ISSN 1229-6783(Print)
ISSN 2288-1484(Online)


# AGV 물류 이동장치의 효율적인 STPA 안전성 분석을 위한 운영 시나리오 연계 분석 프로세스 모델 연구

김 명 성* · 김 영 민*
*아주대학교 시스템공학과

# A Study on the Integrated STPA-Scenario Process Model for Efficient Safety Analysis Based on Operation Scenarios of AGV

Myung-Sung Kim* · Young-Min Kim*
*Department of Systems Engineering, Ajou University

## Abstract

In order to solve the rapidly increasing domestic delivery volume and various problems in the recent metropolitan area, domestic researchers are conducting research on the development of “Urban Logistics System Using Underground Space” using existing urban railway facilities in the city. Safety analysis and scenario analysis should be performed for the safe system design of the new concept logistics system, but the scenario analysis techniques performed in previous studies so far do not have standards and are defined differently depending on the domain, subject, or purpose. In addition, it is necessary to improve the difficulty of clearly defining the control structure and the omission of UCA in the existing STPA safety analysis. In this study, an improved scenario table is proposed for the AGV horizontal transport device, which is a key equipment of an urban logistics system using underground space, and a process model is proposed by linking systematic STPA safety analysis and scenario analysis, and UCA and Control Structure Guidelines are provided to create a safety analysis.

Keywords : STPA, Safety Anlysis, Operation Scenario, AGV

## 1. 서 론

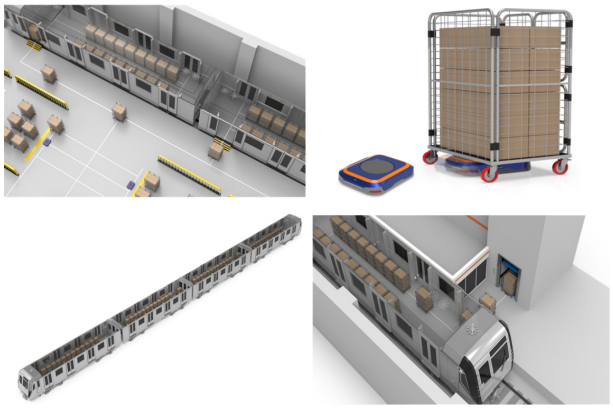
### 1.1 연구 배경

최근 국내 택배 물동량은 수도권을 중심으로 급격하게 증가하고 있는 추세이다. 거대 도시화로 인해 우리나라 전체 인구의 50.2%가 수도권에 거주하면서[1]. 코로나 팬데믹으로 인한 전자상거래 증가 및 1인 · 맞벌이 가구 확대 등의 영향으로 인한 소형가구의 소량 다빈도 배송 등이 국내 수도권 택배 물동량에 큰 영향을 끼친 것으로 보인다. 택배 물동량 수요가 폭발적으로 증가함에도 불구하고, 서울시 내 물류시설은 경기도의 5.3% 수준에 머물러 있으며, 이에 따른 물류인프라 부족으로 서울 택배가 타 지역을 경유해 비효율적으로 배송되고 있다[2]. 기존 도심 물류 시스템은 도로를 중심으로 화물 트럭을 이용한 배송 체계 운영으로 도로 교통 혼잡과 소음 공해, 환경 문제 등 사회적 비용이 동반 상승하는 고비용, 비효율 물류 구조의 문제점이 속출되고 있어 이를 개선하기 위한 새로운 개념의 시스템 적용이 필요한 실정이다[3].

이러한 문제를 해결하기 위해, 국내연구진은 도시 내 존재하는 기존 도시 철도시설과 지하공간 인프라를 활용한 “지하공간을 활용한 도시물류 시스템” 개발 연구가 진행되고 있으며 이는 도심 내 화물 차량의 운송을 대체할 것이라고 기대된다. 지하공간을 활용한 도시물류 시스템은 차량기지 기반의 도시철도 인프라를 활용하여 구축되는

†본 연구는 국토교통부/국토교통과학기술진흥원의 지원에 의하여 수행되었음(21HCLP-C163182-01).
†Corresponding Author : Young-min Kim, Systems Engineering, AJOU University, 206, World cup-ro, Suwon-si, Gyeonggi-do, E-mail: pretty0m@ajou.ac.kr
Received August 21, 2023; Revision September 18, 2023; Accepted September 18, 2023

공동물류 터미널에서 간선이동 화물차량이 차량기지에 입고 되면, 운송이 필요한 화물의 집하와 분류를 진행하고 목적지인 도심 화물 역사까지 운송이 필요한 화물을 화물열차에 탑승시킨다. 화물운송 전용 도시철도 화물열차는 기존의 사람을 운송하기 위한 여객 수송열차가 아닌 화물 수송을 위한 전용 도시철도 차량으로 개발되어 차량 내 화물의 반입과 반출이 가능한 시스템이다. 본 화물 열차를 통하여 목적지인 도심역사로 운송이 완료되면, 도심역사 내 공간의 이송을 위해 22대의 AGV (Automatic Guided Vehicle) 화물 수평이송장치를 통하여 화물을 자동으로 운송한다. 운송된 화물은 수직 이송장치를 통해 도심 역사 공간 내 화물 상, 하차 승강장으로 이송되어 말단배송, 즉 소형 화물 차량에 입고되어 운송지로 전달된다. 도시철도 물류 시스템은 전용 화물열차를 이용하여 화물의 운송과 회수를 수행하는 것에서 기존 물류시스템과의 기술적 차별점과 기존 시스템의 문제점을 해결하는데 기여할 것으로 예상된다. Figure 1은 지하 도시철도 물류 시스템의 주요 장비를 보여준다[4].



