스, 2019. 1. 31, ISBN: 9791162261392, pp.33-53.

[3] X. Yue, Y. Liu, J. Wang, H. Song, and H. Cao, “Software Defined Radio and Wireless Acoustic Networking for Amateur Drone Surveillance,” IEEE Communications Magazine, Vol.56, No.4, Apr. 2018, pp.90-97.

[4] 왕기철, 이병선, 임광재, 안재영, “무인기 제어용 네트워크의 보안 기술 동향”, 한국전자통신연구원, 전자통신동향분석, 32권, 1호, 2017. 2, pp.82-92.

[5] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors,” 24th USENIX Security Symposium, Washington, D.C., USA, Aug. 2015, pp.881-896.

[6] K. Wesson and T. Humphreys, “Hacking Drones,” Scientific American Online, Nov. 2013, pp.55-59.

[7] D. He, S. Chan, and M. Guizani, “Security in the Internet of Things Supported by Mobile Edge Computing,” IEEE Communications Magazine, Vol.56, No.8, Aug. 2018, pp.56-61.

[8] R. M. Ferre, P. Richter, E. Falletti, A. D. Fuente, “A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft,” IEEE Communications Surveys and Tutorials, Vol.22, No.1, First quarter 2020, pp.249-291.

[9] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, “Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System,” IEEE Sensors Journal, Vol.19, No.13, Jul. 2019, pp.5167-5178.

chapter 3-1

초저전력 뉴럴 스파이크 프로세서 SoC

이재진 ‖ 한국전자통신연구원 책임연구원

I. 결과물 개요

개발목표시기	2024. 12.	기술성숙도 (TRL)	개발 전	개발 후
			3	6
결과물 형태	HW-IP, HW-Chip, HW-Module	검증방법	자체검증, 3자검증, 시험인증, 품질보증	
Keywords	뉴럴 스파이크 프로세서, 스파이킹 뉴럴 네트워크, 지능형반도체, 생체인증, Neural Spike Processor, Spiking Neural Network, Intelligent SoC, Biometric Authentication			
외부기술요소	100% 개발기술	권리성	특허, HW-IP, 설계도	

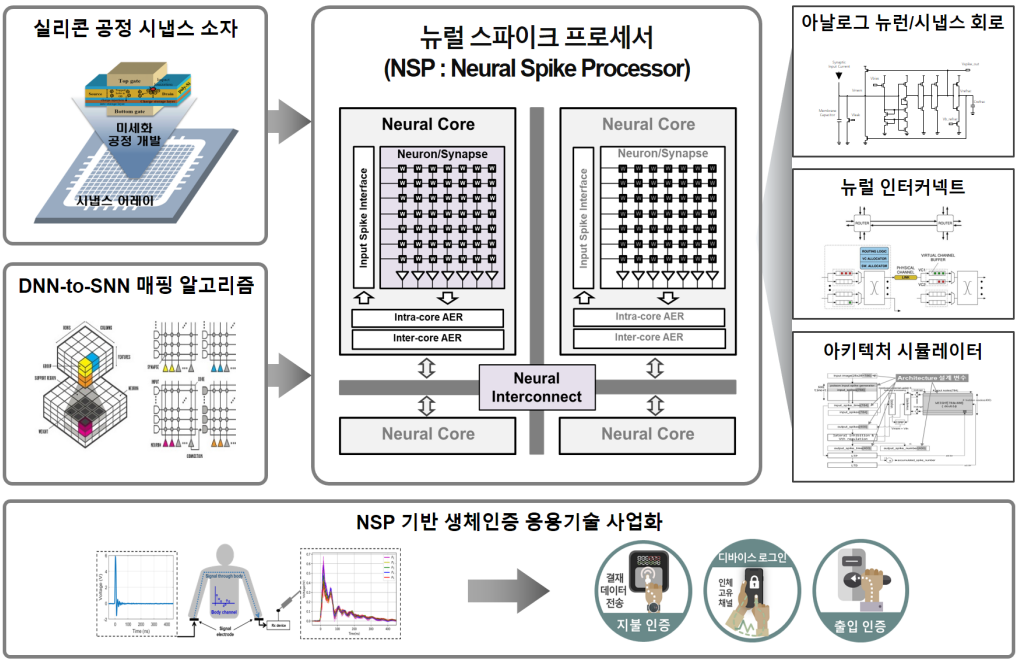
II. 기술의 개념 및 내용

➢ SNN 적용에 최적화된 AIoT 응용을 위한 엣지컴퓨팅 초저전력 인공지능 프로세서 IP 기술

- SNN 기반 뉴럴 스파이크 프로세서(Neural Spike Processor: NSP) 기술

* 본 내용은 이재진 책임연구원(☎ 042-860-1712, ceicarus@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락



