Regular paper

Journal of the KIECS. pp. 725-730, vol. 12, no. 5, Oct. 31 2017, t. 85, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2017.12.5.725

원전 사이버 보안 취약점 점검 도구 개발을 위한 규제요건 분석

김승현* · 임수창* · 김도연**

Regulatory Requirements Analysis for Development of Nuclear Power Plants Cyber Security Vulnerability Inspection Tool

Seung-Hyun Kim* · Su-Chang Lim* · Do-Yeon Kim**

요 약

원전의 안전 유지를 위한 계측제어계통에 일반적인 IT 자원을 활용하는 사례가 증가하고 있다. 이에 따라 기존 IT 자원이 갖는 잠정적인 보안 취약점으로 인해 원전 사이버 보안 침해 사고가 발생할 수 있으며, 원전의 가동 중단뿐만 아니라 국가적 재난에 이르는 심각한 사고를 야기할 수 있다는 문제가 제기되고 있다. 국내 원자력 규제기관에서는 이에 대응하기 위해 원전 사이버 보안 규제지침을 개발하고 규제 대상 및 범위를 확대시키고 있지만, 원전의 일반적인 보안 문제뿐만 아니라 원전 취약점에 특화된 공격에도 대응할 수 있는 방안이 필요하다. 이에 본 논문에서는 R.G.5.71에서 규정하고 있는 내용 중 취약점 점검과 관련된 42개 항목을 선별하여 5가지의 유형으로 분류·분석하였다. 제안된 분석 내용을 바탕으로 취약점 점검 도구를 개발한다면 원전 사이버 보안 취약점 점검 효율성을 향상시킬 수 있을 것으로 판단된다.

ABSTRACT

The use of general IT resources in the Instrumentation and Control system(I&C) for the safety of Nuclear Power Plants(NPPs) is increasing. As a result, potential security vulnerabilities of existing IT resources may cause cyber attack to NPPs, which may cause serious consequences not only to shutdown of NPPs but also to national disasters. In order to respond to this, domestic nuclear regulatory agencies are developing guidelines for regulating nuclear cyber security regulations and expanding the range of regulatory targets. However, it is necessary to take measures to cope with not only general security problems of NPPs but also attacks specific to NPPs. In this paper, we select 42 items related to the vulnerability inspection in the contents defined in R.G.5.71 and classify it into 5 types. If the vulnerability inspection tool is developed based on the proposed analysis, it will be possible to improve the inspection efficiency of the cyber security vulnerability of the NPPs.

키워드

Cyber Security of Nuclear Power Plants, Instrumentation & Control Systems, Regulatory Guide, Vulnerability Inspection
원전 사이버 보안, 계측 제어 계통, 규제 지침, 취약점 점검

* 순천대학교 컴퓨터공학과(skim@scnu.ac.kr, suchangLim@scnu.ac.kr)
** 교신저자 : 순천대학교 컴퓨터공학과
· 접 수 일 : 2017. 07. 04
· 수정완료일 : 2017. 08. 13
· 게재확정일 : 2017. 10. 18
· Received : July 04, 2017, Revised : Aug 13, 2017, Accepted : Oct 18, 2017
· Corresponding Author : Do-Yeon Kim
Dept. of Computer Engineering, Sunchon National University,
Email : dykim@scnu.ac.kr

Ⅰ. 서 론

IT 산업의 발전은 기존 아날로그 방식의 정보처리 과정을 디지털화・자동화하는데 일조하였으며, 사회 전반의 다양한 분야에서 핵심기술로서 자리매김하고 있다. 이러한 경향은 국가기반시설로 보호되고 있는 원전에서도 나타나는데, 원전 설계에 따른 아날로그 방식 스위치 또는 기기 사용을 제외한 나머지 운용 자원에 대해 일반적인 IT 자원을 활용하는 비율이 증가하는 추세다[1]. 이에 따라 기존 IT 자원이 가지고 있는 잠정적인 보안 취약점으로 인해 원전 전반의 안전을 위협하는 사이버 보안 침해 사고가 발생할 수 있다. 특히 원전의 계측제어계통이 불법적인 사이버 공격에 의해 조작될 경우, 원전의 운전중단과 파손뿐만 아니라 국가적 재난에 이르는 심각한 사고를 야기할 수 있다는 문제가 제기되고 있다[2].