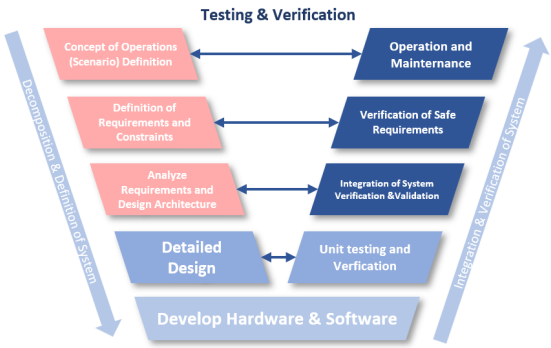
[Figure 1] Important Equipments in Urban undergrounds logistics system

이러한 신개념 물류 시스템을 구현하기 위해서는 시스템 설계 단계에서부터 실제 운영 시나리오에서 발생할 수 있는 위험원 및 위험상황에 대하여 안전성 분석이 우선시 되어야 한다. 본 지하공간을 활용한 도시물류 시스템은 기존 도시철도 시스템에서 사용되지 않는 수직 / 수평이송장치 등의 장치별 연계가 필요하므로 본 시스템의 장치 연계로 인하여 예측불가한 위험상황을 초래할 수가 있다. 따라서 이러한 연계로 발생할 수 있는 위험상황에 대해서 위험원 저감 대책의 마련을 마련하여 시스템 설계에 반영하는 것이 필요하다. 본 연구에서는 지하공간을 활용한 도시물류 시스템의 핵심장비 중 하나인 수평이송장치 AGV에 대하여 개선된 시나리오 분석기법을 통해 효율적인 STPA 안전성 분석을 수행하기 위하여 시나리오 분석 기법과 STPA 안전성 분석이 연계된 새로운 프로세스 모델을 제안한다.

## 2. 관련 선행연구

### 2.1 운영 시나리오 분석 관련 연구

지하공간을 활용한 도시물류 시스템과 같은 신개념 시스템을 효율적으로 구축하기 위해서는 ISO 15288 기반의 시스템 설계를 수행해야 한다. ISO 15288은 시스템의 전체적인 수명주기 프로세스를 다루는 표준으로써, 시스템의 개발 단계에서 생길 수 있는 설계오류를 줄여서 비용 및 기간을 최소화하여 오늘날 점점 복잡해지는 시스템의 설계를 효율적으로 수행할 수 있게 한다[5]. 시스템 수명주기 및 요구사항 정의 관련 표준 ISO/IEC 29148에서는 운영 시나리오에 대해서 “제품 또는 서비스와 환경 및 사용자의 상호 작용뿐만 아니라 제품 또는 서비스 구성 요소 간의 상호 작용을 포함하는 일련의 이벤트에 대한 설명을 제공하고 운영 시나리오는 요구 사항 및 설계를 평가하는데 사용되며 시스템을 확인하고 검증하는 것”이라고 정의되었다[6]. ISO 15288 기반의 시스템 설계를 수행하기 위해서는 우선 운영 시나리오를 정의하고 그에 따른 시스템의 요구사항을 정의하여 시스템에 요구되는 사양을 종합하여 개념설계를 진행하여야 한다. Figure 2는 V모델이라고 불리며, 시스템 개발의 주명주기 단계를 도식화하여 보여준다.




[Figure 2] System Lifecycle V-model based on ISO 15288

시스템 설계를 위해 정의하는 운영 시나리오와는 별개로, 운영 시나리오 정의는 안전성 분석을 진행하는데 앞서 수행되어야 할 기초적인 단계라고 볼 수 있다. HARA, HAZOP, FMEA, STPA 등의 보편적인 안전성 분석 프로세스를 살펴보면 먼저 시나리오를 구성하여 분석을 수행하거나, 발생할 수 있는 위험상황을 정의하면서 가상의 사

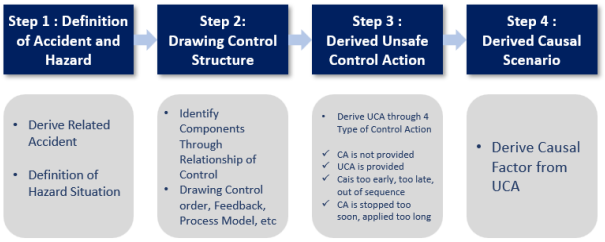
ISSN 1229-6783(Print)
ISSN 2288-1484(Online)