[그림 1] 엣지컴퓨팅 초저전력 인공지능 프로세서 IP 개념도

III. 국내외 기술 동향 및 경쟁력

1. 기술의 특성 및 성능

➢ 뇌의 뉴런/시냅스 동작 모사 아날로그 NSP 코어(뉴런/시냅스) 회로설계 기술 및 이벤트 기반 저전력 뉴럴 인터커넥션 기술을 활용하여 AIoT에 응용 가능한 초저전력 에너지 고효율 인공지능 프로세서 기술

- 실리콘 기반 신소자 시냅스의 동작 모사를 위한 아날로그 시냅스 회로
- 고에너지 효율 달성이 가능한 초저전력 아날로그 뉴런 회로
- NSP 코어 간 스파이크 전송을 위한 재구성 가능 뉴럴 인터커넥션 기술
- 비동기 스파이크 sparse 입력 신호를 처리할 수 있는 NSP 아키텍처
- 아날로그 시냅스 고집적화를 위한 시냅스 가중치 근사화 기술

2. 경쟁기술/대체기술 동향 및 현황

- 빅데이터 및 인공지능 산업이 최근 급속히 확산되고 있는 가운데, 서버 단에서의 데이터 폭증 문제를 해결하기 위해서는 엣지 단에서 의미 있는 데이터만을 선별하여 서버로 전송하는 엣지컴퓨팅 방식을 통해 서버 단에 집중된 데이터를 분산해야 하므로, 이를 위한 핵심 기술인 엣지컴퓨팅 인공지능 프로세서에 관한 수요는 향후 지속적으로 성장할 것으로 예측됨
- 엣지컴퓨팅 인공지능 프로세서 구현을 위해서는 현재 인공지능에서의 가장 큰 문제로 꼽히는 대용량의 전력 문제를 해결해야 하며, 이를 위해 국내외 기업과 연구소를 중심으로 초저전력 인공지능 프로세서를 위한 새로운 아키텍처, 저전력 뉴런 모델 회로, 차세대 시냅스 회로 등에 관한 연구가 활발히 진행 중
- Intel사는 최초의 자가학습 뉴로모픽 칩인 Loihi를 자사의 14㎚ 공정기술로 제작하였는데, Loihi는 뇌의 기본 동작을 모방한 디지털 회로가 포함되어 기계 학습보다 빠르고 효율적으로 업무의 수행이 가능
  - Loihi는 1,024개의 인공 신경세포인 뉴런을 탑재한 128개의 코어로 구성되어 있으며 완전한 비동기식으로 작동하는 코어 메시를 통해 희소성 신경망, 계측정 신경망, 순환 신경망 토폴로지를 지원하며 온칩 학습 엔진을 탑재하여 교육 및 추론 기능을 단일 칩에 결합
- Brainchip사는 SNN 기반의 인공지능처리 칩셋인 Akida를 제작, 발표하였는데, Akida는 120만 개의 뉴런과 100억 개의 시냅스를 내장하고 있으며 주요 CNN 가속장치와 비슷한 수준의 정확도를 확보하였으며 인공지능 처리의 핵심 기능이 될 동적 신경망에 관한 기술을 통해 인공지능 프로세서가 처리하는데 필요한 컴퓨터 자원을 크게 감소시킴

