# STPA Analysis Report of Airport Traffic Control System (ATCS)

Date: December 24, 2024

Generated by: SafeChatbot

Prepared by: Asim Abdulkhaleq

# System Identification

Description: The Airport Traffic Control System (ATCS) is a critical safety and efficiency subsystem designed to manage and coordinate the movement of aircraft and ground vehicles within an airport's airside operations. The system ensures safe and efficient flow by preventing collisions, managing traffic congestion, and optimizing resource utilization. It operates through the integration of multiple components, including sensors, communication systems, controllers, and actuators.  
  
\*\*System Scope and Definition:\*\* The ATCS encompasses all activities related to the safe and efficient movement of aircraft and vehicles within the airport's operational area. This includes managing taxiing, takeoffs, landings, and all ground movements. The ATCS integrates real-time data from various sources to provide controllers with the information needed to make informed decisions and issue timely commands.  
  
\*\*Key Components and their Roles:\*\*  
  
1. \*\*Human Controller - Air Traffic Controller (ATC):\*\*  
 \* \*\*Functionality:\*\* Oversees aircraft in the vicinity of the airport, manages landing and takeoff sequences, and monitors airspace traffic. They make critical decisions based on the information from the system.  
 \* \*\*Key Features:\*\* Real-time monitoring of air traffic, strategic decision-making for flight path management, and direct communication with pilots.  
 \* \*\*Connections:\*\* Receives data from radar and surveillance sensors, communicates directly with pilots via communication systems, issues control actions to Ground Control Unit (GCU).  
 \* \*\*Example:\*\* A controller instructs a pilot to change altitude or heading to maintain safe separation from other aircraft.  
  
2. \*\*Human Controller - Ground Controller (GC):\*\*  
 \* \*\*Functionality:\*\* Manages the movement of aircraft and vehicles on taxiways, aprons, and runways. They coordinate ground traffic to ensure efficient and safe movement on the ground.  
 \* \*\*Key Features:\*\* Real-time monitoring of ground traffic, strategic decision-making for ground movement, and direct communication with vehicle operators.  
 \* \*\*Connections:\*\* Receives data from radar and surveillance sensors, communicates with vehicle operators via communication systems, issues control actions to lighting systems and automated gates.  
 \* \*\*Example:\*\* A controller instructs a pushback vehicle to clear the apron so an aircraft can exit its gate.  
  
3. \*\*Automated Controller - Ground Control Unit (GCU):\*\*  
 \* \*\*Functionality:\*\* An automated system that processes sensor data, identifies aircraft and vehicle positions, and assists ground controllers in decision-making by sending control commands to actuators.  
 \* \*\*Key Features:\*\* Real-time data processing, conflict detection, and automated route planning.  
 \* \*\*Connections:\*\* Receives data from radar and surveillance sensors, sends control commands to actuators and receives control actions from the ATC.  
 \* \*\*Example:\*\* Automatically adjust lighting system on the taxiway to guide the aircraft to a designated parking area.  
  
4. \*\*Sensors - Radar and Surveillance Sensors:\*\*  
 \* \*\*Functionality:\*\* Detects the position, speed, and trajectory of aircraft and ground vehicles.  
 \* \*\*Key Features:\*\* Real-time tracking, accuracy in measurements, and integration with data processing systems.  
 \* \*\*Connections:\*\* Provides data to the Ground Control Unit (GCU) and Human Controller (Air Traffic Controller).  
 \* \*\*Example:\*\* Radar detects a vehicle entering a taxiway without clearance, triggering an alert in the system.  
  
5. \*\*Actuators - Lighting Systems, Automated Gates, and Warning Systems:\*\*  
 \* \*\*Functionality:\*\* Directs and alerts operators by activating lights, opening/closing gates, and sounding alarms.  
 \* \*\*Key Features:\*\* Automated control based on signals, and reliable physical action, and ensures that all commands are carried out accurately  
 \* \*\*Connections:\*\* Receives control commands from the Ground Control Unit (GCU).   
 \* \*\*Example:\*\* Runway lights activate to guide an aircraft during takeoff.  
  