고 시나리오 및 위험상황을 도출하게 된다. 이렇게 수행된 안전성 분석의 결과는 그림 2에서 나타낸 단계와 같이 안전 제약사항을 도출하여 안전한 시스템을 설계하고 개발된 시스템에 대한 안전성을 검증할 수 있다. 허상민 외 2는 노인의 생활을 보조하고 지원하는 실버메이트 지능형 서비스 로봇을 대상으로 로봇이 주변의 상황을 인지하고 그 환경에 적절한 서비스를 사용자에게 제공하기 위한 요구사항을 시나리오 기반의 분석으로 도출하였다. 본 연구의 결과로 최상위 목표로부터 로봇 내부 객체가 포함된 시스템의 행위까지의 요구사항을 도출해 냈으며, 내부 레벨에서의 요구사항 후보들간의 비교를 통해서 충돌 가능한 요구사항 들을 미리 식별 가능했지만 시스템이 커질수록 비교 횟수가 많아지므로 충돌 가능성을 손쉽게 찾아 낼 수 있는 방법에 대한 연구가 필요하는 결론을 얻었다[7]. 백윤석 외 6은 자율주행차량이 V2X의 의존도가 높은 자율주행시스템에서 V2X 통신의 고장으로 인한 위험성에 대하여 자율주행차량의 교차로 시나리오를 제시하여 V2X를 활용한 자율주행시스템의 서비스 시나리오를 정의 하였으며 이를 기반으로 기능을 도출하고 V2X의 위험 요인을 분석하여 오작동을 정의하였다. ISO26262 Part3 프로세스를 활용하여 HARA 및 고장 주입 시나리오의 시뮬레이션을 통해 V2X 모듈의 고장으로 인한 위험성과 이를 확인하는 검증 과정을 제시하였다[8].

앞서 진행된 선행연구를 통하여 시나리오 분석기법은 도메인이나 대상 혹은 목적에 따라 다르게 정의되며 이는 대표적인 분석방법이 존재하지 않아 연구진에 따라 주관적으로 작성될 수 있음을 확인하였다.

## 2.2 STPA 안전성 분석 관련 연구

현대사회에서의 시스템은 기능과 구성이 복잡해짐에 따라 사고의 발생 원인을 특정 컴포넌트및 기능의 문제로 규정하기 어려워졌다. 시스템의 복잡성으로 인해 시스템 내 문제를 식별하기가 어려우며, 시스템들 간 또는 시스템과 외부 요소들 간의 다양한 상호작용으로 복합적인 요인에 의해 예기치 못한 사고가 발생할 수 있기 때문이다. 이에 기존 위험분석 기법과는 다른 새로운 관점의 위험분석 방법이 필요하게 되었으며, 2012년 미국 MIT 대학의 Nancy G. Leveson 교수는 시스템 이론에 기반하여 STPA(System-Theoretic Process Analysis)라는 위험분석 방법을 발표하였다. 해외에서는 2012년 STPA가 발표된 이래 항공, 자동차 등 안전 필수 도메인을 중심으로 STPA에 대한 연구와 활용이 꾸준히 확산되고 있다. 따라서 STPA 안전성 분석은 효율적인 복잡한 시스템에 대한 안전성 분석을 가능하게 하는 최신 기법으로, 지하공간을 활용한 도시물류 시스템과 같은 복잡한 신개념 시스템을 설계할 때 수행되는 것이 적합하다고 판단된다.




[Figure 3] Process Model of STPA

Figure 3은 STPA 안전성 분석 프로세스를 나타낸다. 기존의 STPA 분석 프로세스 대하여 자세히 살펴보자면, 1단계에서 시스템에서 발생할 수 있는 치명적인 사고 및 위험상황에 대해서 정의를 진행한다. 2단계에서 Control Structure는 복잡하게 얽힌 서브 시스템을 식별하기 위해서 제어 관점에 따른 주체(Controller)와 객체(Controlled Process), 그리고 제어(Control Action)와 반응(Feedback)으로 구성된다. 그리고 기능 흐름에 따라 제어명령, 프로세스, 피드백 등을 도식화한다. 3단계에서 Unsafe Control Action(UCA)은 시스템의 위험을 유발할 수 있는 불안전한 기능수행을 의미한다. 기능수행에서 UCA를 도출하기 위해서는 주체가 기능수행을 제공하는 형태와 해당 기능수행이 행해지는 특정 상황 또는 조건이 필요하다. 기능수행이 불안전할 수 있는 형태는 Table 1과 같이 크게 4가지 타입으로 분류된다.

<Table 1> 4 Type of Unsafe Control Action

| Type | Description |
|---|---|
| Not Providing Causes Hazard | Cause hazard due to Controller not providing control action |
| Providing Causes Hazard | Cause hazard due to Controller providing control action |
| Too Late, Too Soon, Out of order | Cause hazard due to Controller providing control action but too late, too soon or out of order |
| Stopped Too Soon/ Applied Too Long | Cause hazard due to Controller providing control action but Stopped Too Soon/ Applied Too Long |

시스템의 위험은 단순히 Control Action 제공 형태에 따라 발생하지 않으며, Control Action이 제공되는 시점의 시스템 및 주변 환경 조건에 따라 위험이 발생할 수 있다. 이러한 정보를 Context로 정의하고 4가지 타입의 Control Action를 조합하여 UCA를 도출한다. 4단계에서는 위험을 유발할 수 있는 UCA가 왜 발생하는 그 원인들

