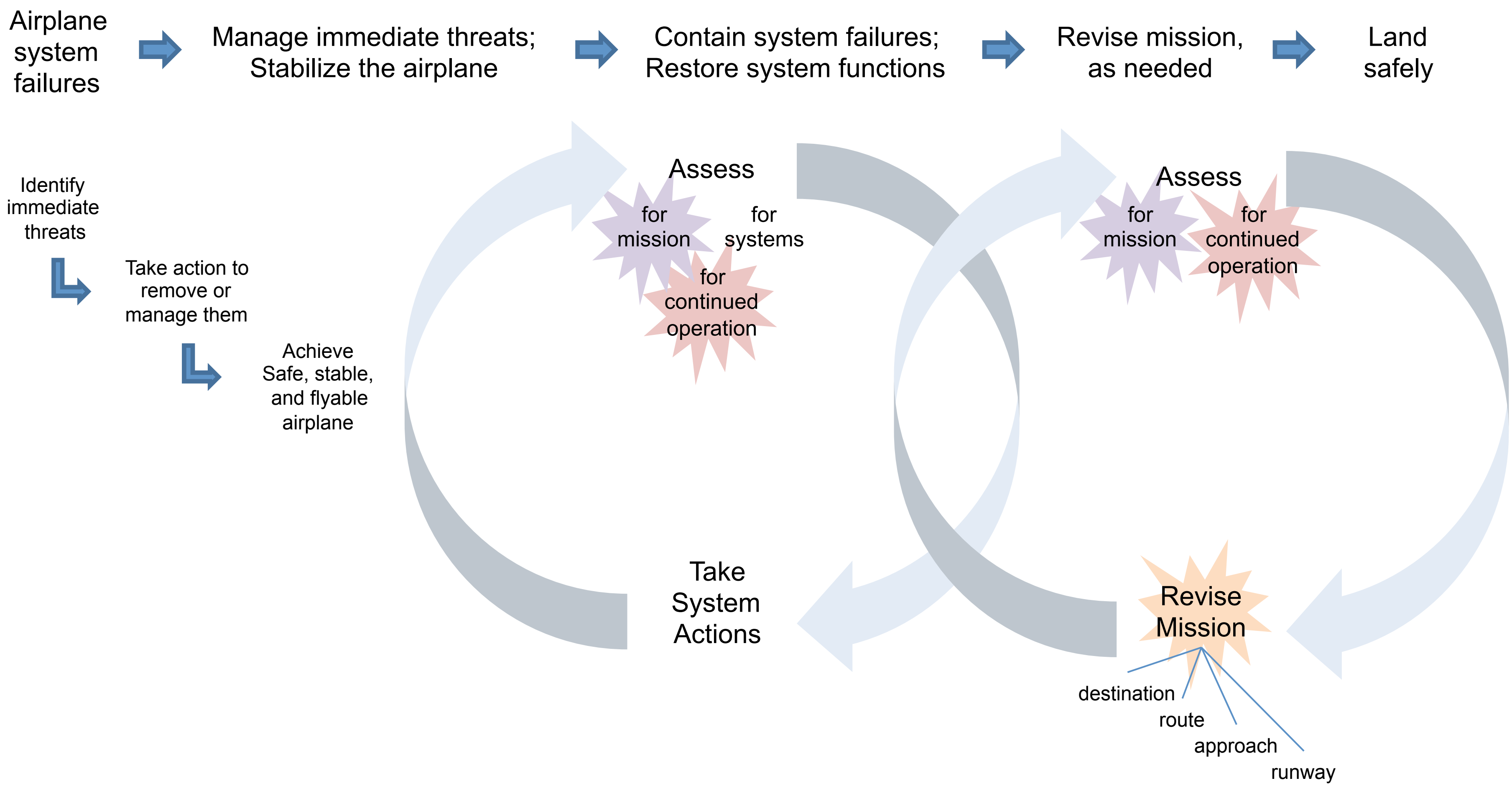
Aircraft Capability Management

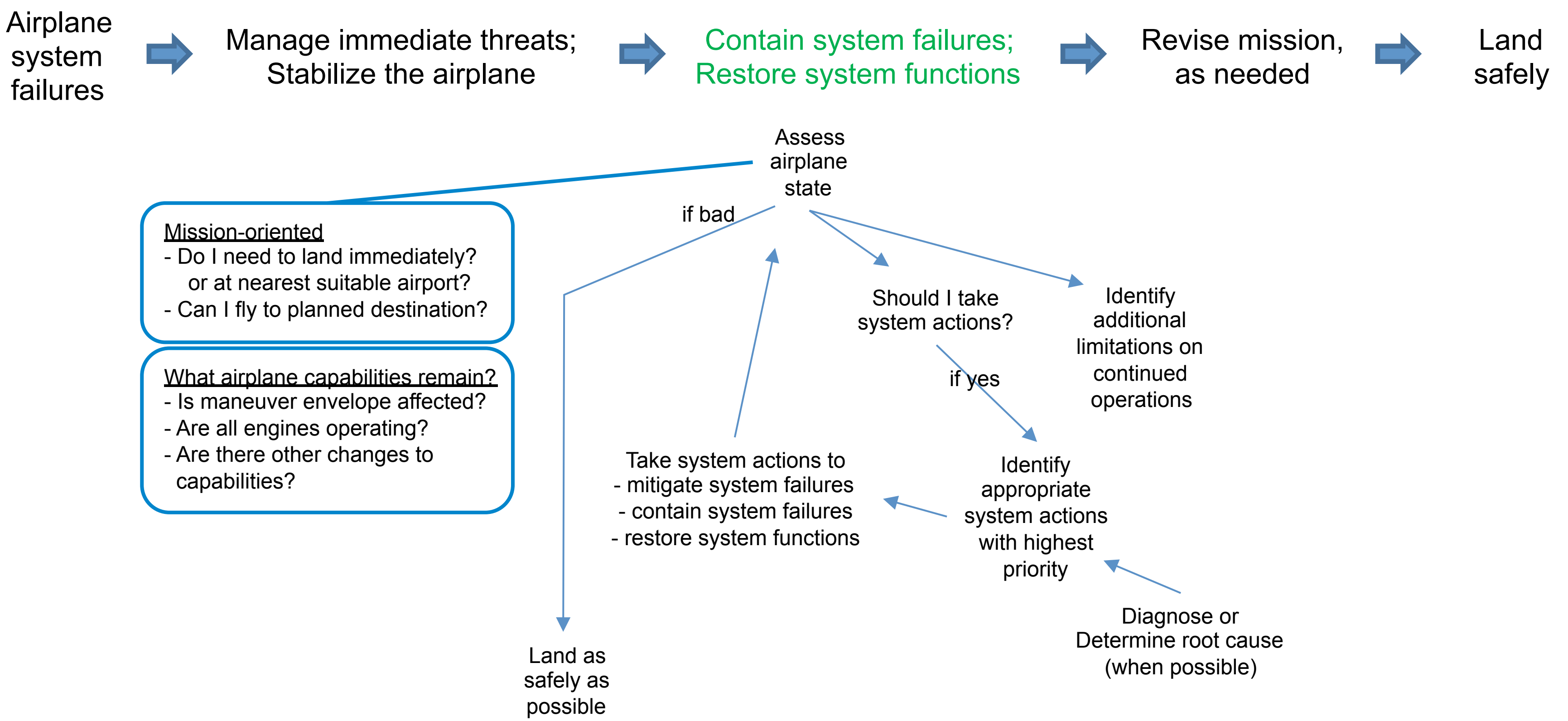
Randy Mumaw
Mike Feary

January 24, 2018

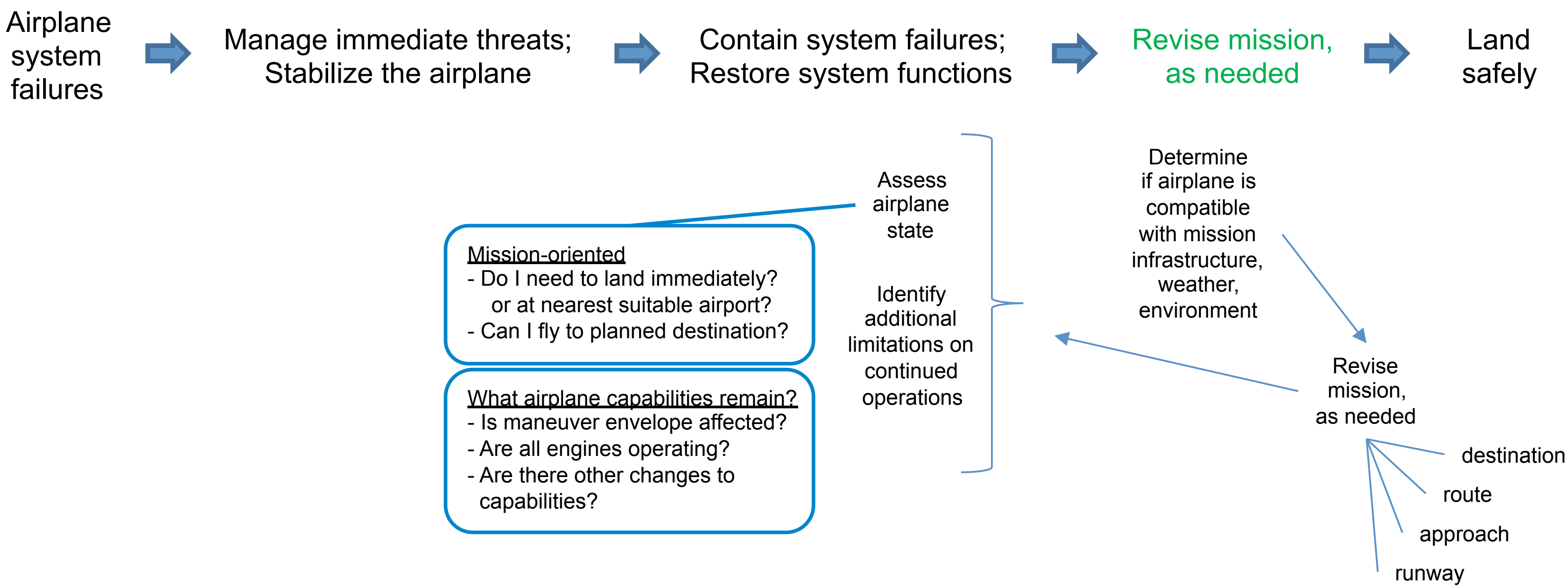
NASA Ames Research Center

From Failure/Change to Safe Landing





Airplane system failures
Manage immediate threats; Stabilize the airplane
Contain system failures; Restore system functions
Revise mission, as needed
Land safely
Assess airplane state
Mission-oriented
- Do I need to land immediately? or at nearest suitable airport?
- Can I fly to planned destination?
What airplane capabilities remain?
- Is maneuver envelope affected?
- Are all engines operating?
- Are there other changes to capabilities?
if bad
Should I take system actions?
Identify additional limitations on continued operations
if yes
Identify appropriate system actions with highest priority
Take system actions to
- mitigate system failures
- contain system failures
- restore system functions
Diagnose or Determine root cause (when possible)
Land as safely as possible


Airplane system failures
Manage immediate threats; Stabilize the airplane
Contain system failures; Restore system functions
Revise mission, as needed
Land safely
Assess airplane state
Identify additional limitations on continued operations
Mission-oriented
- Do I need to land immediately? or at nearest suitable airport?
- Can I fly to planned destination?
What airplane capabilities remain?
- Is maneuver envelope affected?
- Are all engines operating?
- Are there other changes to capabilities?
Determine if airplane is compatible with mission infrastructure, weather, environment
Revise mission, as needed
destination
route
approach
runway

Objectives

- How can we integrate information to better support operational decision making? Can we draw from available sources (airplane, environment, infrastructure) and integrate for decision makers?
- How can we reduce the burden on the flight crew by changing the tasks they need to perform, explicitly
  - remove the need to translate from physical to operational
  - remove the need to gather and organize relevant information
- What is the potential role for automation in this type of operational decision making? How do we shape Human-Automation teaming for this type of operational decision making?

