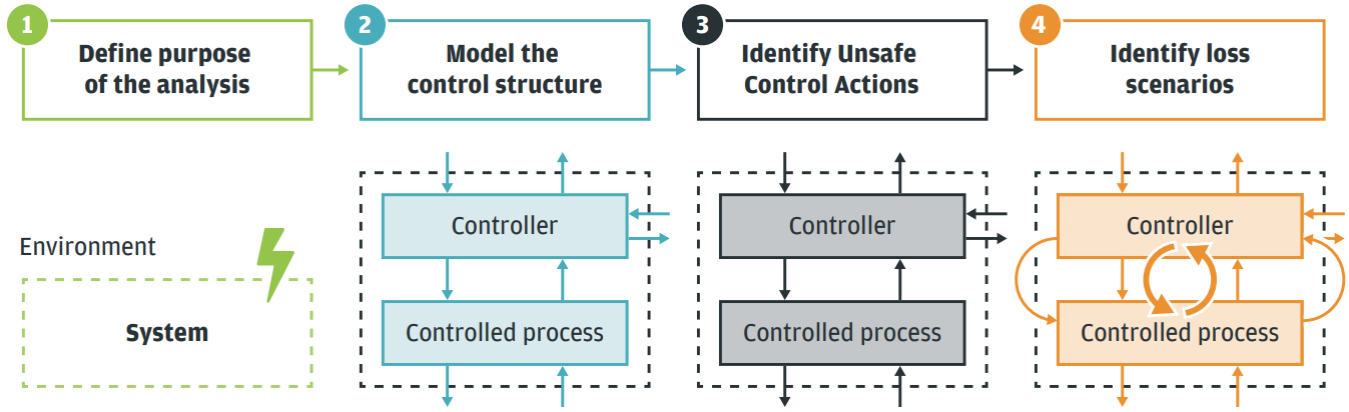
1. STPA (System-Theoretic Process Analysis) 소개

STPA (System-Theoretic Process Analysis)는 소프트웨어 및 시스템 안전 분석 전문가인 MIT Nancy Leveson 교수에 의해서 제안된 안전 분석 기법입니다.

Leveson 교수는 수십 년간의 경험을 통해서 전통적인 안전 분석 기법들이 결함-원인 연쇄(Cause-Effect Chain)의 식별에 집중함으로써 발생하는 한계를 인지하고, 이를 극복하기 위해 결함이 아니라 부정확한 상호작용의 위험을 분석하는 새로운 기법을 제안합니다. 이후 STPA는 다양한 분야에서 널리 적용되고 있으며, 특히 미 SAE에서 자동차 안전분석을 위한 STPA 가이드*가 22년에 발표되었습니다.

STPA 절차



STPA는 위와 같은 절차로 수행됩니다.

1. **분석 목적 수립:** 시스템의 정의와 함께, 손실(Loss), 위험(Hazard) 그리고 위험을 방지하기 위한 안전 제약(Safety Constraints)를 식별합니다.
2. **제어 구조 정의:** 제어와 피드백을 포함하는 계층적인 제어 구조를 정의합니다. 이는 제어 동작(Control Action)과 프로세스 변수(Process Variable)을 포함합니다.
3. **위험 제어 동작 식별:** 제어 동작이 예상되지 않은 특정 상황에서 수행되어 안전 제약을 위반할 수 있는 경우인 위험 제어 동작(UCA: Unsafe Control Action)를 식별합니다.
4. **손실 시나리오 식별**: UCA의 원인을 포함한 손실 시나리오(Loss Scenario)를 도출합니다.

* SAE J3187 - System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems

2. 위험 분석: 위험 제어 동작 식별

위험 제어 동작 (UCA) 분석

STPA는 결함-원인 연쇄의 한계를 극복하기 위해서 제어 동작의 부정확한 상호작용에 집중하는 것이 핵심입니다. 부정확한 상호작용이 특정 상황과 맞물렸을 때 위험을 야기할 수 있습니다. 이를 분석하기 위해서 STPA는 가이드워드(Guideword)에 기반한 UCA 식별 기법을 제안하고 있습니다.

다음은 SCM(Shift Control Module)의 제어 명령 range command에 대해서 네 가지 가이드워드를 사용한 UCA 식별 사례를 보여줍니다.