3. 우수성 및 차별성

[표 1] SNN 기반 초저전력 인공지능 프로세서 기술 사업화의 SWOT 분석

S	초저전력 뉴럴 스파이크 프로세서	W	국내 팹리스 산업의 경쟁력 둔화
강점	- 생물학적 동작 모사 기반으로 SNN에 최적화된 아날로그 뉴런/시냅스 회로로 구성된 mW급의 초저전력 뉴럴 스파이크 프로세서 기술 - 초저전력 뉴럴 스파이크 프로세서가 적용된 위변조가 불가능한 세계 최초의 생체채널 기반 생체인증 디바이스 및 서비스 기술 - 엣지용 인공지능 프로세서 플랫폼 형태로 제공되는 초저전력 뉴럴 스파이크 프로세서이므로 팹리스 산업으로의 기술 확산이 용이함	약점	- 국내 팹리스 업체들은 SNN 기반의 프로세서 관련 원천기술이 미비하고 글로벌 기업들이 관련 기술을 주도하고 있어 독자적인 경쟁력 확보가 어려움 - 초저전력 뉴로모픽 프로세서 기술은 국내 업체들이 자체 개발 시 기술적 난이도, 시장 진입의 저항 및 생태계 확산 등의 문제점이 있음 - 국내 팹리스 업체들이 엣지용 인공지능 프로세서 기술을 자체적으로 개발하기에는 비용 및 인력 측면에서 영세한 측면이 있음
O	엣지컴퓨팅/생체인증 시장의 확대	T	글로벌 기업의 인공지능 기술 투자
기회	- 클라우드 컴퓨팅 환경의 단점을 극복하기 위해 최근 엣지컴퓨팅 기술발전 및 시장의 확대가 가속화되고 있음 - 엣지 인공지능 반도체 세계시장 규모는 2024년 1.67억 달러에서 2029년 18.4억 달러 규모로 고성장이 전망됨 - AI 기술이 다양한 산업 분야와 융합이 가속화되면서 AIoT와 같은 엣지용 초저전력 AI 프로세서의 필요성이 증대	위협	- 글로벌 기업(IBM, Intel, Qualcomm 등)에서 뉴로모픽 인공지능 반도체 기술 개발이 활발히 추진되고 있음 - 글로벌 기업들은 관련 오픈플랫폼 및 표준화를 주도하며 자신들에게 유리한 생태계를 확보하고 있어 시간이 갈수록 국내기업이 위축될 수 있음

4. 표준화 동향

- (TTA) ICT 융합디바이스반도체 PG에서 지능형반도체 및 지능형배터리 관련 주요 국내 표준들을 개발 중에 있음
- 인텔리전트 엣지 개방형 플랫폼 기술 관련해서는 ITU-T, ISO/IEC에서 관련 표준 개발이 활발히 이루어지고 있으며, 글로벌 표준기구인 IETF, IEEE, OGC, OMA, ETSI, oneM2M 등에서도 관련 표준들이 활발히 개발되고 있음
- 지능형반도체 관련 국제 표준화는 ISO/IEC/IEEE, OCP 등에서 관련 표준화를 진행중임

Ⅳ. 국내외 시장 동향 및 전망

1. 국내 시장 동향 및 전망

- 인텔리전트 엣지 적용 가능 IoT 산업은 IT 산업에서 가장 빠르게 성장하고 있는 분야로 반도체 시장규모는 2020년까지 4배 이상 연평균 40% 이상 고속 성장할 것으로 예측
- 경량 인공지능을 포함한 세계 인공지능 시장의 대부분은 제품시장이며 시장규모는 2015년 약 1,270억 달러에서 2017년 약 1,650억 달러로 연평균 14.0%의 고성장을 지속한 것으로 추정
- 2020년 클라우드 트래픽은 약 14 제타바이트에 이를 것으로 전망되며, 일부 제조업계에서는 클라우드 트래픽, 보안 문제 해결 및 지연을 최소화하기 위한 엣지 프로세싱 기술도입을 고려하고 있음
- 4차 산업혁명에 따른 IoT 관련 빅데이터 및 인공지능 산업 활성화로 향후 100조 개의 스마트 센서가 사용될 것으로 예측되며, 스마트 센서는 의미 있는 데이터만을 선별하여 클라우드로 전송하는 인텔리전트 엣지 형태로 진화할 것으로 전망

2.제품화 및 활용 분야

- 목표 제품: 뉴럴 스파이크 프로세서를 적용한 생체인증 제품
  - 생체인증 시장은 전통적 물리 보안시장에서 출입통제 인증을 기반으로 한 개별 디바이스를 중심으로 확장되고 있으며, 최근에는 생체인증 기술과 금융의 융합기술을 통한 핀테크 시장이 활성화됨에 따라 생체인증 시장은 더욱 확대될 것으로 예상
  - 최근 생체인증 시장 확대를 주도하고 있는 핀테크는 생체인증 핵심센서 + 알고리즘 + 핀테크 서비스 + 금융기관 등을 중심으로 한 B2B 시장 및 전통적 생체인증 출입통제 위주의 B2G, B2B 시장을 중심으로 시장을 형성
  - 개별 디바이스 위주의 제품으로 최근 몇 년 사이 중국의 가파른 추격으로 매출 및 이익이 빠른 속도로 중국 업체들에 의해 잠식당하고 있는 추세
  - 이에, 미래 성장을 견인할 수 있는 뉴럴 스파이크 프로세서 기반의 인공지능 복합생체인증 제품을 개발하여 세계최고의 보안성과 편의성을 갖춘 생체인증 개별 디