NOTE: There are a number of NASA Ames projects related to these topics

Current State of Airplane System Failure Management

Boeing 787, Airbus 380, Bombardier C-Series, Embraer 170/190, Gulfstream G500

- The vast majority of non-normal messages are presented in terms of airplane system components (e.g., HYD Y ENG PMP A PRESS LO)
- Failure messages are presented for single failures
- EICAS messages get linked to electronic checklists (except Gulfstream)
- Flight crew can, generally, select the NNC they think is most appropriate (not on the A380)
- Changes to operational limitations are generated from NNCs but not integrated (Airbus does a better job here)

Interesting Items for each Airplane

Boeing 787
- easy access to ECL and NNC list
- some elimination of NNC messages

Airbus 380
- inability to see the entire set of ECAM messages / NNC and ECL together
- automatic linking of synoptics
- more sophisticated handling of operational consequences (landing performance)

Bombardier C-Series
- more complex displays for listing/accessing checklists
- some elimination of NNC messages

Embraer 170/190 (1st gen Primus Epic)
- large area for NNC messages (22 lines)

Gulfstream G500
- use of “umbrella” messages (hide downstream consequences)
- no ECL; no display-based ops consequences

The Problem

- Airplane system failures lead to a listing of failed components,
  which leads to one or more NNC messages,
  which leads to system actions (maybe) and
  statements about changes to operational limitations.
- It can be hard to
  - quickly assess ability to perform mission
  - see the “big picture” regarding airplane capability
  - keep track of changes to operational limitations
  - make well-informed diversion decisions
- For the operational decisions that need to be made
  - some information is missing
  - some information requires gathering and integrating

We believe operational decisions can be better supported.

Focus of Analysis (in 2017)

from
Occurrence of airplane system failures

to

Initial decisions regarding compatibility with the current mission
and
Overall state of the airplane

Display Concepts

- Mission Compatibility
- Airplane Capabilities
- Maneuver Envelope
- Operational Limitations by Phase of Flight
- Mission Risks
- Diversion Decision Making

Mission Compatibility

Figure 7a. Compatible with mission

Figure 7b. Not compatible with arrival and approach

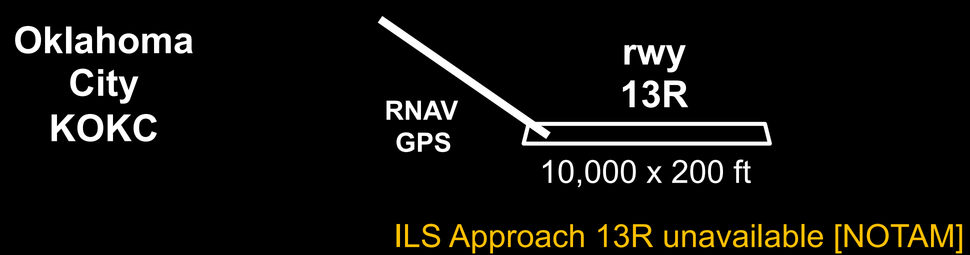


Figure 7c. Loss of options, from information in a NOTAM

How compatible are the airplane's current capabilities with the specifics of the planned destination

- Range/Endurance
  - Land immediately (or Land as soon as possible)
  - Land at nearest suitable airport
  - XXXX [airport specifier] may be out of range
- Landing distance
- Approach/Departure/Arrival
- Airspace along the route
- Airport
- Runway

What is a Capability?

Airplane System Components

- Hydraulic system
- Thrust Reverser
- Battery
- Air conditioning pack

Airplane Capabilities

- Range / Endurance
- Stopping Distance (on runway)
- Ability to perform a specific approach
- Ability to enter RVSM airspace
- Maneuver envelope

Airplane system components have failed

What can I do?
Where can I go?

Initial Ideas about Airplane Capabilities

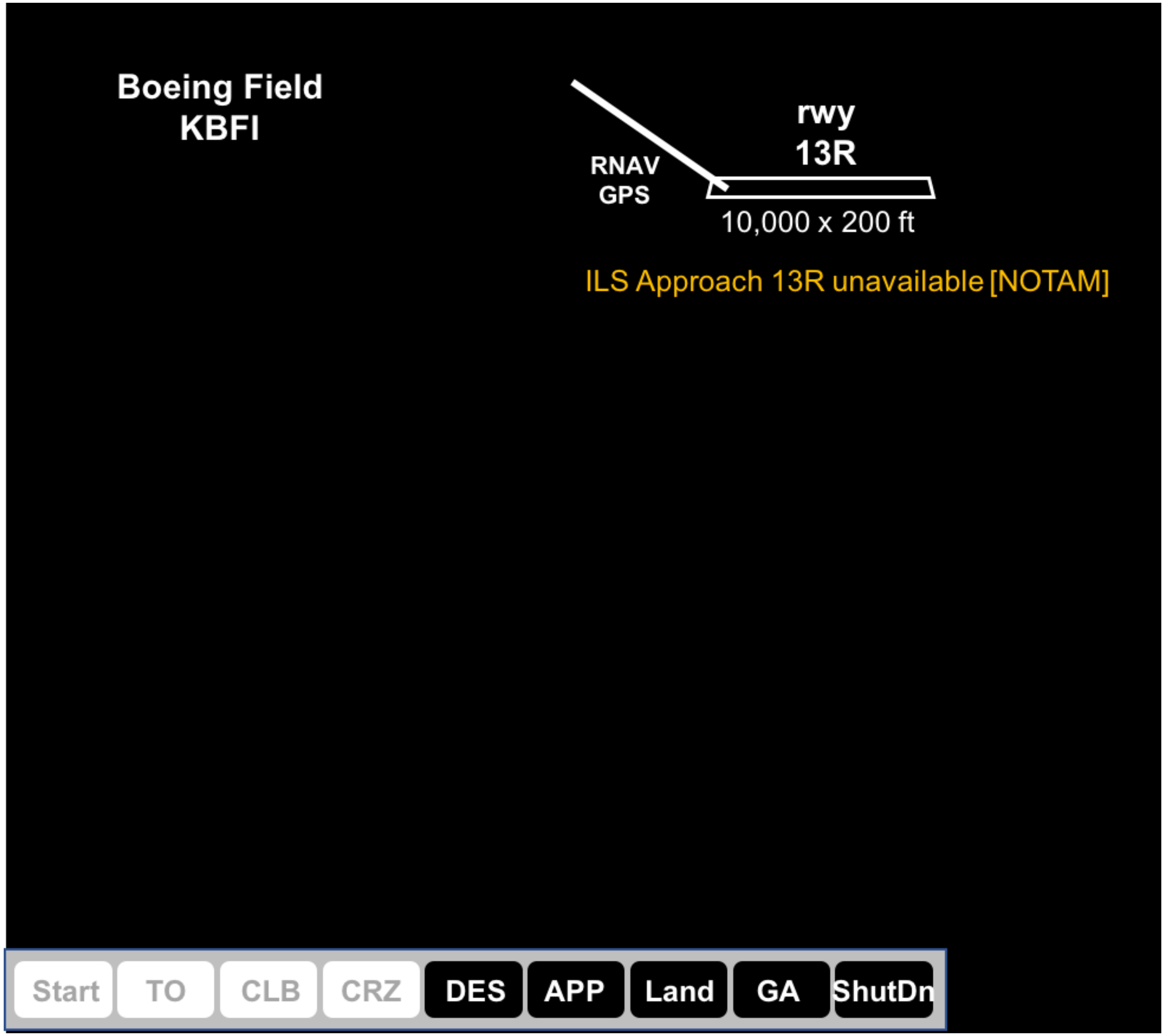
Can I Take–off?
Can I reach my planned destination?
Can I land?
Envelope