원전의 계측제어계통은 원자로와 전력생산을 위한 주변 설비들의 계측, 제어, 보호 및 감시 역할을 수행하는 시스템으로서 구조, 기능 및 규제등급에 따라 두 가지 계통으로 구분된다. 최근 국내 원자력 안전규제기관에서는 계측제어계통의 안전을 위한 사이버 보안 규제지침을 개발하고 규제 대상 및 범위를 확대시키는 추세이며, 이에 따라 물리적 격리 및 전략 수행계획 수립을 기반으로 원전 사이버 보안 구현을 진행하고 있다. 또한, 산업계 보안 기술을 적용하여 보편화된 사이버 공격 기술에 대응하기 위한 수단을 마련하고 있다[3]. 그러나 실제 원전 사이버 보안 침해 사고 사례가 환기하는 바와 같이, 원전 사이버 보안 취약점은 일반적인 IT 자원의 보안 취약성과 관련이 있으며, 원전의 일반적인 보안문제뿐만 아니라 원전 취약점에 특화된 공격 기술에도 대응할 수 있는 방안이 필요하다.

이에 본 논문에서는 Regulatory Guide 5.71(: R.G. 5.71)에서 규정하고 있는 사이버 보안 취약점 점검 관련 규제요건을 분석하였다. 논문의 Ⅱ장에서는 원전 사이버 보안 침해 사고 사례에 대하여 나열하고, Ⅲ장에서는 원전 사이버 보안 연구 동향에 대하여 서술하며, Ⅳ장에서 취약점 점검을 위한 규제요건에 대하여 서술한다. Ⅴ장에서는 취약점 요건을 분석하고, 마지막 Ⅵ장 결론을 끝으로 논문을 마무리하였다.

Ⅱ. 원전 사이버 보안 침해 사고 사례

2003년 미국 오하이오 주의 Davis-Besse 원전이 슬래머 웜(Slammer Worm)에 감염되어 감시계통 관련 장비가 불능 상태가 되는 사고가 발생하였다. 당시 유지보수 담당자가 사설 제어 네트워크를 통해 원전의 T1 회선에 전화 접속 하였는데, 개인 컴퓨터에 잠복해있던 슬래머 웜이 제어 네트워크에 퍼져 약 5시간 동안 안전감시시스템의 안전 매개변수 표시 시스템이 비활성화 되었다[4].

2006년 미국 앨라배마 주의 Browns Ferry 원전에서 통신망 오류로 인한 가동중지 사고가 발생하였다. 당시 이중의 PLC(: Programmable Logic Controller)로 작동되도록 설계된 2개의 원자로 재순환 펌프에 고장이 발생하여 원전이 수동 정지되었고, 재순환 펌프의 제어기가 반응하지 않는 증상을 보였으며, 발전소 내부의 시스템 네트워크가 과도한 트래픽 부하를 견디지 못한 것이 원인으로 조사되었다. 그러나 PLC의 고장과 트래픽 부하에 따른 재순환 펌프 제어기 고장 중 어떤 것이 원전을 정지시킨 원인인지에 대한 결론에는 아직 도달하지 못하였으며, 네트워크의 식별되지 않은 취약점 때문에 발생한 정지사고 정도로 추측되고 있다[5].

2010년 이란의 Bushehr 원전에서 우라늄 농축시설의 원심분리기 20% 가량이 파괴되는 사고가 발생하였다. 이 사고로 인해 해당 원전의 가동이 2년 동안 중단되었으며, 사고의 원인은 USB(: Universal Serial Bus)를 통해 침투한 스턱스넷(Stuxnet)의 공격 때문인 것으로 밝혀졌다. 스턱스넷은 특정 소프트웨어 및 장비에 감염되어 산업시설을 공격하도록 설계된 웜 바이러스의 일종으로, 시스템의 일부 구성 요소를 자신이 생성한 파일로 교체하여 공격자가 산업제어시스템을 감시하거나 임의제어 할 수 있도록 한다. 당시 Bushehr 원전은 독일 지멘스(Siemens)사의 SCADA(: Supervisory Control And Data Acquisition) 시스템을 사용하고 있었으며, 스턱스넷이 SCADA의 SIMATIC WinCC7과 SIMATIC Step7 통합관리도구를 공격한 것으로 알려져 있다[6].

