“CPS 보안” 특집호 발간에 즈음하여

오늘날 ICT 기술의 비약적인 발전에 따라서 우리의 사회적, 경제적 삶은 물리적인 공간을 넘어서 사이버 공간을 중심으로 재편되고 있습니다. 국가 차원의 신성장 동력 창출을 위한 기회 또한 사이버 공간으로 이동하고 있습니다. 그러나, 기회의 땅인 사이버 공간에서 국가 안보에 직결되는 사이버 공격이 발생할 수 있다는 사실을 우리 모두는 잘 알고 있습니다. 특히, 사이버물리시스템(CPS)에 대한 사이버공격은 사회적, 경제적 손실 뿐만아니라 국민의 생존권을 위협할 수 있습니다.

우리는 이미 2010년 스턱스넷(stuxnet)이 이란의 원자력시설을 공격하여 물리적인 파괴를 일으켰고, 2014년 독일 철강회사 용광로 제어시스템이 사이버공격으로 물리적인 피해를 입은 사실과 2016년 우크라이나에 사이버공격으로 대규모 정전사고가 발생한 사실들을 기억하고 있습니다. 이후 국가기반시설 제어시스템에 대한 사이버 공격은 매년 지속적으로 증가하고 있으며, 사이버 공격에 활용될 수 있는 제어시스템 보안 취약점 발견 건수도 매년 지속적으로 증가하고 있습니다. 특히, 전력, 원자력, 교통, 수자원 분야의 국가기반시설 제어시스템이 사이버 공격의 핵심 대상이 되고 있으며, 그 영역은 확장되어 스마트시티, 스마트팩토리, 자율주행자동차, 해양선박 및 항공우주 등의 CPS 분야로 확장되고 있습니다. 지금 이 시각에도 제2의 스턱스넷이 개발되어 우리나라의 국가기반시설 제어시스템을 겨냥하고 있는지도 모릅니다. 따라서, 제어시스템의 사이버 안정성 검증, 제어시스템 통합보안관제, 제어시스템 특화 정보보호 R&D 로드맵 수립, 기반시설 CERT 운영 및 클린 제어시스템 개발·도입 등이 매우 중요한 시점입니다.

본 특집호에서는 산업제어시스템의 IDS 성능 향상에 대한 연구, 차세대 원전인 SMR 개발과 사이버 보안, 원자력 시설 취약점 정량화 평가체계 적용 방안, 물리적 복제 불가능 함수에 기반하는 양자 내성 암호의 키 관리시스템, 인공위성 대상 우주방사선 차폐 방안, 리스크 기반 신조선 사이버 설계보안 접근 방식, 해양선박 대상 사이버 복원력 연구 동향, 엣지 컴퓨팅 기반 IIoT 보안 연구 동향을 분석하여 소개합니다. 본 논문들은 CPS 보안을 연구하는 전문가 및 정보보호 분야 연구원들에게 아주 유용한 정보가 될 것이라고 생각합니다.

끝으로 본 특집호의 완성을 위해 귀한 시간과 노력을 기울여 논문을 기고해 주신 모든 집필자 여러분과 편집에 수고해 주신 학회지 편집 위원회, 학회 사무국 관계자 여러분들께 심심한 감사의 말씀을 전합니다.

2023년 12월

가천대학교 서 정 택