<u>Resources</u>
Electric Power
Hydraulic Power
Pneumatic Power
Equipment Cooling

Engines (state)

Navigation
Communication
Autoflight
Surveillance
Cabin/Cargo Environment
Ice Protection
Fire Detection & Extinguishing
Airspace Access
Approach Access
Landing Distance
Runway Directional Control
Fuel Supply

Case 1: Radio Altimeter failure



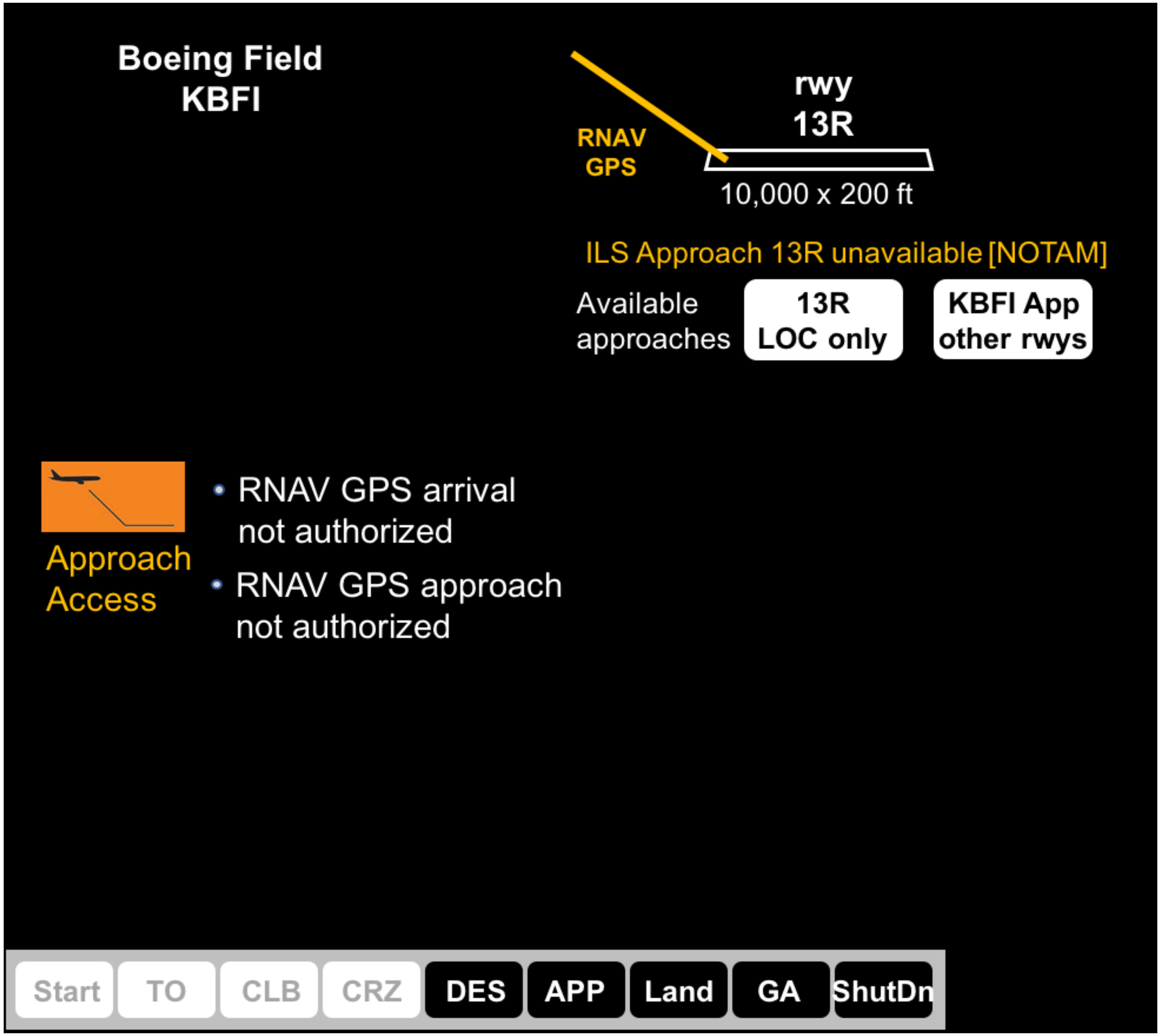
Enroute to KBFI, in Descent.

NOTAM has indicated that 13R ILS is out.