Ⅲ. 원전 사이버 보안 관련연구 동향

3.1 원전 사이버 보안

계측제어계통은 원전의 사고 방지 및 완화 목적의 고유 기능을 수행하는 안전계통과 플랜트 운전에 필요한 계측, 제어 및 감시 기능을 수행하는 비-안전계통으로 구분된다. 두 계통 모두 다양한 시스템으로 구성되어 있기 때문에 원자력 기술 전문가와 IT 사이버 보안 전문가의 협력이 필요하다[7]. 안전계통과 비-안전계통은 기능 및 특성에 따라 다시 세부적인 계통들로 구분될 수 있으며, 각 계통별로 사이버 보안 위험등급을 책정하여 계측제어계통 보안의 효율성 및 가독성을 향상시킬 수 있다[8]. 대부분의 원전은 원전의 폐쇄성 유지를 통해 외부 접근을 근본적으로 차단하고 있으며, 신규 원전의 경우 강화된 접근 통제, 물리적 방호, 방어 아키텍처 설계 요소가 포함되어 원전 사이버 위협에 대한 대응 수단을 마련하고 있다. 한편, 근래의 계측제어계통에 직접적으로 적용할 수 있는 원전 사이버 보안 기술과 장비는 부족한 현실이며, 관련 연구기관 및 산업체가 이것을 개발하기 위한 R&D를 추진하고 있다[9]. 국내에서는 개발 대상 계통의 취약점 분석이 원전 디지털 안전계통의 국산화 과정에서 진행된 바 있다. 첨단 원전의 개발, 건설 및 해외수출이 상대적으로 활발한 우리나라에서는 원전에 특화된 사이버 보안 기술 개발을 위해 기술체계 분석 및 방향설정 등 체계적인 연구가 필요하다[10].

3.2 원전 규제지침

R.G. 5.71[11]은 사이버 공격으로부터 원자력발전소 컴퓨터, 통신 시스템 및 네트워크를 보호하기 위해 미국 원자력규제위원회(NRC: Nuclear Regulatory Commission)에서 발간한 규제지침으로, 미 연방법 10CFR73.54에 기재된 사이버 보안 법령을 세분화한 것이다. R.G. 5.71은 디지털 자산의 중요도에 따라 사이버 공격으로부터 반드시 보호되어야 할 요소들을 선정하여 주요 디지털 자산(CDA: Critical Digital Asset)으로 구분하고 있고, CDA의 사이버 보안 위협에 대응하기 위해 포괄적인 보안 통제수단과 방어 아키텍처를 적용하고 있으며, CDA의 SSEP(: Safety, Security, Emergency Preparedness) 기능 수행 여부에 따라 사이버 보안 적용 범위를 정의하고 있다. R.G. 5.71은 디지털 컴퓨터, 통신시스템 및 네트워크 분석, CDA 식별과 방어 아키텍처 적용뿐만 아니라 잠재적인 사이버 위협으로부터 CDA를 보호하고 보안 수명주기(Security Life Cycle) 활동을 이행하기 위한 보안 프로그램을 작성/유지토록 지시하고 있다.

Ⅳ. 취약점 점검을 위한 규제요건

R.G. 5.71은 원전의 사이버 보안을 위한 규제지침으로써 안전계통과 안전 유지를 위해 필수적인 계통, 보안 기능 및 비상대응설비, 그리고 이들을 보완하는 계통, 디지털 컴퓨터와 통신계통 및 네트워크의 보호를 위해 적용되며, 원전의 기술적·운영적·관리적 통제를 위해 원전 사이버 보안 계획서를 작성하도록 지시하고 있다. 본 장에서는 원전의 규제요건 중 취약점 점검과 관련성이 높은 일부 항목의 규제요건에 대하여 나열한다.

○ 사고 대응

사이버 보안 계획은 아래의 내용을 해결할 수 있는 방법을 포함하는 사고 대응 및 복구 조치를 기술해야 한다.