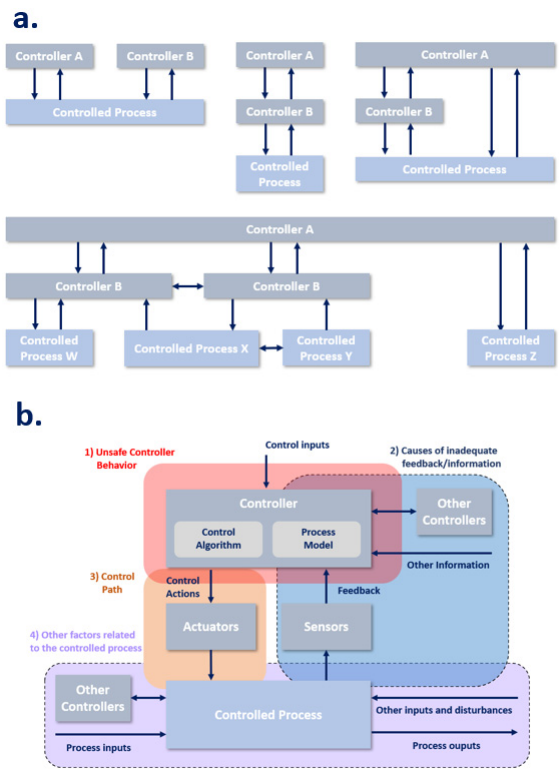
을 Control Structure를 기반으로 분석한다. 최종적으로 이러한 원인(Causal Factor)들을 토대로 하여 원인 시나리오(Causal Scenario)를 작성함으로 위험원을 식별하는 것을 목표로 한다[9]. 최나연 & 이병걸은 국제 표준 IEC 61508에서 명시하고 있는 안전 생명주기에 따라 소프트웨어 안전성 품질을 확보하기 위해서 개발 초기 단계에서 위험원 및 위험 분석(Hazard and risk analysis)을 통한 안전 요구사항을 개발하기 위해 SysML을 활용한 STPA 기반의 위험원 분석 프로세스를 제안한다. 본 연구의 결과로 SysML의 BDD과 IBD 다이어그램을 활용하여 기존 STPA 분석에서 활용되고 있는 Control Structure를 보다 명확하게 정의할 수 있도록 개선하였고, SD 다이어그램을 활용하여 안전 제약사항(요구사항)을 상세화할 수 있도록 하였다. 제안 방법의 적용 결과, STPA에서 누락되었던 위험원을 추가적으로 식별할 수 있었고, 위험원의 발생 시나리오도 상세하게 구체화할 수 있었다[10]. 양현수 & 권기현은 안전 요구사항과 연결되는 STPA 사고 시나리오 식별 단계에서의 누락을 최소화하기 위하여, 이전 연구들에서 제시되었던 접근법들의 공통점을 통합하고, 취약점을 보완하는 방법에 대한 연구를 진행하였다. 본 연구의 결과로 사고 시나리오 식별 절차와 이를 보조해주는 시나리오 테이블을 제안하였으며 마지막으로 제안하는 시나리오 테이블을 철도 디오라마 시스템의 위험원 분석에 적용하여 확인하였다[11].

앞서 진행된 선행연구 분석을 통해 STPA 안전성 분석을 위해 정의되는 시나리오는 시스템 설계를 위해 정의되는 운영 시나리오와 형식 및 구성의 차이가 있음을 확인하였고, STPA 안전성 분석이 수행됨에 있어서 Control Structure의 명확한 정의의 어려움과 UCA의 누락을 보완하기 위하여 여러 연구가 진행된다는 것을 확인할 수 있었다.

## 2.3 문제정의

앞 절에서는 지하공간을 활용한 도시물류 시스템 AGV에 대한 STPA 안전성 분석 및 시나리오 분석과 관련된 선행연구 분석을 실시하였고, 이에 따라 두가지 문제점이 존재한다는 것을 발견하였다.

첫 번째로, 지하공간을 활용한 도시물류 시스템과 같은 새로운 시스템의 안전성 분석을 진행하기 위해서는 시나리오 분석을 수행하여야 하는데, 현재까지 선행연구들에서 수행되는 시나리오 분석기법은 기준이 존재하지 않고, 도메인이나 대상 혹은 목적에 따라 다르게 정의되고 있다. 특히, 시스템에 설계를 위해서 정의되는 운영 시나리오와 안전성 분석을 위해 정의되는 운영 시나리오의 형식 및 구성의 차이로 인하여 제작되는 운영 시나리오 기준의 모호함이 요구사항을 정의하는 운영 시나리오와 안전성 분석을 수행하기 위해 정의되는 운영 시나리오가 따로 정의되는 비효율적인 시스템의 설계와 안전성 분석을 진행한다고 판단되었다. 두 번째로는, 기존의 STPA 안전성 분석을 수행함에 있어서 Control Structure의 명확한 정의의 어려움과 UCA의 누락에 대해서도 개선이 필요한 실정이다. 기존의 STPA 안전성 분석을 살펴보자면, 분석 대상이 되는 시스템의 범위를 정의하여 한 개 또는 여러 개의 Control Structure를 구성하여야 한다. 대형 시스템이거나 서브시스템이 복잡하게 얽혀있는 시스템일수록 Control Structure의 도식화와 UCA의 발생 원인을 도출하기 위한 관점이 매우 복잡해지며, Figure 4의 a와 같이 Control Structure는 시스템을 어떻게 정의하는지에 따라서 다양한 형태로 작성될 수 있기 때문에 실제 STPA를 수행할 때, 시스템에 따라 Control Structure가 복잡해질수록 Figure 4의 b와 같이 UCA를 도출하기 위해 분할하는 관점 또한 모호해져 Control Structure의 작성이 복잡하고 어려워질 수 있다.