13R RNAV GPS approach was selected.

There are currently no operational limitations

Case 1: Radio Altimeter failure

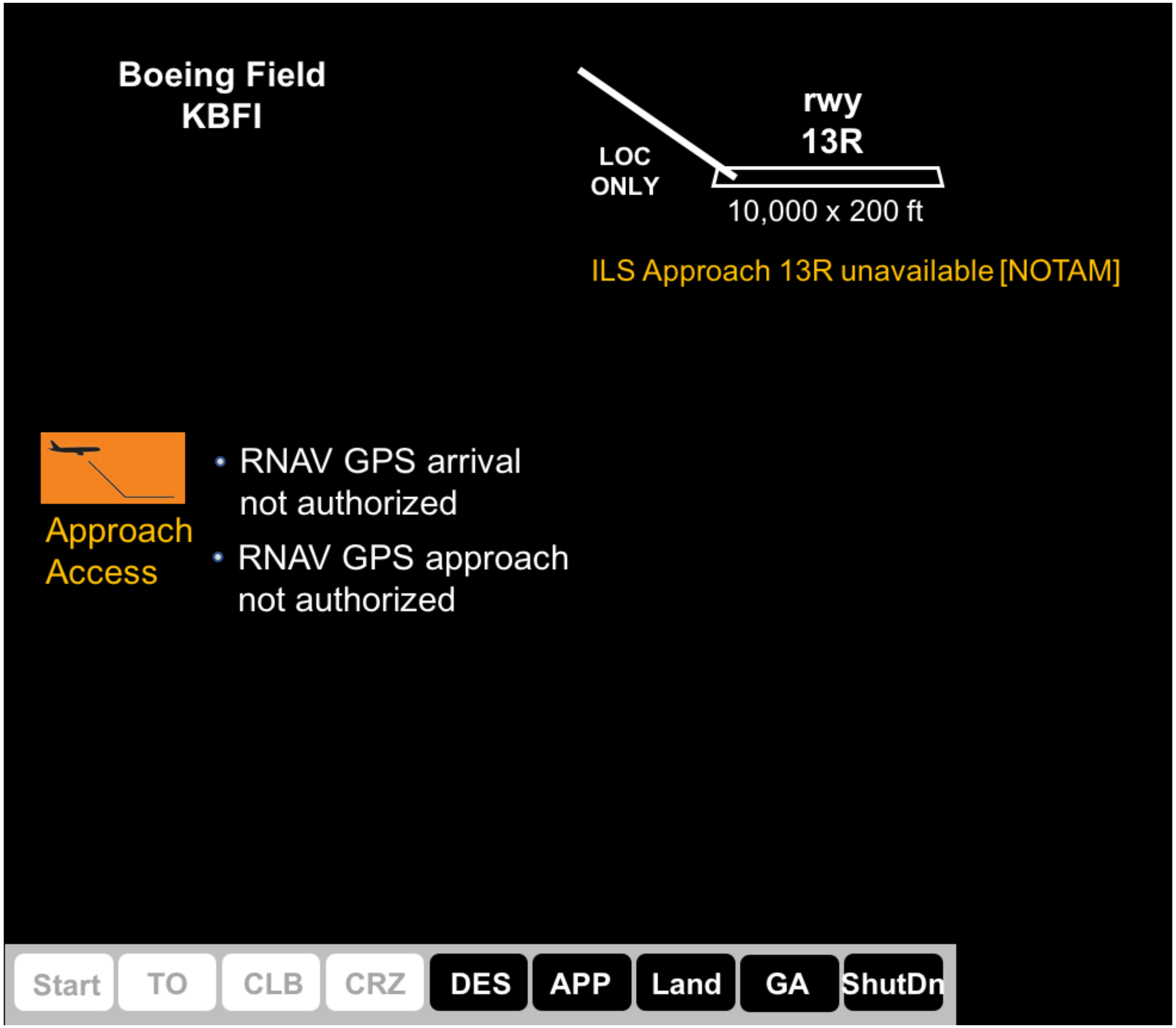


A radio altimeter fails.

“Alerting” on the approach and the notification that there have been changes to Approach Access. Language is “not authorized”.

Other available approaches are offered.