- 사이버 공격에 대한 시기적절한 탐지 및 대응 능력 유지
- 사이버 공격의 결과 완화
- 악용된 취약점 수정
- 사이버 공격에 영향을 받은 시스템, 네트워크 및 장비의 복원

○ 사이버 보안 프로그램의 유지

- 지속적인 감시 및 평가
- 형상 관리
- 변경 관리
- 변화와 환경에 대한 보안 영향 분석
- 효과 분석
- 지속적인 보안 통제 및 프로그램의 효과 평가
- 취약점 검사 및 평가
- 변경 제어
- 보안 프로그램 검토

○ 보안 통제의 효율성 분석

- 사이버 위협 및 취약점들이 끊임없이 변화하는 환경에서 기존의 보안 통제가 지속적으로

적절하게 수행되고 있는지 평가
- 각 보안 통제에 대한 특정 요구사항에 따라 최소 1년 또는 더 자주 보안 통제의 유효성을 검증

○ 취약점 스캔 및 평가
- CDA의 보안 상태에 잠재적으로 영향을 미칠 수 있는 새로운 취약점을 확인한 경우, 모든 CDA에 대하여 정기적으로 취약점 스캐닝을 수행
- 취약점 관리 프로세스의 일부를 자동화하는 취약점 스캐닝 도구와 기법의 채택
- 취약점 검사 보고서를 분석하고 현장의 SSEP 기능 및 CDA를 위협하는 취약점들에 대해 언급 필요
- 다른 CDA에 영향을 미칠 수 있는 유사 취약점들에 대하여 이해하고, 평가 및 완화 수행
- 취약점 스캐닝 프로세스가 SSEP 기능에 악영향을 주지 않도록 보장

○ 소프트웨어의 취약점 점검
- 약하거나, 검증되지 않았거나, 비표준 암호화 모듈의 사용 여부
- 민감한 통신에 안전하지 않은 네트워크 프로토콜의 사용 여부
- 안전하지 않다고 알려진 소프트웨어 컴포넌트 또는 라이브러리의 사용 여부
- 알려진 취약점의 내포 여부
- 안전하지 않은 구성파일 또는 응용 프로그램의 특징을 제어하는 옵션을 제공하는지 여부
- 시스템 자원 접근 제어를 위한 액세스 제어 매커니즘의 부적절성 또는 부적절한 사용의 유무
- 사용자, 프로세스 또는 응용 프로그램에 대한 부적절한 권한 부여의 유무
- 약한 인증 매커니즘 사용 여부
- 입출력 데이터 검증 실패 또는 부적절성
- 시스템 오류 또는 보안 관련 정보를 부적절하게, 또는 안전하지 않게 로깅하고 있는지 여부
- 부적절하게 제한된 버퍼의 사용 여부
- 문자열 포맷 취약점 내포 여부
- 권한 에스컬레이션 취약점 내포 여부
- 안전하지 않은 데이터베이스 트랜잭션 사용 여부
- 안전하지 않은 네이티브 함수 호출 사용 여부
- 숨겨진 기능 및 취약 기능의 코드 포함 여부
- 사이버 공격에 대한 취약성을 높이거나 설계 기반 기능의 신뢰성을 저하시키는지 여부
- 지원되지 않거나 문서화되지 않은 메서드 또는 함수의 사용 여부
- 문서화되지 않은 코드 또는 악의적 기능의 포함 여부

○ 개발된 소스코드의 분석을 통한 취약점 점검

모든 프로그래밍 언어에 대하여, 아래의 요소들은 문서화된다.
- 잠재적 보안 결함
- 보안 결함의 유형, 분류 및 원인
- 보안 결함 추적에 사용된 추적 메트릭스
- 요구사항에 명시된 설계 기능을 코드로 변환하는 동안 발생한 결함

Ⅴ. 취약점 요건분석

5.1 취약점 점검 규제요건 분류

R.G. 5.71 규제지침에 정의된 내용 중, ‘vulnerability’ 단어를 포함하고 있는 요건들은 총 42개 항목이며, 관련 내용에 따라 다음 5가지 유형으로 분류할 수 있다.

