Hazard Analysis and Risk Assessment

The HARA consists of the following steps:

Assumptions

Assumptions are created on how terminology is used and about the environment the product is in.

For this project, an example assumption is that the primary obstacles to be avoided will be stationary furniture and walls along with the users of the drones in the testing room.

Existing External Mitigating Measures

These are risk reducing factors that are already present in an environment. They exist independently of the systems.

For this project, to prevent the drone from hitting people, the only person(s) that can be present in the testing room are the drone operators. This mitigating measure is not in any drone control systems.

Operational Situations

These are the scenarios that the designers expect their product to be in regularly while it is operating, active, or in use. The designers will come up with 'Considered Situational Attributes' which are guide words that describe 'motion', 'mode', 'obstacle exposure', and 'control'.

Guide words

In Functional Safety, guide words are created to produce operational scenarios. For this project some of our guide words were as follows: Mode = Launched, Motion = Forward, Control = Independent (not in swarm configuration), Obstacle Exposure = 'Static'. An example operational scenario is 'a single independent drone is launched and in a forward motion surveying a space with static objects.'

Hazard List

List of potential hazards and their type pulled from a list in the ISO12100 standard. Relevant Mechanical Hazards for the project include:

- Impact due to collision with stationary object
- Impact due to collision with moving object

Hazardous Operation

Hazardous Operation combines Tasks and Functions along with suggested guidewords pulled from the SAEJ2980 standard to create potential resulting malfunctions. The resulting malfunctions constitute Hazardous Operation.

In this project, when the 'Automated drone(s) is exploring' an environment 'as intended', there is hazard exposure do to obstacles that are present in the environment. The resulting malfunction is an errant flight path if a collision occurs.

Hazardous Events

Hazardous events combine Hazardous Operation and Operational Situation to describe the Hazardous Event that needs to be mitigated.

In this project when the ‘Automated drone(s) is exploring’ an environment ‘as intended’, and there is hazard exposure due to obstacles that are present in the environment while ‘a single independent drone is launched and in a forward motion surveying a space with static objects’, the hazardous event is that the drone or operator is at risk of being hit by the drone should a malfunction occur because of the collision.

Risk Reduction Measure

These are the safety features, which could either be design based or policy/procedural based, that are implemented to reduce the HARA line item to a lower risk rating per the ASIL risk rating chart.

For this project, we utilized the Tello Mission Pads to constrain the drone to an airspace, and built a netted cage for redundancy, as the basis for collision-based Risk Reduction Measures that lowered our SIL1 rating down to SIL0.