Comprehensive Definitions of Safety Issues

A. Navigation Subsystem

Its basic requirement is to provide the data about the relative position and velocity between receivers and tankers to facilitate docking. The closer the receiver approaches the tanker, the higher the precision requirement of a navigation subsystem should be. Current sensors such as Global Navigation Satellites (GPS), cameras, radar and electro-optical (laser) are often used. Their signals are fused with the inertial navigation system to generate the relative position and velocity. The subsystem has three transitions.

1) **Navigation_suspension**: Precision can fulfill the basic requirement of the navigation subsystem, but it is degrading to surpass a specified threshold. The reasons are multiple, such as bad weather for cameras, radars & lasers; multi-path effects, hostile jamming and spoofing for GPS.
2) **Navigation_recover**: Precision quality exceeds a specified threshold, and the Navigation subsystem is healthy again.
3) **Navigation_breakdown**: The *minor damage* state has lasted more than a given threshold or the data provided do not fulfill the basic requirement of the navigation subsystem.

B. Control Subsystem

Its basic requirement is to keep the receiver's position and velocity within an allowable range according to its current AAR mode, to avoid collision with other aircraft and achieve the successful docking. The closer the receiver approaches the tanker, the higher the precision requirement should have. This subsystem can be implemented by different control laws such as linear quadratic regulators and nonlinear control laws. The subsystem has three transitions:

1) **Control_suspension**: The estimated position or velocity exceeds the allowable range, or the control error is out of the ability of controllers. This may result from atmospheric turbulence, measurement noise, and control surface failure, etc.
2) **Control_recover**: The estimated position and velocity return to the allowable range, and the control error is decreased below a specified threshold.
3) **Control_breakdown**: The *minor damage* state has lasted more than a given threshold or the receiver has collided with other aircrafts.

C.FUEL SUBSYSTEM

Its basic requirement is to provide the necessary fuel for flight. Slightly different from the holon given in Figure 1(a), there is no "recover" transition and this holon is shown in Figure 1(b).

1) **Fuel_suspension**: The fuel is insufficient for AAR tasks. For safety consideration, the receiver is supposed to abandon the current AAR task and return to the airbase.
2) **Fuel_breakdown**: The fuel is insufficient for returning to the airbase. For safety consideration, the receiver is supposed to make an emergency landing.