6. \*\*Controlled Process - Airport Airside Operations (including Aircraft, Ground Vehicles and the HMI):\*\*  
 \* \*\*Functionality:\*\* Represents the overall movement of aircraft and vehicles within the airport operational area, and the HMI.   
 \* \*\*Key Features:\*\* Dynamic environment with moving objects, requiring precise and coordinated control.  
 \* \*\*Connections:\*\* Receives commands from actuators, provides data to sensors.  
 \* \*\*Example:\*\* All movements of aircraft and vehicles including the HMI information displayed on the controllers screens.  
  
7. \*\*Communication Systems\*\*  
 \* \*\*Functionality:\*\* Enables real-time information exchange between controllers, pilots, and ground operators, as well as between system components.  
 \* \*\*Key Features:\*\* Reliable and clear audio and data transmission, and seamless integration with the overall system.  
 \* \*\*Connections:\*\* Facilitates the communication between controllers, pilots, and the ground operators.  
 \* \*\*Example:\*\* A ground controller sends a message to a pilot to proceed to a holding point via radio communication.  
  
\*\*Operations:\*\* The ATCS continuously monitors the airport environment, gathering data from radar, sensors, and communication inputs. Ground controllers use this data to direct aircraft and vehicles on the ground, while the air traffic control tower manages airside movements. Commands are issued via communication systems to pilots and ground operators, ensuring adherence to safety protocols and efficient operations.  
  
\*\*Safety Objectives:\*\*  
\* \*\*Prevent Collisions:\*\* Avoid aircraft-to-aircraft, aircraft-to-vehicle, and vehicle-to-vehicle collisions.  
\* \*\*Minimize Delays:\*\* Optimize traffic flow to reduce congestion and ensure timely operations.  
\* \*\*Enhance Situational Awareness:\*\* Provide real-time information to controllers and operators for informed decision-making.  
\* \*\*Facilitate Emergency Responses:\*\* Ensure the system can adapt quickly to emergencies, such as runway incursions or technical failures.

Boundary: The system boundary includes all components and interactions within the airport's airside operational area including the Air Traffic Controller, Ground Controller, Ground Control Unit (GCU), Radar and Surveillance Sensors, Lighting Systems, Automated Gates, Warning Systems, Aircraft, Ground Vehicles, Communication Systems, and the Human Machine Interface(HMI). It also includes external entities such as pilots and ground operators that interact with the system through communication systems and controlled processes.

# Purpose

The purpose of the analysis is to identify potential safety hazards and unsafe control actions within the Airport Traffic Control System (ATCS) to ensure safe and efficient airside operations, including preventing collisions and managing traffic flow. This analysis aims to reduce the risk of accidents, and improve the overall reliability and performance of the ATCS.

# System Goals

* Ensure safe and efficient airside operations
* Prevent collisions between aircraft, vehicles, and other ground objects
* Minimize traffic congestion and delays
* Maintain optimal resource utilization
* Provide controllers with real-time and accurate information
* Ensure the system can adapt quickly to emergencies

# Accidents

|  |  |
| --- | --- |
| id | description |
| A1 | Collision between aircraft on the ground or in the air. |
| A2 | Collision between aircraft and ground vehicles. |
| A3 | Runway incursion by vehicles or aircraft. |
| A4 | Loss of human life or injury due to system failure. |
| A5 | Damage to aircraft or airport infrastructure due to system malfunction. |
| A6 | Significant delays or disruptions in airport operations. |