[Figure 4] a- Variety shape of Control Structure / b- Viewpoint of Derive UCA

따라서 시스템에 대한 요구사항을 정립하는 개발 첫 번째 단계에서 운영 시나리오를 정의하여 이를 기반으로 시스템의 개념설계 및 시스템에 대한 안전성 분석을 동시에 수행할 수 있다면 더 효율적인 시스템 개발 및 안전성 분

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)


석이 가능해지리라고 판단된다. 뿐만 아니라 이는 STPA 안전성 분석 수행의 가이드 라인이 되어 Control Structure의 도출과 UCA의 도출 및 보완에도 도움이 될 것으로 예상된다.

이러한 문제를 개선하기 위하여 본 연구에서는 지하공간을 활용한 도시물류 시스템의 핵심장비인 AGV 수평이송장치를 대상으로 논리적으로 접근할 수 있는 시나리오 테이블을 제안하며, 체계적인 STPA 안전성 분석 및 시나리오 분석을 연계하는 하나의 새로운 시나리오-STPA 연계분석 프로세스 모델을 제시하여 UCA 및 Control Structure를 작성하는데 가이드라인을 제공하고 편리하게 결과를 도출할 수 있도록 하였으며 이를 통해 지하공간을 활용한 도시물류 시스템의 효율적인 안전성 분석을 수행하고자 한다.

## 2.4 논문의 구성

본 논문은 다음과 같이 구성된다. 2장에서는 기존에 존재하던 시나리오 분석 및 STPA 안전성 분석에 대한 개념 및 절차를 소개하고 각각에 대한 선행 연구와 문제정의 및 시나리오- STPA 연계 분석 프로세스의 필요성에 대해 설명하였다. 3장에서는 새로운 형태의 시나리오 분석 테이블을 통해 STPA 안전성 분석 절차와 시나리오 분석 기법을 연계한 시나리오- STPA 연계 분석 프로세스 모델을 제안한다. 4장에서는 제안한 프로세스 모델 및 시나리오 기법을 반영하여 AGV 수평이송장치에 대한 시나리오 및 STPA 안전성 분석 사례 연구로 수행한 결과를 보여준다. 마지막으로 5장에서는 이에 대한 결론을 도출한다.

# 3. 시나리오-STPA 연계분석 프로세스 구축

## 3.1 제안하는 시나리오 정의 테이블

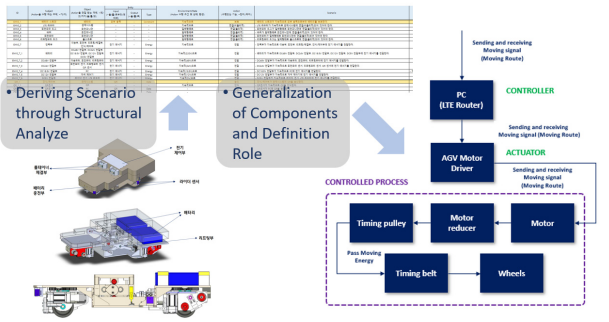
본 연구에서는 체계적이고 효율적인 안전성 분석을 위해서 논리적으로 시나리오를 정의할 수 있도록 Figure 5와 같이 새로운 형태의 테이블로 시나리오 분석 기법을 제시하였다. 개선된 시나리오 정의 테이블은 문법 구성적 관점으로 개발되었으며, 체계적인 상세 운영 시나리오를 정의하기 위해서 세부적 단계로 나누어 진행하였다. 먼저 시스템의 각 구성요소를 계층적 구조로 정의한 뒤 각 구성요소의 활동을 주체 및 객체로 나누어 Subject와 Object로 설정한다. Entity에는 전달하는 데이터 및 동력에 대하여 Input과 Output을 설정해 데이터 및 동력의 변환을 정의할 수 있고, 이는 시나리오에 따라서 생략가능하다. Environment/tate에는 기능의 수행 조건 및 상태, 환경에 대하여 정의하고, Action에는 수행되는 기능을 정의한다. 마지막으로 최종적으로 정의된 기능수행 및 활동에 대한 내용을 문장으로써 Scenario에 정의한다. 이렇게 도출된 운영시나리오는 시간에 따라 진행되는 기능 흐름에 대하여 STPA를 포함한 다른 정성적 안전성 분석의 기반 데이터로 활용될 수 있으며 또한 이를 기반으로 기능 요구사항을 도출할 수 있다.

| No. | ID | Subject | Object | Entity | | | Environment/State | Action | Scenario |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Input | Output | Type | | | |
| Rabeling ID for Distinguish Scenaro | | Subject of Action | Object received action | Input Data or Control signal | Output data or Control signal | Type of Data/ Signal | Action condition or Environments /state | Descrition of Action | Intergrated Scenario |