Case 1: Radio Altimeter failure

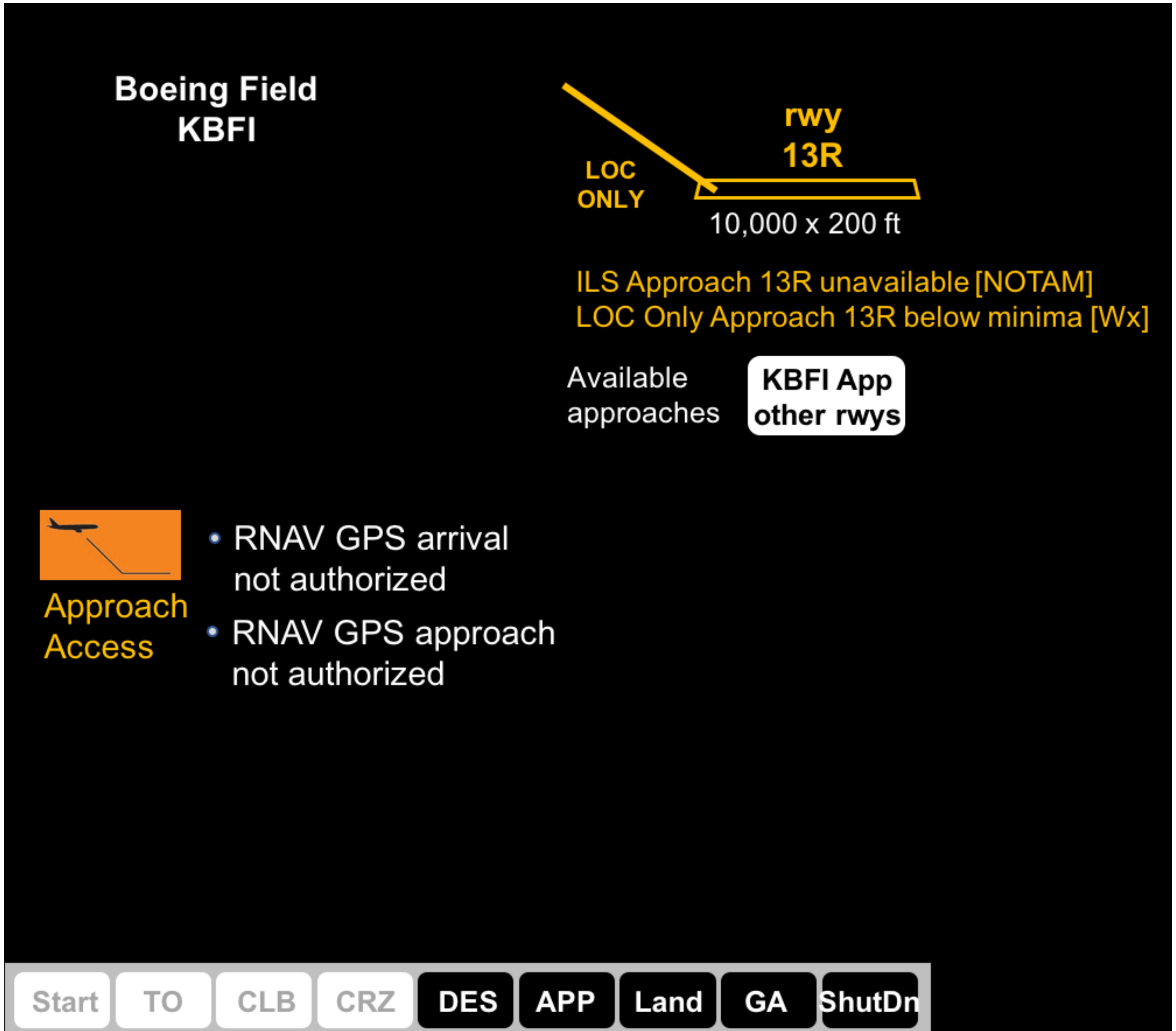


Pilot selected the LOC only approach.

Everything is fine again.

Changes to airplane capabilities are not really relevant to the new mission. Should they be preserved?

