Resilience Engineering for CPS

“ Cyber-Physical System을 위한 안전분석 방법 - STPA ”

자동차, 철도와 같은 운송기관 뿐 아니라 항만/도로 등 사회기반 시설, 자동화 생산시설 등 다양한 영역에서 자율 제어가 확대되고 있습니다. 이는 IoT를 활용한 광범위한 데이터의 수집과 Big Data를 통한 데이터의 처리, 그리고 AI를 활용한 지식 학습을 통해서 기존과 차별화된 기능과 성능을 제공할 수 있기 때문입니다. 이처럼 소프트웨어를 통해서 물리환경에 대한 제어를 수행하는 시스템을 Cyber-Physical System (이하 CPS)라고 합니다.

이러한 CPS의 경우 자율 제어에 기반하고 있으므로, 제어의 오동작/기능 장애/외란의 발생 시 심각한 위험을 발생시킬 수 있습니다. 예를 들어 자율주행 자동차의 경우, 제어 소프트웨어의 오동작/기능 장애 시 인명 사고와 같은 심각한 재난이 일어날 수 있으며, 악천후와 같은 심각한 외란도 유사한 재난을 야기합니다. 따라서 CPS의 개발 시에 안전성/신뢰성/복구성에 대한 분석 및 이에 대한 대응 설계가 체계적으로 수행되어야 하며, 이 경우 제어 대상에 대한 물리환경과 이에 대한 자율제어의 특성이 동시에 고려되어야 합니다.

CPS에 대한 안전분석을 위해서 MIT의 STPA (System-Theoretic Process Analysis)의 적용이 확대되고 있습니다. STPA는 시스템 이론 기반의 안전분석 체계로서 제어대상이 운영 상에 유지되어야 하는 속성들을 명시적으로 정의하고, 이에 대한 위반을 야기할 수 있는 원인들을 식별함으로써 기존의 방법으로 분석할 수 없었던 안전 이슈를 도출할 수 있으며, 특히 물리환경의 특성을 고려하는데 유용합니다.

이러한 STPA의 장점을 활용하여 기존의 안전성 뿐 아니라 신뢰성 및 복구성을 위협하는 원인들을 식별할 수 있도록 확장하여 다음과 같은 체계를 제공하고 있습니다.

■ CPS 안전성 / 신뢰성 / 복구성 분석 및 대응 설계 체계