1) SSEP 기능 또는 성능과 보안 통제에 대한 요건
2) 취약점 평가 및 스캔 수행 필요성에 대한 요건
3) 취약점 스캔의 세부사항에 대한 요건
4) 소스코드 분석을 통한 취약점 점검 요건
5) 취약점 점검 도구 개발과 연관성이 낮은 요건

5.2 취약점 점검 규제요건 분석

5.2.1 SSEP 기능 또는 성능과 보안 통제에 대한 요건

해당 유형 요건의 주된 내용은 SSEP 기능 또는 성능에 악영향을 미치는 보안 통제를 적용해서는 안 되며(예를 들어, 시스템 응답 시간의 허용되지 않는 변경이나 바람직하지 않은 시스템 복잡성의 증가 등), CDA 기능 또는 성능에 미치는 악영향 때문에 보안

통제를 수행하지 않음으로서 발생할 수 있는 CDA의 잔여 취약점은 대체 통제방법으로 제거되거나 완화되어야 한다는 것이다. 그러나 개발하고자하는 취약점 점검 기술 또는 점검 도구를 해당 계통 기능의 일부분으로 구현하여 적용하는 것에 어려움이 있을 것으로 보이기 때문에 온라인 형태의 도구 개발을 위한 추가적인 작업이 필요할 것으로 판단된다.

5.2.2 취약점 평가 및 스캔 수행 필요성에 대한 요건

이 유형의 요건은 사이버 보안 유지를 위해 취약점 평가와 스캔이 필요하다는 점을 강조한다. 보안 프로그램이 마련된 후, 라이선시(Licensee)는 반드시 사이버 위험에 대한 평가와 관리를 수행하여야 하며, 보안 수명주기 안에 취약점 검사 및 평가를 포함해야 한다는 것이다. 이는 끊임없이 변화하는 사이버 위협과 취약점에 대응하기 위해 취약점 점검 도구가 반드시 갖추어야할 요건으로 판단된다.

5.2.3 취약점 스캔의 세부사항에 대한 요건

해당 요건은 취약점 스캔의 주기적인 수행, 취약점 스캔 도구 및 기술 적용과 같은 취약점 스캔의 세부사항에 대한 내용을 서술하고 있다. 라이선시는 CDA 보안에 영향을 미칠 수 있는 잠재적인 취약점이 발견된 경우 모든 CDA에 대해 적어도 정기적인 취약점 스캐닝을 수행하여야 하고, 도구 간의 상호 운용성 촉진 및 관리 프로세스의 일부를 자동화할 수 있는 취약점 스캐닝 도구와 기법이 채택되어야 하며, 취약점 스캔 결과 보고서를 분석해야 한다는 것이다. 특히, 취약점 스캐닝이 SSEP 기능에 악영향을 미치면 안되며, 악영향을 미칠 경우 스캔 대상의 CDA는 서비스(온라인)에서 제외되어야 함을 언급하고 있다. 이 내용들은 취약점 스캔이 일시적으로 수행되어서는 안되며, 취약점 스캔 주기, 점검내용, 도구 및 제한요소에 대한 계획을 바탕으로 수행되어야 함을 강조한다.

5.2.4 소스코드 분석을 통한 취약점 점검 요건

이 유형의 요건은 소스코드의 정적·동적 분석을 통한 취약점 점검과 관련된 요건이며, 라이선시가 CDA 시스템 개발자 및 통합자로부터 해당 제품이 알려진 모든 테스트 가능한 취약점과 악성코드로부터 안전한지 식별하고, 새로운 기술로 인해 변경될 수 있는 몇 가지 취약점 및 취약점 제거 요구사항을 충족하는지 확인하고, 문서화를 요구하여야 한다고 서술한다. 이 때 점검해야할 내용은 비표준 암호화 모듈 사용 여부, 안전하지 않은 네트워크 프로토콜 및 라이브러리 사용 여부, 부적절한 액세스 로직 등을 소스코드 레벨에서 정적·동적으로 분석하여야 한다고 언급한다.

5.2.5 취약점 점검 도구 개발과 연관성이 낮은 요건

마지막 요건은 취약점 점검 도구 개발과 연관성이 낮은 요건들이며, 특이사항이 없는 것으로 판단된다.