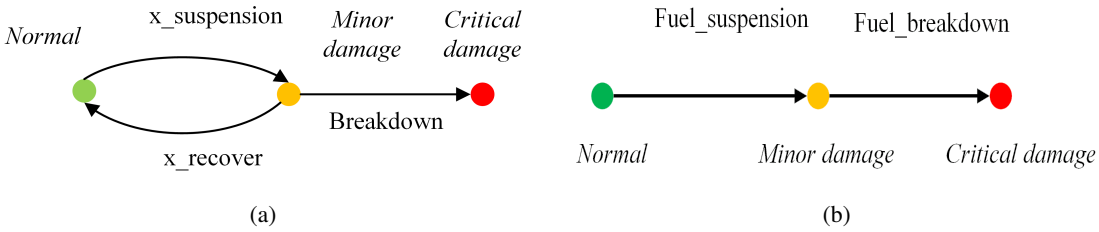


Fig. 1: (a) The general holon (b) The fuel holon

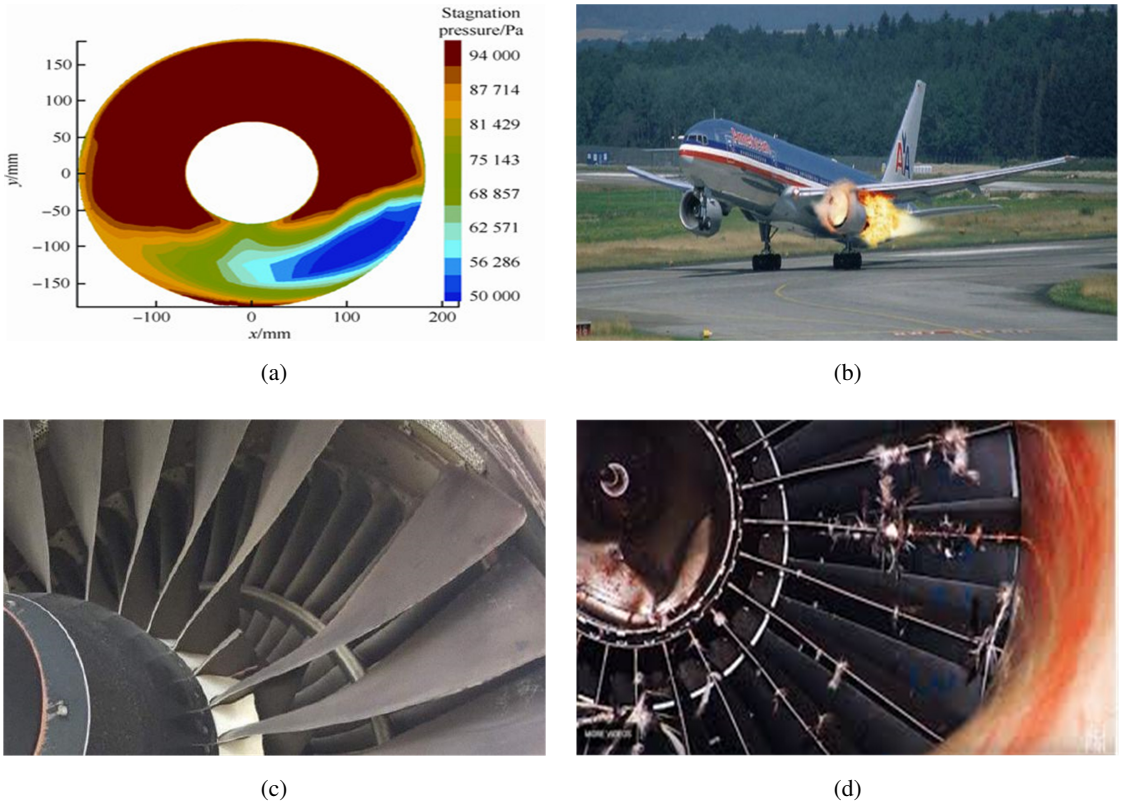
D.ENGINE SUBSYSTEM

Its basic requirement is to provide the necessary power and thrust for flight. The system transitions are given as follows.

1) **Engine_suspension**: The engine power is decreased below a specified threshold. The reasons may be compressor surge, flow distortion and shaft overrun, etc.
2) **Engine_recover**: The engine power returns to the normal level.
3) **Engine_breakdown**: The *minor damage* state has lasted more than a given threshold or severe damage happens, such as engine flame caused by surge, blade missing and accidental inhalation of foreign objects like birds and drogue&probe wreckages.

E.DROGUE&PROBE SUBSYSTEM

Its basic requirement is to establish a robust contact between the drogue and probe, and then transfer fuel from the tanker to the receiver. This subsystem mainly consists three parts: the drogue, the hose, and the Hose Drum Unit (HDU). It is not uncommon for the drogue to make contact with, and occasionally cause damage to the receiver. These common failures are summarized in the three transitions.



(a) (b)

(c) (d)

Fig. 2: Common engine failures (a)Engine flow distortion, (b) Engine flame caused by surge, (c) Blade missing, (4) Engine inhalation of birds.

1) **Drogue&probe_suspension**: This transition includes fuel leakage resulting from unstable contact, hose wave whipping, and entanglement resulting from atmospheric turbulence or excessive relative velocity.
2) **Drogue&probe_recover**: The probe disconnects with the drogue, and this whole subsystem still remains the ability to carry on another contact.
3) **Drogue&probe_breakdown**: The *minor damage* state has lasted more than a given threshold, the drogue or probe is damaged, the hose is dropping off, etc.

F.DATALINK SUBSYSTEM

Its basic requirement is to exchange data for communication and the high-accuracy computation of relative locations. The closer the receiver approaches the tanker, the less the transmission delay, data dithering and package loss rate should have. The subsystems' transitions are similar to those of navigation subsystem.