[Figure 5] Suggested Table for Scenario Analysis

## 3.2 개발된 시나리오-STPA 연계 분석 프로세스 모델

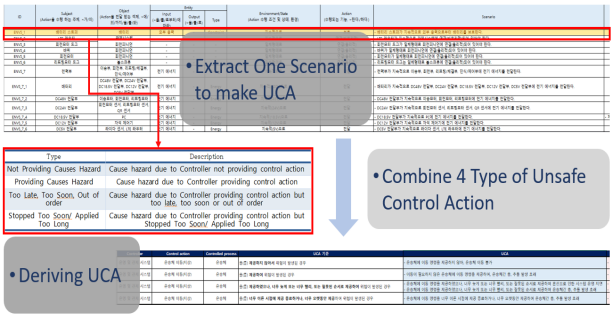
제안하는 테이블을 통하여 시나리오를 분석하는 과정에 대해서 설명하자면, 운영 시나리오 분석은 시스템을 설계할 때 앞선 Figure 2에서 먼저 수행되는 요구사항 정의 단계에서 수행된다. 시스템에 대한 범위와 운영 프로세스에서 사용되는 객체 및 구성요소가 계층적으로 정의되고 나면, 이에 대한 운영 프로세스를 시스템 하위 단계인 서브 시스템 수준으로 정의하고 점차 하위단계인 파트 수준으로 상세화를 진행하여 상세한 운영 프로세스를 정의한다. 이를 통하여 시스템 구성요소에 요구되는 기능 요구사항을 정의 및 보완할 수 있다. 이렇게 정의된 상세 운영 시나리오는 Control Structure를 도식화하는데 가이드라인이 된다. 서브 시스템 수준의 시나리오에 정의된 Subject와 Object를 식별하여 Controller, Actuator를 구분하고 Action에 대해서는 Controlled Process로 정의한다. Figure 6은 이러한 과정의 예시를 나타낸다.




[Figure 6] The Process of Deriving Control Structure

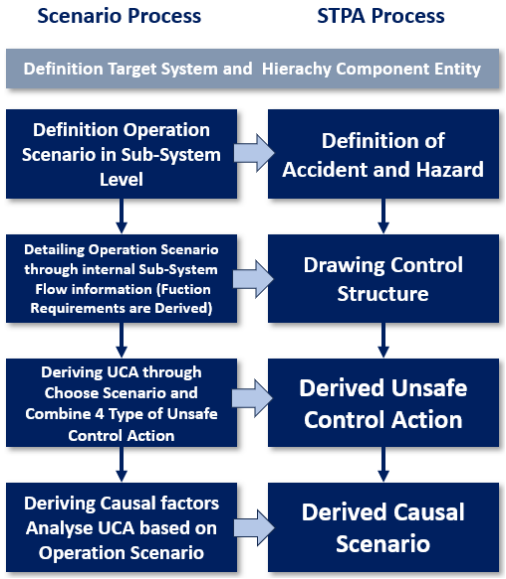
다음은 이러한 상세 운영 시나리오를 STPA 안전성 분석을 하기 위하여 상세 운영 시나리오의 각 단계마다 운영

프로세스에 관한 Action을 추출하여 Table 1과 같이 STPA에서 제시하는 4개의 Control Action을 조합하여 운영 시나리오에서 발생할 수 있는 UCA를 도출할 수 있다. 이렇게 도출된 UCA는 Control Structure를 통해 도출된 UCA와 같이 통합될 수 있다. Figure 7은 이러한 예시를 나타낸다.




[Figure 7] The Process of Deriving UCA

이러한 과정을 통해서 시스템의 기초 개념 설계단계에서 정의한 운영 프로세스를 통하여 STPA 안전성 분석의 기반을 마련하고, UCA와 Control Structure를 도출할 수가 있게 된다. 이를 통하여 안전성 분석을 위해 위험 시나리오를 따로 정의하는 비효율적인 반복 수행에 대해 효율적으로 수행기간을 줄일 수 있으며, 시스템의 개발 전 STPA 안전성 분석에 대한 결과는 시스템을 설계할 때 안전 제약사항으로 반영되어 시스템의 개발 실패를 방지할 수 있다. Figure 8은 개선된 시나리오– STPA 연계 분석 프로세스를 도시한다.




[Figure 8] The Process Model of Intergrated Scenrio–STPA Analysis Process

## 4. 시나리오 분석 도출 절차 및 STPA 안전성 분석 사례 연구

본 장에서는 앞서 도출된 시나리오– STPA 연계 분석 프로세스를 AGV 수평이송장치에 대하여 적용한 사례를 보여준다. 먼저 AGV의 구동 시스템 구성요소를 계층적으로 정의하여 Table 2와 같이 정의하였다. 정의한 구성요소를 토대로 AGV의 기능 흐름에 맞춰 주체와 객체를 식별하여 서브 시스템 수준부터 컴포넌트 수준까지 기능을 세부적으로 분석하여 운영 프로세스를 앞서 제안한 시나리오 분석 테이블을 통해 나타내었다. Table 3은 이를 요약한 결과를 보여준다.

<Table 2> The Hierarchical Structure of Driving System

| System | Sub–System | Component |
|---|---|---|
| Driving System | Moving Department | Motor |
| | | Motor reducer |
| | | Timing pulley |
| | | Timing belt |
| | | Wheels |
| | Rotate Department | Rotation motor |
| | | Rotation pinion |
| | | Rotation gear |
| | Lifting/ Bondage Department | Lifting motor |
| | | Lifting motor reducer |
| | | Ball screw |
| | | Cam |
| | | Link equipment |
| | | Lifting board |
| | | Bondage magnet |