바이스 단품이 아닌 복합기능, 복합서비스를 제공하는 뉴로모픽 생체인증 스마트 기기를 개발하여 시장 선점 및 글로벌 히든 챔피언 기업으로의 성장이 목표

➢ 목표 서비스: 위변조 불가한 안전하고 편리한 복합 생체인증 서비스

- 현재 미국 연방정부의 LOGIN.GOV, 영국의 National Health Service, 한국의 디지털 원패스, 홍콩의 E-ID 사업 등이 모두 가장 안전한 인증의 방법으로 OS 및 브라우저에서 지원되면서 H/W 생체인증을 인증 수단으로 하는 FIDO 서비스가 시작
- 이에, 생체인증의 위변조를 뉴로모픽 인공지능 기술을 활용하여 인증을 강화시키는 복합생체인증 기술이 향후 주목받는 보안 인증 분야의 핵심기술로 부상될 가능성이 많음
- 스마트 기기 로그인부터 그룹웨어, 웹사이트 인증, IoT 인증, 자율주행 및 로봇 인증에 이르기까지 하나의 강력한 복합생체인증 기기로 서비스하는 사업모델

V. 기대효과

1. 기술도입으로 인한 경제적 효과

➢ 초저전력 뉴럴 스파이크 프로세서 기술은 엣지 디바이스에 지능을 부여함으로써 4차 산업혁명의 핵심인 데이터 수집/처리에 있어 엣지 디바이스를 이용한 신서비스를 다양한 산업으로 확산하여 국내 반도체 산업의 재도약에 크게 기여할 것으로 기대됨

➢ 엣지향 지능형반도체 세계 시장규모는 2024년 1.67억 달러 규모에서 2029년 18.4억 달러 규모로 연평균(CAGR) 61.6% 고성장이 전망되며, 2024년부터 6년 동안 3,314억 원의 매출효과 창출이 기대됨

2. 기술사업화로 인한 파급효과

➢ 4차 산업혁명 시대가 도래함에 따라 인공지능, IoT 등을 기반으로 하는 기술 혁신이 기업의 생존을 위한 핵심 요소로 부각되고 있는 가운데, 클라우드에서 포화된 빅데이

터 지능 처리 능력을 엣지로 분산하여 처리하는 패러다임의 변화와 이에 요구되는 엣지용 초저전력 인공지능 프로세서에 대한 시장 재편성이 예상되는 바, 본 과제를 통한 초저전력 인공지능 프로세서 원천기술 확보로 IoT 제품의 차별성 및 기술 경쟁력 제고가 기대됨

chapter 3-2

초고속 직렬 통신 인터페이스 IP

정덕균 ‖ 서울대학교 산학협력단 교수

I. 결과물 개요

개발목표시기	2023. 12.	기술성숙도 (TRL)	개발 전	개발 후
			4	6
결과물 형태	HW-IP	검증방법	자체검증, 공인시험기간을 통한 3자 검증	
Keywords	직렬인터페이스, 차세대 데이터 전송 표준, 다중 속도, Serial Interface, PCIe-Gen5, Multi-rate			
외부기술요소	100% 개발기술	권리성	HW-IP, 특허	