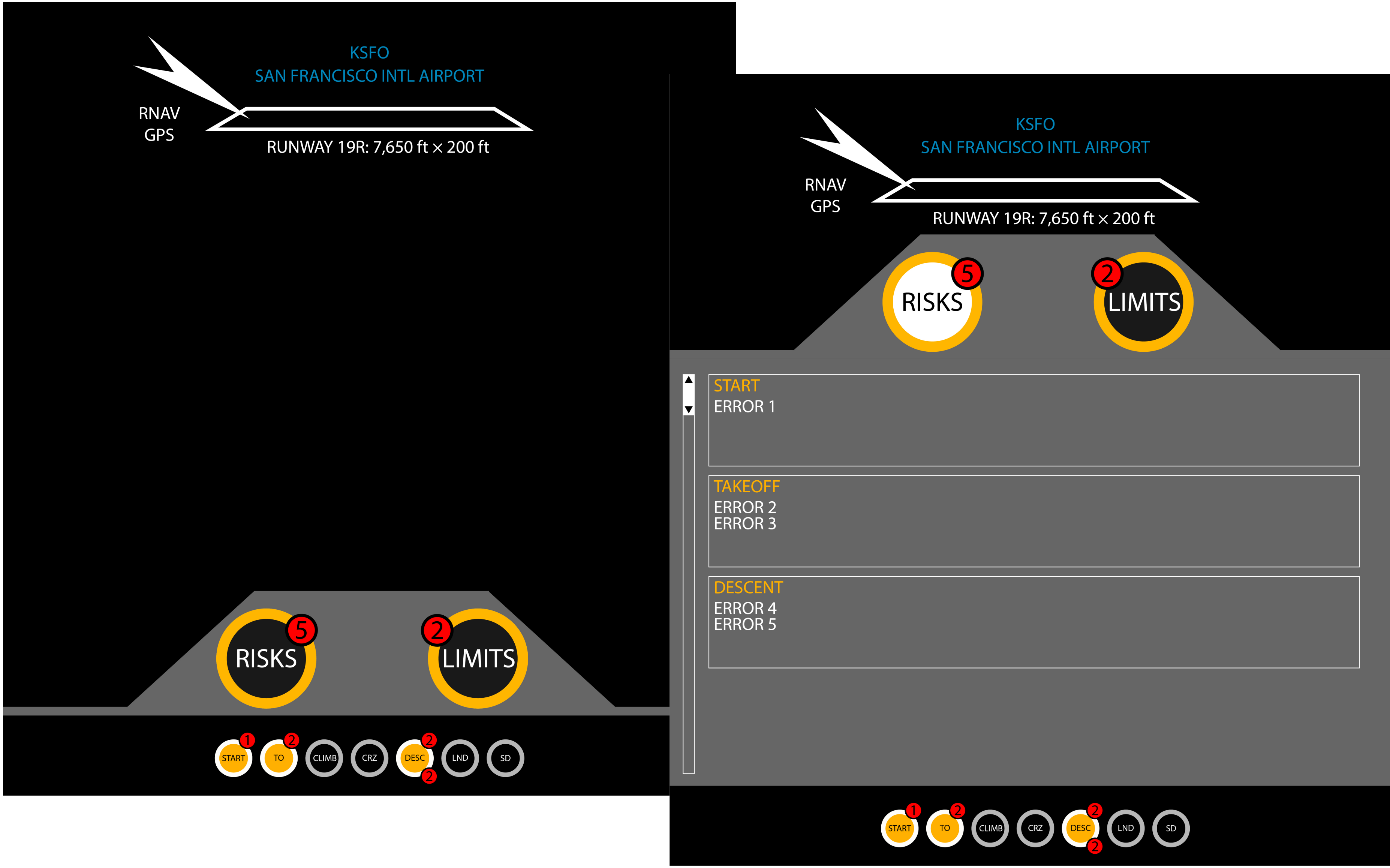
Case 1: Radio Altimeter failure



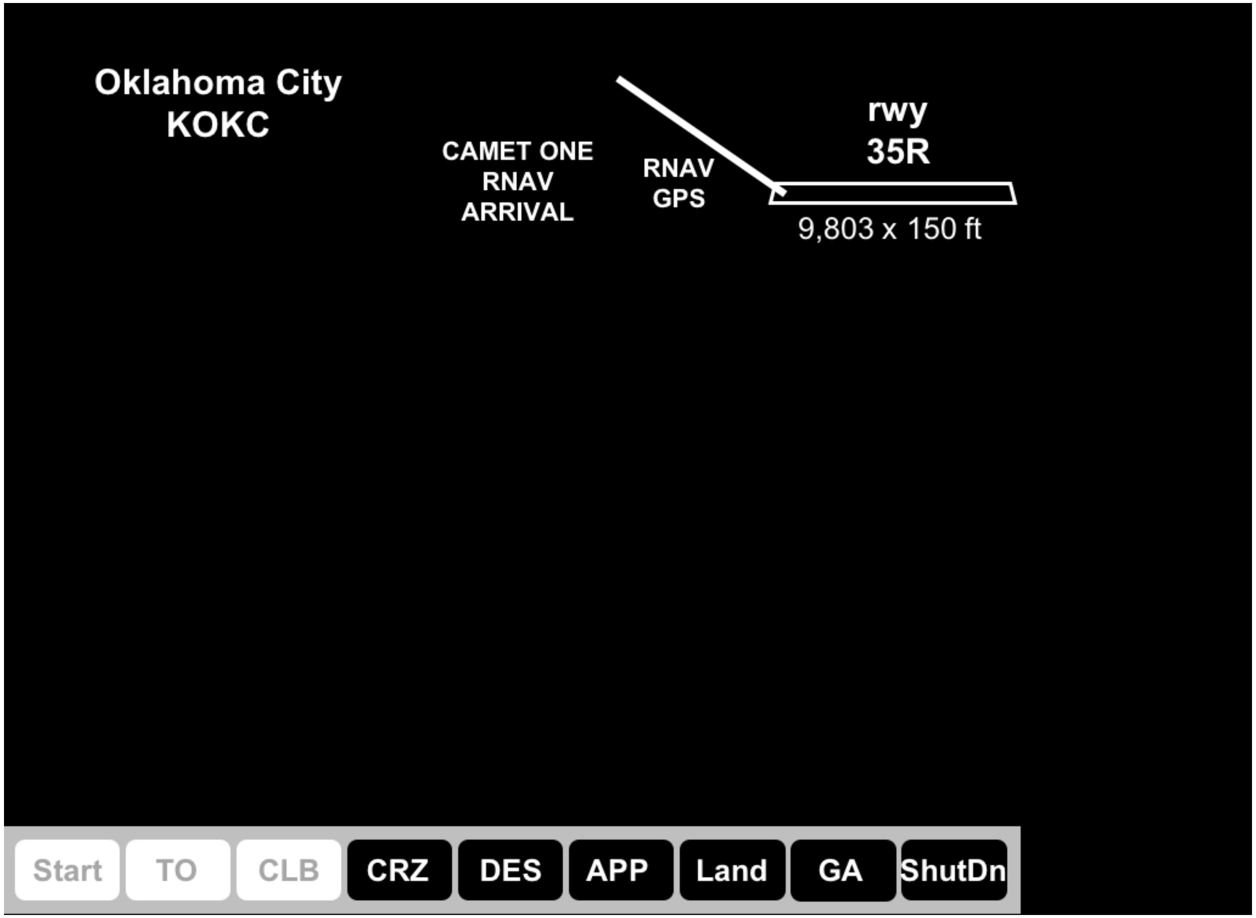
Weather gets worse and LOC only approach should NOT be flown.

Divert?
Pilot must trigger a diversion support tool in this case.