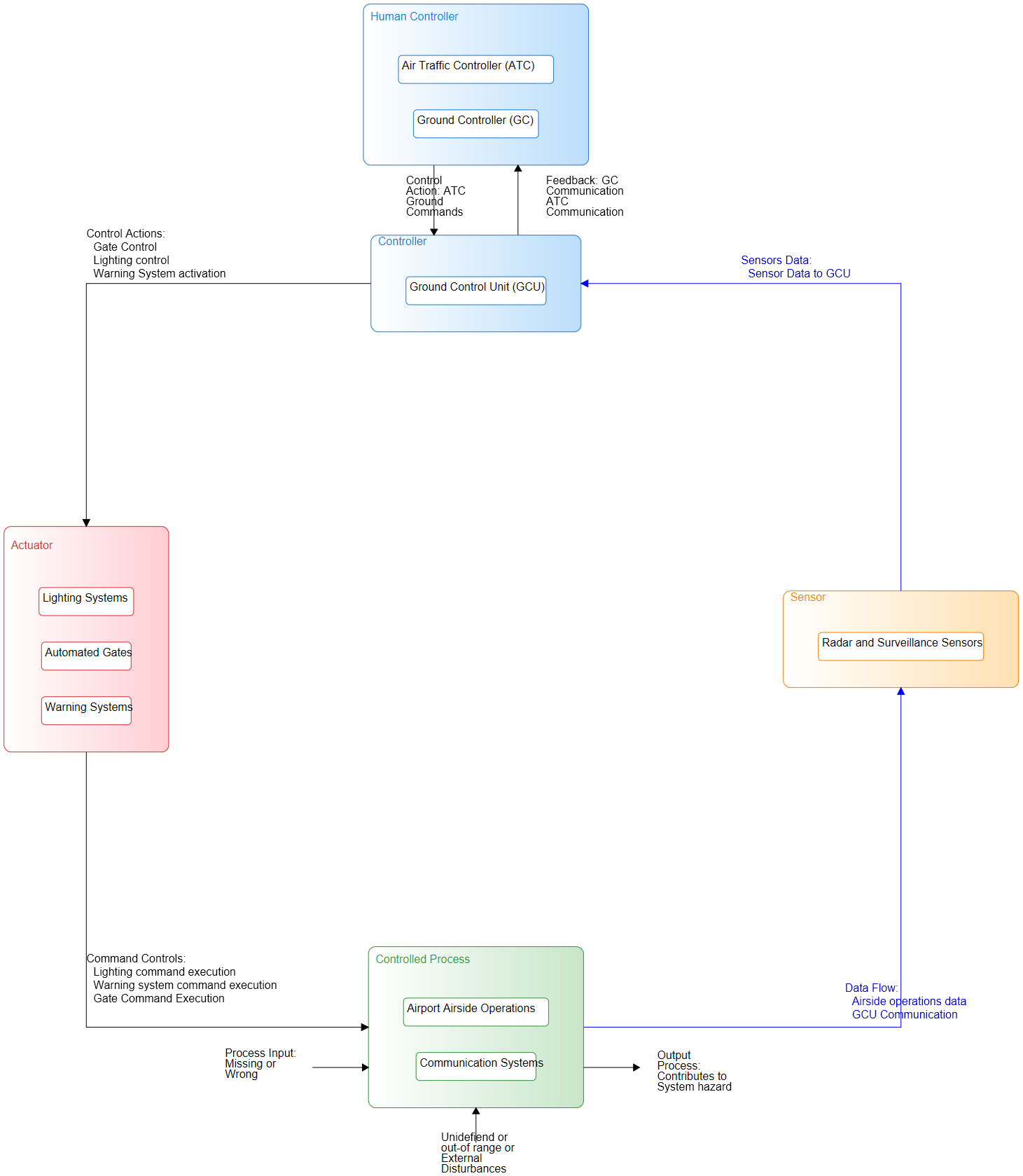
# Hazards

|  |  |  |
| --- | --- | --- |
| id | description | linked\_accidents |
| H1 | Aircraft or ground vehicle exceeds minimum separation distance with other objects on the ground or in the air. | ['A1', 'A2', 'A3', 'A4', 'A5', 'A6'] |
| H2 | Unauthorized access of aircraft or vehicle into active runway or taxiway. | ['A1', 'A2', 'A3', 'A4', 'A5', 'A6'] |
| H3 | Incorrect control action during critical phases of operation (takeoff, landing, taxiing). | ['A1', 'A2', 'A3', 'A4', 'A5', 'A6'] |
| H4 | Failure of communication systems leading to loss of situational awareness. | ['A1', 'A2', 'A3', 'A4', 'A5', 'A6'] |
| H5 | Failure of actuators leading to unsafe states | ['A1', 'A2', 'A3', 'A4', 'A5', 'A6'] |
| H6 | Failure of Sensors leading to incorrect states for controllers | ['A1', 'A2', 'A3', 'A4', 'A5', 'A6'] |

