STPA Step 1: Losses, Hazards, and Constraints for Commercial Airliner System

System Safety Analysis Team

September 19, 2024

Table of Contents

Introduction

This document presents the results of Step 1 of the System-Theoretic Process Analysis (STPA) for a next-generation commercial airliner system. It identifies the potential losses, system-level hazards, and system-level constraints based on the Concept of Operations (ConOps) document.

Losses

The following losses have been identified for the commercial airliner system:

ID	Description
L-1	Loss of human life or serious injury to passengers, crew, or ground personnel
L-2	Damage to or loss of the aircraft
L-3	Damage to property or environment on the ground
L-4	Significant economic losses for the airline or other stakeholders
L-5	Loss of public trust in air travel safety

System-Level Hazards

The following system-level hazards have been identified:

ID	Hazard Description	Associated Losses
H-1	Aircraft violates minimum separation standards with other aircraft, terrain, or obstacles	L-1, L-2, L-3, L-4, L-5
H-2	Aircraft deviates from safe flight envelope (e.g., stall, overspeed, structural limits exceeded)	L-1, L-2, L-4, L-5
H-3	Aircraft enters prohibited or restricted airspace	L-1, L-2, L-3, L-4, L-5
H-4	Passengers or crew are exposed to harmful environmental conditions (e.g., depressurization, extreme temperatures, toxic substances)	L-1, L-4, L-5
H-5	Aircraft is not in a controllable state during critical phases of flight (e.g., takeoff, landing, severe weather)	L-1, L-2, L-3, L-4, L-5
H-6	Aircraft is unable to complete its intended flight plan safely	L-1, L-2, L-4, L-5
H-7	Aircraft poses a danger to ground personnel or equipment during ground operations	L-1, L-3, L-4, L-5

System-Level Constraints

The following system-level constraints have been defined to prevent the identified hazards:

ID	Constraint Description	Related Hazard
SC-1	The aircraft must maintain minimum separation standards with other aircraft, terrain, and obstacles at all times	H-1
SC-2	The aircraft must operate within its safe flight envelope under all operational conditions	H-2
SC-3	The aircraft must avoid entering prohibited or restricted airspace unless specifically authorized	H-3

ID	Constraint Description	Related Hazard
SC-4	The aircraft must maintain a safe and habitable environment for passengers and crew throughout the flight	H-4
SC-5	The aircraft must remain in a controllable state during all phases of flight, including critical phases and severe weather conditions	H-5
SC-6	The aircraft must have sufficient capabilities and redundancies to safely complete its intended flight plan or divert to an alternate destination when necessary	H-6
SC-7	Ground operations involving the aircraft must be conducted in a manner that ensures the safety of ground personnel and equipment	H-7

Conclusion

This document presents the results of STPA Step 1 for the commercial airliner system, including identified losses, system-level hazards, and system-level constraints. These elements form the foundation for further analysis in subsequent STPA steps, such as identifying unsafe control actions and causal scenarios.

The analysis adheres to STPA best practices by:

1. Focusing on system-level hazards rather than component failures or causes
2. Avoiding ambiguous or recursive wording in hazard descriptions
3. Maintaining a manageable number of system-level hazards
4. Linking hazards to potential losses and constraints to hazards

This document will serve as a reference for system engineers, safety analysts, and other stakeholders involved in the development and operation of the next-generation commercial airliner system.