가이드워드 1. **Not providing**	가이드워드 2. **Providing**	가이드워드 3. **Too Early, Too Late , Wrong Order**	가이드워드 4. **Stopped Too Soon, Applied too long**
[UCA 1] SCM **does not provide range command when ~**	[UCA 2] SCM **provide range command when ~**	[UCA 3] SCM provide **range command too late after when ~**	N/A

UCA는 특정 상황에서 위험하기 때문에 문맥이 특정되어야 합니다. 다음은 문맥을 포함한 UCA 1입니다.

[UCA 1] SCM does not provide range command when driver selects new range.

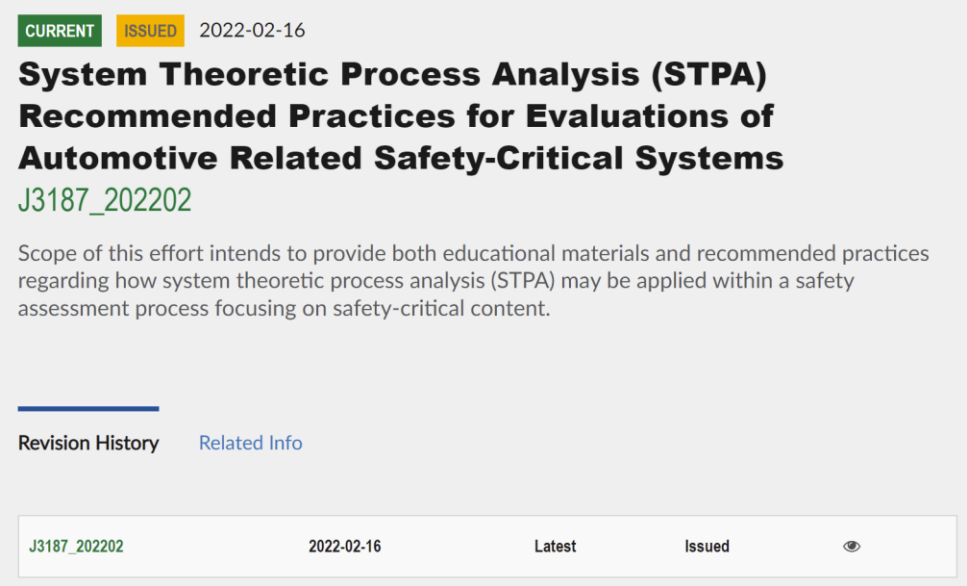
UCA가 식별되면 UCA를 발생시킬 수 있는 다양한 원인들을 식별할 수 있습니다. 다음은 UCA 1에 대한 손실 시나리오의 사례입니다.

Causal Scenario Description
S-1: SCM **does not provide range command because it incorrectly believes no new range was selected.** **S-2:** SCM **does not provide range command because it incorrectly believes the range was already achieved.** **…**

* 참조: Thomas, J., Sgueglia, J., Suo, D., Leveson, N. et al., "An Integrated Approach to Requirements Development and Hazard Analysis," SAE Technical Paper 2015-01-0274

3. SAE J3187 가이드

STPA와 관련된 자동차 분야 표준은 SAE J3187이 있습니다. J3187 표준은 SAE Functional Safety Committee의 승인을 얻어 STPA Task Force에서 진행하고 있으며, 22년 2월에 초판본이 제정되었습니다.


CURRENT ISSUED 2022-02-16

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems

J3187_202202

Scope of this effort intends to provide both educational materials and recommended practices regarding how system theoretic process analysis (STPA) may be applied within a safety assessment process focusing on safety-critical content.

Revision History Related Info

J3187_202202	2022-02-16	Latest	Issued	

SAE J3187은 다음과 같은 노력을 통해서 개발되었습니다.

Working Groups and Topics
Group 1 - Basic STPA, Recommended Practices, Lessons Learned
Group 2 - SOTIF and STPA
Group 2 - HMI and STPA
Group 2 - MBSE and STPA
Group 3 - High Level Use of STPA within Safety Process & STPA with Other Safety Evaluation Methods
Examples - Aerospace, Automotive, Automotive HMI, MBSE, SOTIF
Glossary

Source: Standards Presentations and Group Discussion, MIT STAMP Workshop 2019

* 참가 조직(23):
Nissan, FCA, Ford, GM, Toyota, Mercedes-Benz USA, Rolls Royse, Jaguar Land Rover, Continental (Germany), Magna Electronics Inc., Zenuity, Waymo, Renesas (Univ of Waterloo), WMG – Univ Warwick, Edge Case Research, Embraer, NVIDIA, APTIV, SAE ORAD Working Group, SAE Members, VOLPE (US Depart of Transportations)