# System Constraints

|  |  |  |
| --- | --- | --- |
| id | description | linked\_Hazard |
| SC\_1 | If aircraft or ground vehicle violate minimum separation, the violation must be detected, and measures taken to prevent collision | ['H1'] |
| SC\_2 | If an unauthorized access of aircraft or vehicle into active runway or taxiway is detected, the violation must be detected and warning systems activated to prevent runway incursion and collision | ['H2'] |
| SC\_3 | If incorrect control action during critical phases of operation detected, the system must have fail-safe mechanisms to avoid accidents | ['H3'] |
| SC\_4 | If the communication system fails, the controllers must have redundant and fail-safe alternative method of communication | ['H4'] |
| SC\_5 | If actuators failure occurs, the system must have fail-safe modes | ['H5'] |
| SC\_6 | If Sensors failure occurs, the system must have fail-safe modes | ['H6'] |

# Control Structure



## Components

|  |  |
| --- | --- |
| name | type |
| Air Traffic Controller (ATC) | Human Controller |
| Ground Controller (GC) | Human Controller |
| Ground Control Unit (GCU) | Controller |
| Radar and Surveillance Sensors | Sensor |
| Lighting Systems | Actuator |
| Automated Gates | Actuator |
| Warning Systems | Actuator |
| Airport Airside Operations | Controlled Process |
| Communication Systems | Controlled Process |

## Connections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| label | source | target | description | connection\_type |
| control action to GCU | Air Traffic Controller (ATC) | Ground Control Unit (GCU) | Air Traffic Controller sends control actions to ground control unit to control the lighting systems |  |
| Control Action | Ground Controller (GC) | Lighting Systems | Control action to control the lighting systems |  |
| Control Action | Ground Controller (GC) | Automated Gates | Control action to control the Automated gates |  |
| Control Action | Ground Controller (GC) | Warning Systems | Control action to control the warning systems |  |
| Control command to lighting system | Ground Control Unit (GCU) | Lighting Systems | Control command from GCU to the Lighting system |  |
| Control command to Automated gates | Ground Control Unit (GCU) | Automated Gates | Control command from GCU to the automated gates |  |
| Control command to warning system | Ground Control Unit (GCU) | Warning Systems | Control command from GCU to the warning system |  |
| sensor data to GCU | Radar and Surveillance Sensors | Ground Control Unit (GCU) | Sensor data sent to the GCU for monitoring and control |  |
| Data from sensor to ATC | Radar and Surveillance Sensors | Air Traffic Controller (ATC) | data flow from sensor to Air Traffic Controller for monitoring and control |  |
| Data from sensor to GC | Radar and Surveillance Sensors | Ground Controller (GC) | data flow from sensor to Ground Controller for monitoring and control |  |
| Data from Airport airside to Sensor | Airport Airside Operations | Radar and Surveillance Sensors | Data flow from airport airside operations to the radar and surveillance sensors |  |
| data from operations to communitcation systems | Airport Airside Operations | Communication Systems | Data flow from Airport Airside Operations to Communication systems |  |
| Data from communitcation systems to operations | Communication Systems | Airport Airside Operations | Data flow from Communication systems to Airport Airside Operations |  |