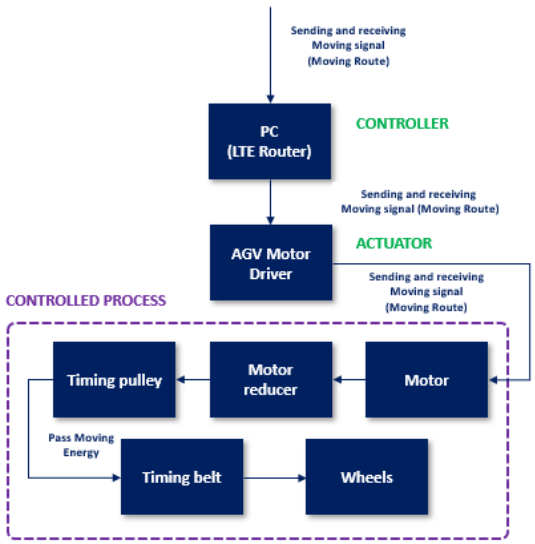
<Table 3> Sample of Operation Scenario of Driving AGV

| Subject | Object | Action | Scenario |
|---|---|---|---|
| Driving System | – | Drive | – Driving System is operate with 1.2m/s Velocity, Hill Climbing Ability is atleast 1kW. |
| Control System | PC | Send | – Control system sending moving order signal to PC. |
| PC | – | Receive | – PC received moving order signal. |
| PC | Motor Driver | Send | – PC sending moving order signal to motor driver. |
| Motor Driver | – | Receive | – Motor driver received moving order signal. |
| Motor Driver | Motor | Send | – Motor driver sending moving order signal to motor. |
| Motor | – | Receive | – Motor received moving order signal. |

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)


| Subject | Object | Action | Scenario |
|---|---|---|---|
| Motor | Motor reducer | Transfer | – Motor Transfer moving energy to motor reducer through moving order signal (Moving route). |
| Motor reducer | Timing pulley | Transfer | – Motor reducer Transfer moving energy to Timing pulley through moving order signal (Moving route). |
| Timing pulley | Timing belt | Transfer | – Timing pulley Transfer moving energy to Timing elt through moving order signal (Moving route). |
| Timing belt | Wheels | Transfer | – Timing belt Transfer moving energy to wheels through moving order signal (Moving route). |
| Wheels | – | Drive | – Wheels are moving through moving order signal (Moving route) |

정의된 상세 운영 시나리오는 AGV 시스템 구성요소에 요구되는 기능 요구사항을 반영하여 시스템 사양 및 요구사항을 보완할 수 있으며 도출된 운영 시나리오를 기반으로 STPA 안전성 분석을 실시하였다. Figure 9는 AGV의 운영시나리오 중 구동/정지 프로세스에 대해 Control Sructure를 도식화한 결과를 나타낸다.




[Figure 9] Control Structure based on Operation Scenario

도출된 Control Structure를 통하여 UCA를 도출할 수 있으며, 운영 시나리오 기반 UCA를 도출하여 통합할 수 있다. Table 4는 구동/정지 프로세스의 시나리오에서 이송부의 구동 시나리오에 대해 4개의 Control Action과 조합하여 UCA를 도출한 결과의 예시를 나타낸다.

<Table 4> Sample of Derived UCA from Operation Scenario

| Scenario | Type of Unsafe Action | UCA |
|---|---|---|
| – Driving System is operate with 1.2m/s Velocity, Hill Climbing Ability is atleast 1kW. | Not Providing Causes Hazard | As the AGV cannot drive, there is a risk of collision with other AGVs and system operation is stopped. (UCA-1) |
| | Providing Causes Hazard | The AGV leaves the stop position and continues to drive, resulting in collisions with obstacles and other AGVs and falling cargo. |
| | Too Late, Too Soon, Out of order | System operation delays due to confusion caused by giving movement commands to the AGV, but giving them too late, too soon, or in the wrong order |
| | | A movement command was given to the AGV, but it was given too late, too quickly, or in the wrong order, resulting in a collision or collision between AGVs. |
| | Stopped Too Soon/ Applied Too Long | Collision or collision between vehicles is caused by ending the move command to vehicles too early or for too long. |

마지막으로 Table 4의 UCA-1에 대해 Control Structure를 통하여 도출한 UCA와 상세 운영 시나리오를 통하여 도출한 UCA를 통합하여 Causal (Factor) Scenario를 분석하여 Table 5와 같이 나타내었다. 도출한 Causal Scenario는 시스템의 안전 제약사항으로 추가되었다.

<Table 5> Sample of UCA-1 Causal Scenario

| Descrition of UCA-1 | | |
|---|---|---|
| As the AGV cannot drive, there is a risk of collision with other AGVs and system operation is stopped. | | |
| Components | | Causal Scenario |
| PC | Algorithm | -Input moving signals of incorrect information<br>-Transmission and reception of incorrect information due to algorithmic calculation errors |
| | LTE Router | -Contamination and damage of LTE router communication module |
| Motor driver | Algorithm | -Input moving signals of incorrect information from PC<br>-Transmission and reception of incorrect information due to calculation errors in motor driver algorithms |
| | H/W | -Contamination and damage of communication module |

| Descrition of UCA-1 | |
|---|---|
| Motor | -Damage caused by fatigue or excessive load, such as cracks or ruptures<br>-Transmission of inappropriate signals |
| Motor reducer | |
| Timing plley/belt | |
| Wheels | |