1) **Datalink_suspension**: Communication quality can still fulfill the basic requirement of the datalink subsystem, but it suffers from delay, dithering and package loss, etc. The

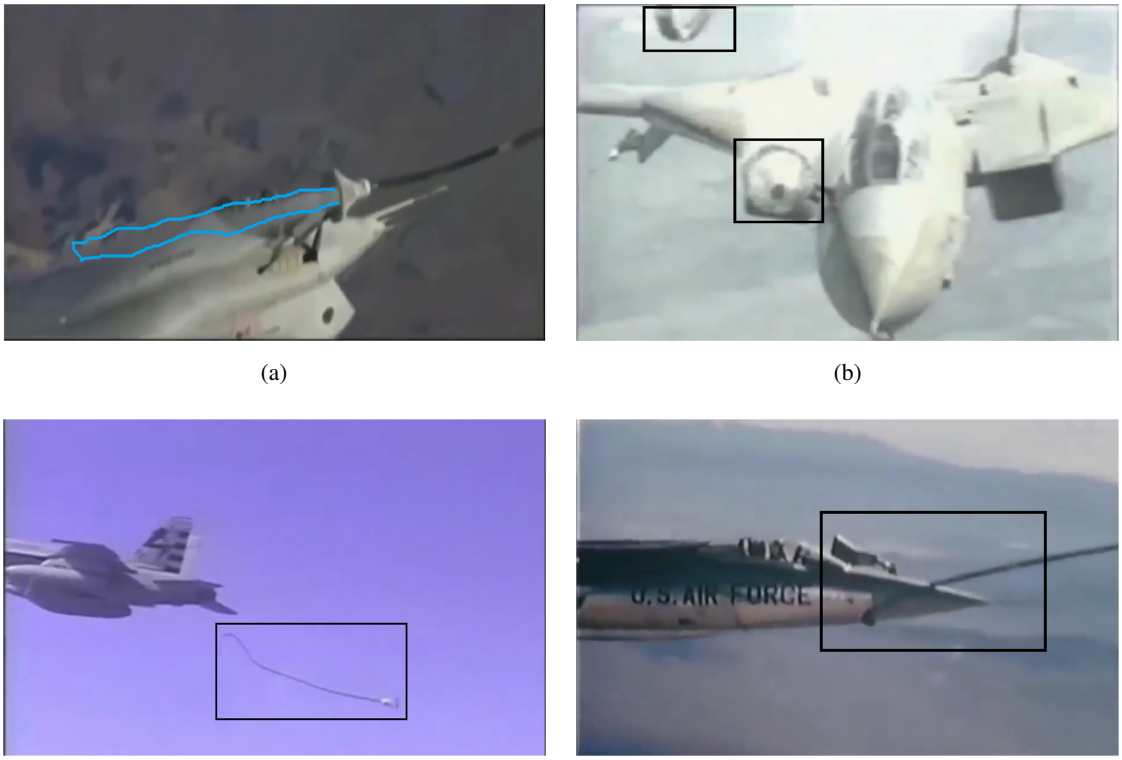


Fig. 3: Common drogue&probe failures (a)Fuel leakage, (b) Drogue breakaway, (c) Hose dropping off, (d) Hose entanglement.

reasons are multiple, such as hostile signal jamming, spoofing and bad weather like thunderstorms.

2) **Datalink_recover**: Communication quality exceeds a specified threshold.
3) **Datalink_breakdown**:The *minor damage* state has lasted more than a given threshold or the data provided can not fulfill the basic requirement of the datalink subsystem.

G.TANKERSAFETY SUBSYSTEM

The tanker's health conditions are also important to the success of AAR. Since it is similar to the receiver and for simplicity, the tanker is modeled as a whole using the holon shown in 1(a), and names it after *Tanker safety subsystem*. Its basic requirement is to facilitate the stable connection and transfer the fuel. The state transitions are given as follows.

1) **Tankersafety_suspension**: Any of the tanker's navigation, control and engine subsystems is at *minor damage* state.
2) **Tankersafety_recover**: All of the subsystems are at *normal* state.

3) **Tankersafety_breakdown**: The fuel would be not enough for the tanker to return to the airbase after a successful AAR or any of the tanker's navigation, control and engine subsystems is in *critical damage* state.