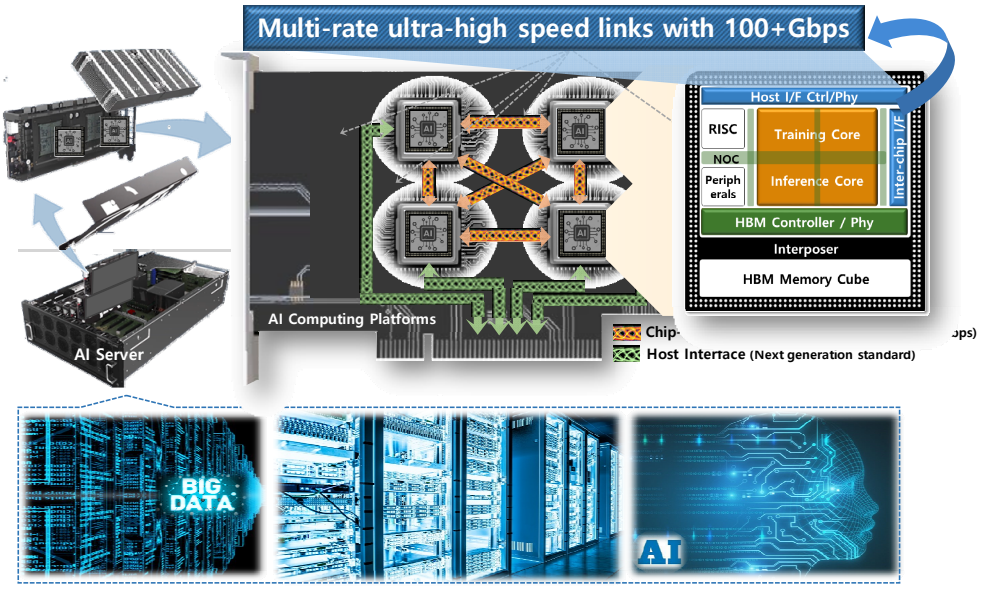
II. 기술의 개념 및 내용

1. 기술의 개념

➢ 4차 산업혁명의 핵심 기술인 빅데이터, 인공지능 등의 산업적 적용이 확대됨에 따라 고성능 인공지능 컴퓨팅 플랫폼 구현을 위한 인공지능 반도체의 중요성이 급격히 부상

* 본 내용은 정덕균 교수(☎ 02-880-7437, dkjeong@snu.ac.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함

OPEN 출처표시 상업용금지 공공누리 공공저작물 자유이용허락



[그림 1] 기술개념도

하고 있으며, 학습·추론 등 인공지능 구현에 요구되는 대용량 데이터 연산/처리를 위해 초고속 대용량 데이터 전송 기술이 요구

➢ 데이터 중심 고성능 인공지능 컴퓨팅 플랫폼의 반도체 칩 간 대용량 데이터 연산에 필요한 초고속(100Gbps 이상) 저지연 데이터 전송 기능과 높은 데이터 전송 에너지 효율을 가지고 차세대 데이터 전송 표준과 호환 가능한 직렬 인터페이스 기술을 개발

III. 국내외 기술 동향 및 경쟁력

1. 기술의 특성 및 성능

➢ 데이터 중심 고성능 인공지능 컴퓨팅 플랫폼의 칩 간 대용량 데이터 전송을 위한 차세대 데이터 전송 표준[1] 호환과 수 pJ/bit의 고에너지 효율을 갖는 100Gbps 이상의

1) PCIe-Express Gen-5 이상

초고속, Multi-rate, Multi-mode[2] 데이터 전송 가능 저전력 ML-Inspired[3] 초고속 직렬 인터페이스 기술

2. 경쟁기술/대체기술 동향 및 현황

➢ 100Gbps 이상의 초고속 직렬 데이터 인터페이스 IP 기술 및 제품은 현재 핀펫과 같은 초미세 공정을 사용한 제품이 주를 이루고 있으며, 초기 IP 개발 비용이 많이 소요되어 글로벌 기술 선도 기업들을 중심으로 차세대 기술/제품이 개발됨

기업	국가	설립	사업 분야	제품/기술 현황
SYNOPSYS	미국	1986	반도체 설계 Tool 및 IP	- 고속 SerDes IP 보유 기업이며 최근 미소 공정의 다양한 IP 제품군을 보유
cadence	미국	1988	반도체 설계 Tool 및 IP	- 고속 SerDes IP 보유 기업이며 최근 미소 공정의 다양한 IP 제품군을 보유
XILINX ALL PROGRAMMABLE.	미국	1984	Reconfigurable H/W FPGA	- FPGA 전문 기업으로 초고속 직렬 I/O IP 제품을 보유

3. 우수성 및 차별성

경쟁기술	본 기술의 우수성/차별성
High Speed SERDES IP	- 머신러닝 기술을 직렬 인터페이스에 최초 적용하여 고속 광대역 동작 주파수 범위에서 수 pJ/bit의 고효율 데이터 전송 가능 - 실시간 인공지능 컴퓨팅을 위한 레인당 대역폭 50Gb/s/lane 이상을 갖는 Chip-to-Chip 초고속/저지연 데이터 전송 - 범용성 높고 개별 사업화 가능한 차세대 데이터 전송 표준 호환