## 5. 결론

국내 택배 물동량이 급증함에 따라, 기존 도심 내 물류 배송체계에 도로 교통 혼잡 및 소음 공해, 환경 문제 등 비효율 물류 구조의 문제점을 해결하기 위해 국내 연구진은 지하공간을 활용한 도시물류 시스템을 설계 및 개발 중에 있다. 지하공간을 활용한 도시물류 시스템은 신개념 시스템으로 기존 도시철도 시스템에서 사용되지 않는 AGV와 같은 신개념 물류 장치 등을 사용하여 본 시스템의 장치 연계로 인하여 예측불가한 위험상황을 초래할 수가 있다. 지하공간을 활용한 도시물류 시스템과 같은 새로운 시스템의 설계를 진행하기 위해서는 시스템의 요구사항을 도출하기 위해 시나리오 분석을 수행하여야 하는데, 현재까지 진행된 선행연구들에서는 시나리오 분석기법의 기준이 존재하지 않고, 여러 목적에 따라 다르게 정의되고 있다. 시스템에 설계를 위해서 정의되는 운영 시나리오와 안전성 분석을 위해 정의되는 운영 시나리오의 형식 및 구성의 차이로 인하여 비효율적인 시스템의 설계와 안전성 분석을 개선하기 위해 따라서 논리적인 시나리오를 정의하여 효율적으로 두 기법을 연계하는 방법 및 프로세스 모델에 대한 연구가 필요하다.

이에 본 연구는 운영 시나리오 분석에 논리적으로 접근할 수 있는 시나리오 테이블을 제안하며, STPA 안전성 분석 및 시나리오 분석을 효율적으로 연계하는 하나의 새로운 프로세스 모델로 제안하였다. 뿐만 아니라 개선된 시나리오 분석 기법을 통해 기존의 STPA 에서 발생할 수 있는 복잡하고 어려운 Control Structure의 도식화와 UCA 등의 도출에 대해서 시스템의 기초 개념 설계단계에서 정의한 운영 프로세스를 통하여 STPA 안전성 분석의 기반을 마련하고, UCA와 Control Structure 도출의 가이드라인을 제공할 수 있게 되었다. 제안하는 프로세스 모델을 지하공간을 활용한 도시물류 시스템의 핵심장비인 AGV 수평이송장치를 대상으로 시나리오- STPA 연계 분석을 수행하였고, 이를 통하여 안전성 분석을 위해 위험 시나리오를 따로 정의하는 비효율적인 반복 수행에 대해 효율적으로 수행기간을 줄일 수 있으며, 시스템의 개발 전 STPA 안전성 분석에 대한 결과는 시스템을 설계할 때 안전 제약사항으로 반영되어 시스템의 개발 실패를 방지할 수 있을 것으로 사료된다.

## 6. References

[1] Statistics Korea(2023), Population by administrative district (si/gun/gu) and gender. https://kosis.kr/statml/statHtml.do?orgId=101&tblId=DT_1B040A3

[2] B. K. Kim, J. S. Park(2022), In the era of 10 million living logistics in the metropolitan area, a new logistics system needs to be established. Gyounggi Research Institute Research Report.

[3] S. J. Jung, J. S. Moon(2004), Strategies for revitalizing rail freight transport to strengthen logistics competitiveness. The Korea Transport Institute.

[4] J. M. Park, J. U. Kim, Y. M. Kim(2022), "Model-based analysis to improve the safety of urban logistics system using vacant space." Journal of Korea Safety Management & Science, 24(1):1-9.

[5] S. Y. Han, J. H. Kim, T. K. An, W. D. Lee, W. S. Shin(2008), "A development plan for core system of urban transit based on system engineering process." Proceedings of Korean Railroad Society, 2005-2013.

[6] S. H. Park, B. C. Kim(2019), "Quality analysis of the request for proposals of public information systems project: System operational concept." Journal of Information Technology Services, 18(2): 7-54.

[7] S. M. Huh, S. J. Park, S. Y. Park(2007), "Goal and scenario based analysis method for robot system." Proceedings of The Korea Society of Computer and Information, 34(1B):123-128.

[8] Y. S. Baek, S. G. Shin, J. K. Park, H. K. Lee, S. W. Eom, S. W. Cho, J. K. Shin(2021), "A study on the risk analysis and fail-safe verification of autonomous vehicles using V2X based on intersection scenarios." The Journal of the Korea Institute of Intelligent Transportation Systems, 20(6):299-312.

[9] Telecommunications Technology Association(2018), Risk analysis guide using STPA.

[10] N. Y. Choi, B. G. Lee(2019), "Hazard analysis process based on STPA using SysML." Journal of Korean Society for Internet Information, 20(3):1-11.

[11] H. S. Yang, K. H. Kwon(2019), "Identifying causes

of an accident in STPA using the scenario table." Journal of Computing Science and Engineering, 46(8):787-799.

## 저자 소개

**김 명 성**
현 아주대학교 시스템공학과 석사과정.
관심분야 : 모델기반 시스템공학, 신뢰성 공학, 신뢰성 분석 등.
주소 : 경기도 수원시 영통구 월드컵로 206 아주대학교 성호관 244호.

**김 영 민**
현 아주대학교 시스템공학과 교수.
관심분야 : 자율주행자동차 안전 시스템 구축, 첨단 자율 운송 시스템, 첨단 교통시스템 및 스마트시티, 스마트물류체계 구축 등.
주소 : 경기도 수원시 영통구 월드컵로 206 아주대학교 성호관 243호.