Ⅵ. 결 론

본 논문에서는 R.G 5.71 규제요건 분석을 통해 취약점 점검 도구 개발에 필요한 필수 요건들을 제시하였다. 취약점 점검 도구는 취약점 스캐닝이 SSEP 기능 또는 성능에 악영향을 미치지 않아야 하며, 주기적인 스캔 계획을 바탕으로 스캔도구, 점검내용 및 제한요소가 충분히 고려되어야 할 것으로 판단된다. 특히 보안 통제와 관련된 요건의 경우, 온라인 형태의 도구 개발이 필요할 것으로 판단된다. 본 연구에서 제시한 규제요건 분석 내용을 통해 추후 취약점 점검 도구 개발에 적용하여 원전 사이버 보안 취약점 점검이 효율적으로 수행될 것으로 판단된다.

감사의 글

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2016M2A8A4952280, 원전 계측제어 사이버보안 취약점 점검 기술).

References

[1] G. Jeong, J. Lee, and G. Park, “Application Trend of Cyber Security in Nuclear Power Plant Measurement Control System,” *J. of the*

Korea Information Processing Society Review, vol. 19, no. 5, 2012, pp. 69-77.
[2] D. Kim, "Vulnerability Analysis for Industrial Control System Cyber Security," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 1, 2013, pp. 137-142.
[3] D. Kim, "Implementation Plan and Requirements Analysis of Access Control for Cyber Security of Nuclear Power Plants," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 1, 2016, pp. 1-8.
[4] C. Cho, W. Chung, and S. Kuo, "Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 46, no. 3, 2016, pp. 356-369.
[5] Nuclear Regulatory Commission, "Potential Vulnerability of Plant Computer Network to Worm Infection," Nuclear Regulatory Commission Information Notice 2003-14, Aug, 2003.
[6] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 46, no. 10, 2016, pp. 1429-1444.
[7] M. Chung, W. Ahn, B. Min, and J. Seo, "A Study on Method to Establish Cyber Security Technical System in NPP Digital I&C," *J. of the Korea Institute of Information Security & Cryptology*, vol. 24, no. 3, 2014, pp. 561-570.
[8] C. Lee, "Trend of Technology of instrumentation and control system in Nuclear Power Plants," *J. of the Korea Institute of Information Security & Cryptology*, vol. 22, no. 5, 2012, pp. 28-34.
[9] W. Lee, M. Chung, B. Min, and J. Seo, "Risk Rating Process of Cyber Security Threats in NPP I&C," *J. of the Korea Institute of Information Security & Cryptology*, vol. 25, no. 3, 2015, pp. 639-648.
[10] C. Park, "Current Status for Cyber Security of Nuclear Power Plants and Long-term R&D Strategy," *J. of Electrical World*, vol. 430, 2012, pp. 59-65.
[11] US Nuclear Regulatory Commission, "Cyber Security Programs for Nuclear Power Facilities," Nuclear Regulatory Commission Regulatory Guide 5.71, Jan., 2010.

저자 소개

김승현(Seung-Hyun Kim)

2014년 순천대학교 컴퓨터공학과 졸업 (공학사)
2016년 순천대학교 대학원 컴퓨터과학과 졸업 (이학석사)
2016년 ~ 현재 순천대학교 대학원 컴퓨터공학과 박사과정
※ 관심분야 : 컴퓨터보안, 빅데이터, 기계학습

임수창(Su-Chang Lim)

2015년 순천대학교 컴퓨터공학과 졸업 (공학사)
2017년 순천대학교 대학원 컴퓨터공학과 졸업 (공학석사)
2017년 ~ 현재 순천대학교 컴퓨터공학과 박사 과정
※ 관심분야 : 컴퓨터비전, 영상처리, 인공지능

김도연(Do-Yeon Kim)

1986년 충남대학교 계산통계학과 졸업 (이학사)
2000년 충남대학교 대학원 정보통신공학과 졸업 (공학석사)
2003년 충남대학교 대학원 컴퓨터공학과 졸업 (공학박사)
1986 ~ 1996년 한국원자력연구원 선임연구원
1997 ~ 2008년 한국전력기술(주) 책임연구원
2008 ~ 현재 순천대학교 컴퓨터공학과 교수
※ 관심분야 : 영상보안, 산업제어시스템보안, 패턴인식, 컴퓨터비전