4. 표준화 및 특허

➢ 표준화 동향

- Peripheral Component Interconnect Special Interest Group(PCI-SIG)은 32Gb/s의 속도를 가지는 PCIe-Gen5 규격을 최근에 완성하였으며, 3~4년 안에

2) Multi-Mode: NRZ(Non Return to Zero) & PAM4(Pulse Amplitude Modulation-4)
3) Machine Learning-Inspired

해당 규격을 사용하는 제품이 개발될 것으로 예상되며, 향후 64Gb/s 속도를 가지는 PCIe-Gen6 데이터 전송 표준 규격 개발을 추진 중임

- 딥러닝용 GPGPU 및 하이엔드 서버 시장을 위한 성능 향상이 요구되는 현 시점에서 개인용 장비 PCIe-Gen4 공식 지원 이후 서버 장비의 PCIe-Gen5 도입 준비단계에 있음

IV. 국내외 시장 동향 및 전망

1. 국내 시장 동향 및 전망

➢ 인공지능 반도체는 학습·추론 등 인공지능 구현에 요구되는 대규모 데이터 처리를 위해 고성능·저전력 기술 중심으로 발전이 가속화되고 있음

➢ Google은 SW 및 빅데이터 기반 인터넷 전문 기업으로, 인공지능 기술을 활용한 신서비스의 수요가 증대되면서 자사의 데이터센터에 사용하기 위한 서버향 인공지능 병렬 프로세서 반도체를 직접 개발하기 시작

➢ 딥러닝 학습을 위한 병렬연산 처리 능력과 수요변화에 대응하기 위한 컴퓨팅 파워 구성의 확장성과 유연성, 운용비용 관점에서의 전력효율 등을 중심으로 시장이 형성

➢ CPU가 중앙에서 모든 데이터를 처리·제어하므로 연산량이 많아질수록 CPU와 메모리 사이 및 Chip-to-chip 병목현상이 발생하여 대규모 데이터를 처리할 경우 속도 저하 및 막대한 전력 소모가 발생하므로 초고속 직렬 인터페이스 IP가 필요

2.제품화 및 활용 분야

활용 분야(제품/서비스)	제품 및 활용분야 세부내용
High Speed SERDES IP 적용 SoC	- 인공지능 컴퓨팅 플랫폼의 칩 간 대용량 데이터 전송을 위한 통신 Link에 활용 - 차세대 데이터 전송 표준을 지원하는 Chip의 PCIe-Gen5 대응 가능한 IP로 활용

V. 기대효과

1. 기술도입으로 인한 경제적 효과

- 초고속 직렬 인터페이스는 시스템 반도체 분야에서 데이터 전송을 위해 폭넓게 사용되고 있으며, 서버용 시스템 반도체들 이외에도 컴퓨터, 하드웨어 가속기, 고성능 모바일 등 다양한 분야의 시스템 반도체 개발에 적용되어 국내 시스템 반도체 제품의 완성도를 제고하는데 기여할 수 있을 것으로 기대
- 직렬 인터페이스 IP는 시스템 반도체에 광범위하게 사용됨에도 불구하고, 초고속 대역용 IP는 주로 해외 선도사들의 제품을 구매해서 사용하는 실정이며, 본 과제를 통해 세계 최고 수준인 100Gb/s급 직렬 인터페이스 IP를 확보함으로써 기존 해외 수입 IP를 국산화하는 효과를 기대할 수 있음

2. 기술사업화로 인한 파급효과

- 하드웨어 시스템의 핵심부인 시스템 반도체들의 데이터 통신을 담당하는 직렬 인터페이스 설계 과제 수행은 관련 시스템 및 솔루션 분야의 산업 경쟁력을 강화하는 데에 결정적인 기여를 할 것으로 전망됨

- 사업책임자: 문형돈(기술정책단장)
- 과제책임자: 이성용(융합정책팀장)
- 참여연구원: 이재환, 이효은, 권요안, 김용균, 박주혁, 김우진, 김도현, 전영미(위촉)

주간기술동향

통권 1980호(2021-02)

발 행 년 월 일 : 2021년 1월 20일
발 행 소 : IITP 정보통신기획평가원
편집인겸 발행인 : 전성배
등 록 번 호 : 대전 다-01003
등 록 년 월 일 : 1985년 11월 4일
인 쇄 인 : ㈜승일미디어그룹

IITP 정보통신기획평가원

(34054) 대전광역시 유성구 유성대로 1548(화암동 58-4번지)
전화 : (042) 612-8296, 8210 팩스 : (042) 612-8209