# Unsafe Control Actions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Control Action** | **Not providing causes hazard** | **Providing causes hazard** | **Too early, too late, out of order** | **Stopped too soon, applied too long** |
| *1* | *Control action to GCU* | UCA\_1: ATC does not provide correct control action to GCU leading to wrong control command being sent to actuators during landing approach, potentially causing a collision. | UCA\_2: ATC provides incorrect control action to GCU causing wrong control command being sent to actuators and leading to runway incursion | UCA\_3: ATC provides control actions to GCU too late or out of order, causing a conflict in the airport airside operations |  |
| *UCA\_1: ['H1', 'H2', 'H3']* | *UCA\_2: ['H2', 'H3', 'H5']* | *UCA\_3: ['H1', 'H3', 'H4', 'H5']* |  |
| *2* | *Control Action to Lighting System* | UCA\_4: GC does not issue control action to activate the lighting system when aircraft is taxiing on the runaway, causing the aircraft to get lost or collide with other objects. | UCA\_5: GC issues control action to activate lighting system when there is no aircraft on the runaway causing confusion to other operators and possible collision | UCA\_6: GC activates the lighting system too early or too late during the aircraft landing or takeoff causing possible collisions |  |
| *UCA\_4: ['H1', 'H2']* | *UCA\_5: ['H2', 'H3', 'H5']* | *UCA\_6: ['H1', 'H3', 'H5']* |  |
| *3* | *Control Action to Automated Gates* | UCA\_7: GC does not issue control action to open the gates at the gate area when aircraft is pushing back causing possible collisions or damage | UCA\_8: GC issues control action to open gates unintentionally causing unauthorized access of vehicles to restricted areas | UCA\_9: GC opens the automated gates too early or too late leading to collision between aircraft or vehicles |  |
| *UCA\_7: ['H1', 'H2']* | *UCA\_8: ['H2', 'H3']* | *UCA\_9: ['H1', 'H3', 'H5']* |  |
| *4* | *Control Action to Warning Systems* | UCA\_10: GC does not activate the warning systems during runway incursions or any other system failures leading to possible accidents | UCA\_11: GC activates the warning system without any system failure or incursions causing confusion to the operators | UCA\_12: GC activates the warning systems at the wrong time (too early, or too late) leading to possible collisions |  |
| *UCA\_10: ['H1', 'H2', 'H4', 'H5']* | *UCA\_11: ['H3', 'H4', 'H5']* | *UCA\_12: ['H1', 'H3', 'H5']* |  |

# Controller Constraints

|  |  |  |
| --- | --- | --- |
| id | controller constrain | Linked Unsafe control\_action |
| C\_1 | ATC must provide the correct control action to GCU during landing approach to prevent collision | ['UCA\_1'] |
| C\_2 | ATC must not issue any wrong control action to GCU that may lead to runway incursion | ['UCA\_2'] |
| C\_3 | ATC must provide control action to GCU at the right time to prevent conflict in airport airside operations | ['UCA\_3'] |
| C\_4 | GC must always provide control action to activate lighting system when aircraft is taxiing on the runaway | ['UCA\_4'] |
| C\_5 | GC must not issue the control action to activate the lighting system when there is no aircraft on the runway to prevent confusions | ['UCA\_5'] |
| C\_6 | GC must activate the lighting system at the correct time to prevent collisions | ['UCA\_6'] |
| C\_7 | GC must provide control action to open the automated gates when aircraft is pushing back from gates to prevent collisions | ['UCA\_7'] |
| C\_8 | GC must not open the automated gates unintentioanlly to prevent unathorized access to restricted areas | ['UCA\_8'] |
| C\_9 | GC must open automated gates at the correct time to prevent collisions | ['UCA\_9'] |
| C\_10 | GC must activate the warning system whenever a system failure or runway incursion is detected | ['UCA\_10'] |
| C\_11 | GC must not activate warning system unneccesarily without any system failures or incursion to avoid confusion | ['UCA\_11'] |
| C\_12 | GC must activate the warning systems at the right time to prevent collisions | ['UCA\_12'] |

# Loss Scenarios

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| id | uca | Linked Unsafe control\_action | type | scenario |
| L\_S\_1 | Control action to GCU | ['UCA\_1'] | Controller Failure | ATC experiences a system failure, causing the inability to provide correct control actions to GCU during landing approach resulting in wrong control actions being sent and causing potential collisions |
| L\_S\_2 | Control action to GCU | ['UCA\_2'] | Controller Error | ATC provides the incorrect control action to GCU leading to a wrong control command being sent to the actuators which leads to a runway incursion. |
| L\_S\_3 | Control action to GCU | ['UCA\_3'] | Timing Issue | ATC provides control actions to GCU too late or out of order due to high workload or miscommunication leading to conflict in airside operations |
| L\_S\_4 | Control Action to Lighting System | ['UCA\_4'] | Controller Error | GC fails to provide control action to activate the lighting systems due to a sudden power outage resulting in an aircraft getting lost or colliding with an object on the runway. |
| L\_S\_5 | Control Action to Lighting System | ['UCA\_5'] | Controller Error | GC issues control action to activate lighting system when there is no aircraft on the runway due to incorrect feedback data, causing confusion to operators and possible collisions |
| L\_S\_6 | Control Action to Lighting System | ['UCA\_6'] | Timing Issues | GC activates the lighting system too early or too late during the aircraft landing or takeoff due to flawed control algorithm causing possible collisions |
| L\_S\_7 | Control Action to Automated Gates | ['UCA\_7'] | Controller error | GC does not issue a control action to open the automated gates at the gate area when the aircraft is pushing back due to miscommunication causing a collision or damage. |
| L\_S\_8 | Control Action to Automated Gates | ['UCA\_8'] | Controller Error | GC provides an incorrect control action to open gates due to sensor failure causing unauthorized access of vehicles to restricted area. |
| L\_S\_9 | Control Action to Automated Gates | ['UCA\_9'] | Timing Issue | GC opens the automated gates too early or too late due to system lag or external interference leading to collision between aircraft or vehicles |
| L\_S\_10 | Control Action to Warning Systems | ['UCA\_10'] | Controller error | GC fails to activate the warning system during a runway incursion due to a hardware malfunction leading to potential accidents |
| L\_S\_11 | Control Action to Warning Systems | ['UCA\_11'] | Controller Error | GC activates the warning system without any system failure or incursion due to human error causing confusion to the operators |
| L\_S\_12 | Control Action to Warning Systems | ['UCA\_12'] | Timing issue | GC activates the warning system at the wrong time due to incorrect sensor data or system lag resulting in collisions |

# Safety Constraints

|  |  |  |
| --- | --- | --- |
| id | Safety constraint | Linked\_loss\_scenarios |
| S\_C\_1 | The system must have a mechanism in place to ensure the ATC control action to GCU is always correct and precise during landing approaches to prevent collision | ['L\_S\_1'] |
| S\_C\_2 | The system should implement checks and balances to prevent ATC from providing wrong control action to GCU causing runway incursion | ['L\_S\_2'] |
| S\_C\_3 | System must ensure control actions from ATC are provided to GCU at the correct time to prevent conflict in airside operations | ['L\_S\_3'] |
| S\_C\_4 | The system must have a backup power source for lighting system activation, to ensure lighting is always activated when aircraft is taxiing. | ['L\_S\_4'] |
| S\_C\_5 | The system must have sensor checks and validation to ensure GC activates the lighting system only when aircraft are on the runway to avoid confusion | ['L\_S\_5'] |
| S\_C\_6 | The GC must activate the lighting system at the correct time during landing and takeoff to avoid any possible collision | ['L\_S\_6'] |
| S\_C\_7 | The system must ensure the automated gate controller receives correct control action from GC when aircraft is pushing back to avoid any collisions | ['L\_S\_7'] |
| S\_C\_8 | The system should use multiple validations to prevent GC from providing incorrect control action to open gates and prevent unauthorized access | ['L\_S\_8'] |
| S\_C\_9 | The system must have a built in time check to prevent gates from opening too early or too late to prevent collisions | ['L\_S\_9'] |
| S\_C\_10 | The system must be equipped with automatic warning system activated by sensor and controller when a runway incursion is detected by the system to avoid any accidents | ['L\_S\_10'] |
| S\_C\_11 | The system must validate the status before the warning system is activated to avoid any confusion caused by human error | ['L\_S\_11'] |
| S\_C\_12 | The system must activate the warning system at the correct time according to sensor information to avoid collision and confusions | ['L\_S\_12'] |