Alternative Design

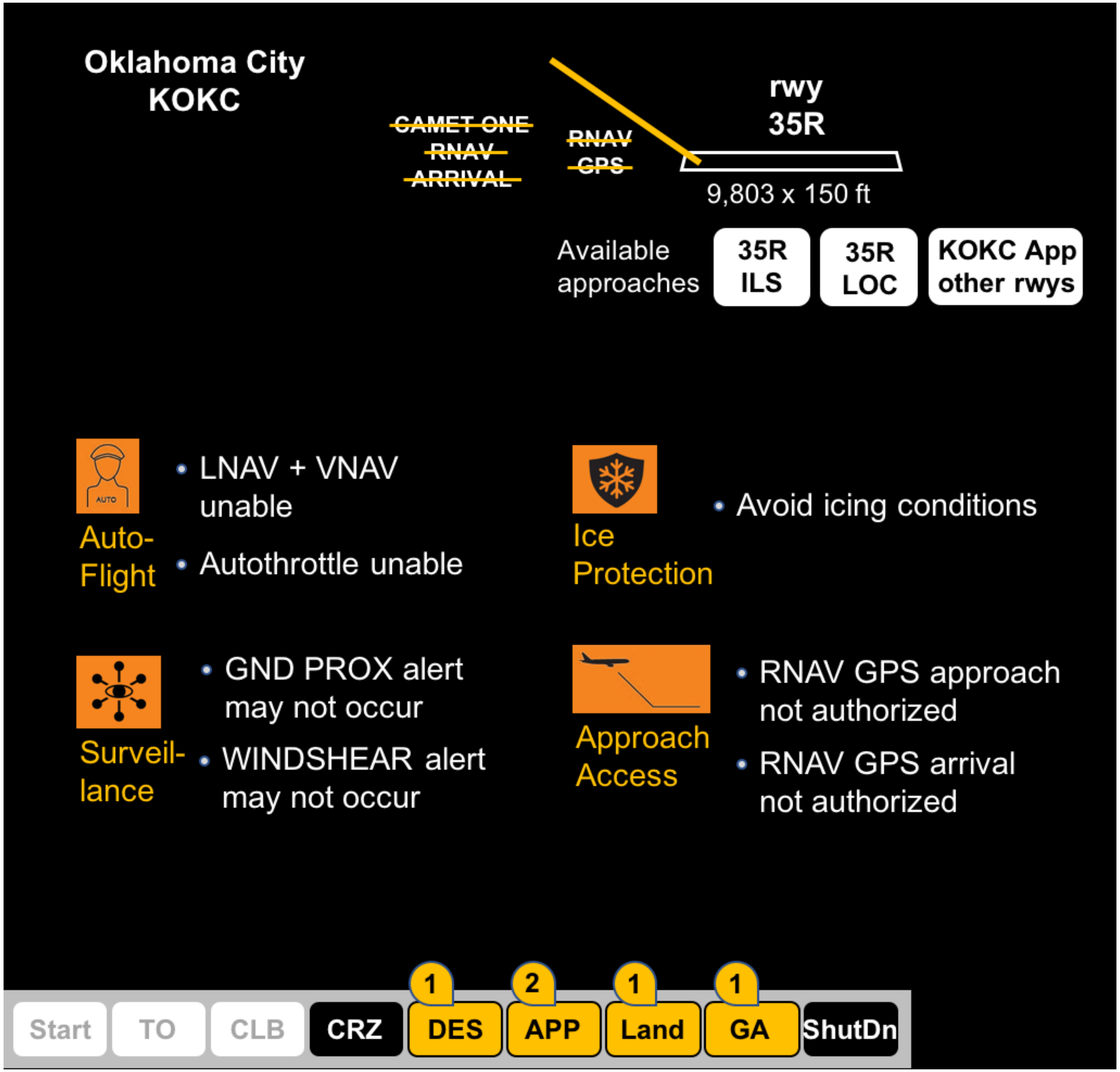


Case 2: AC Bus Failure



Enroute to OKC, in Cruise.

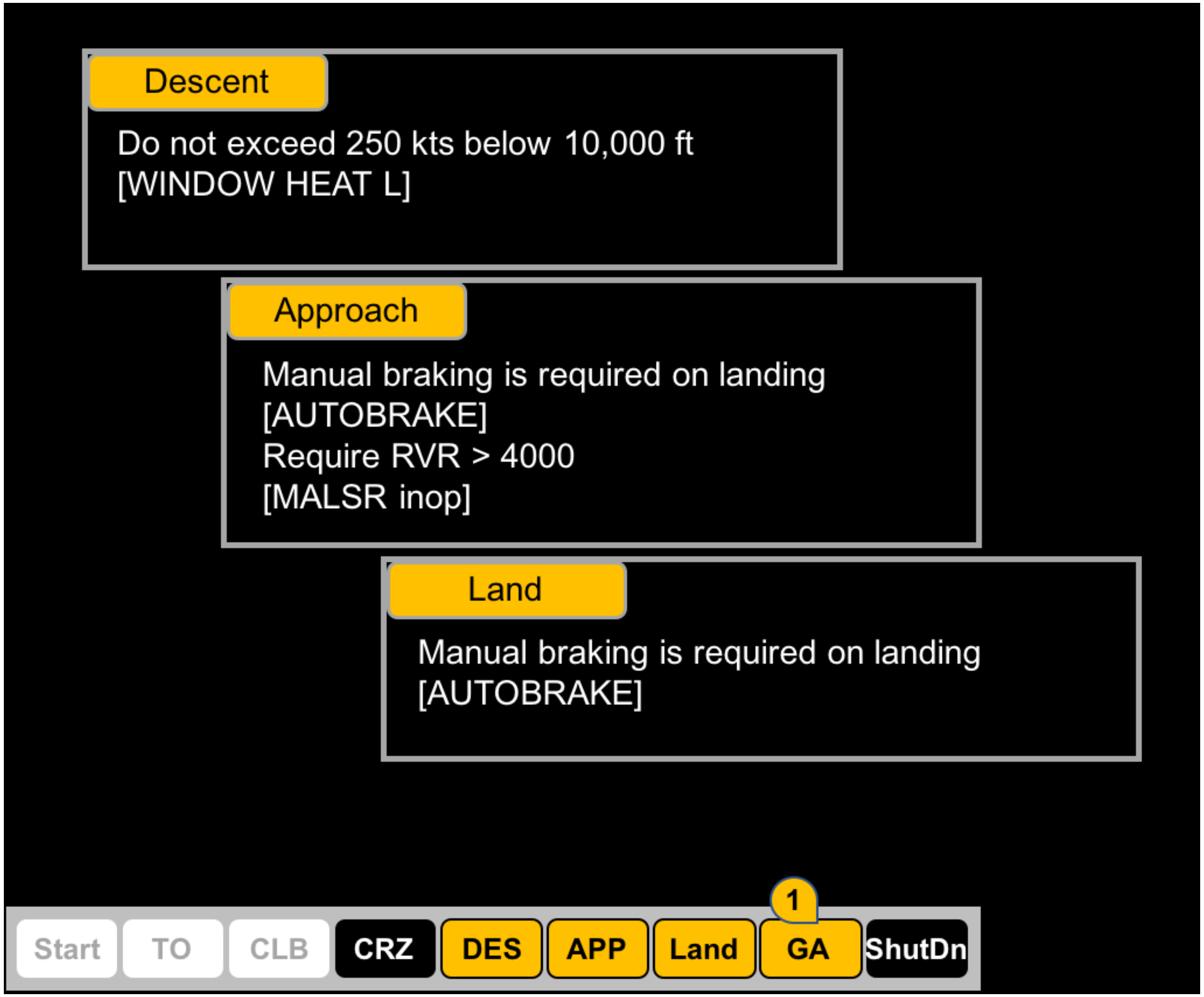
Case 2: AC Bus Failure



AC Bus Faiure occurs.
EICAS messages would be
- AC BUS 1 OFF
- AUTOTHROT DISC
- ENG 1 EEC MODE
- FUEL PUMP 2
- FUEL PUMP 3
- WNSHR ALERT SYS
- GND PROX SYS
- HEAT L TAT
- OUTFLOW VLV L
- HEAT L AOA
- WINDOW HEAT L
- HEAT P/S CAPT
- AUTOBRAKE
- ELEC UTIL BUS L

Some changes to operational limitations have occurred.

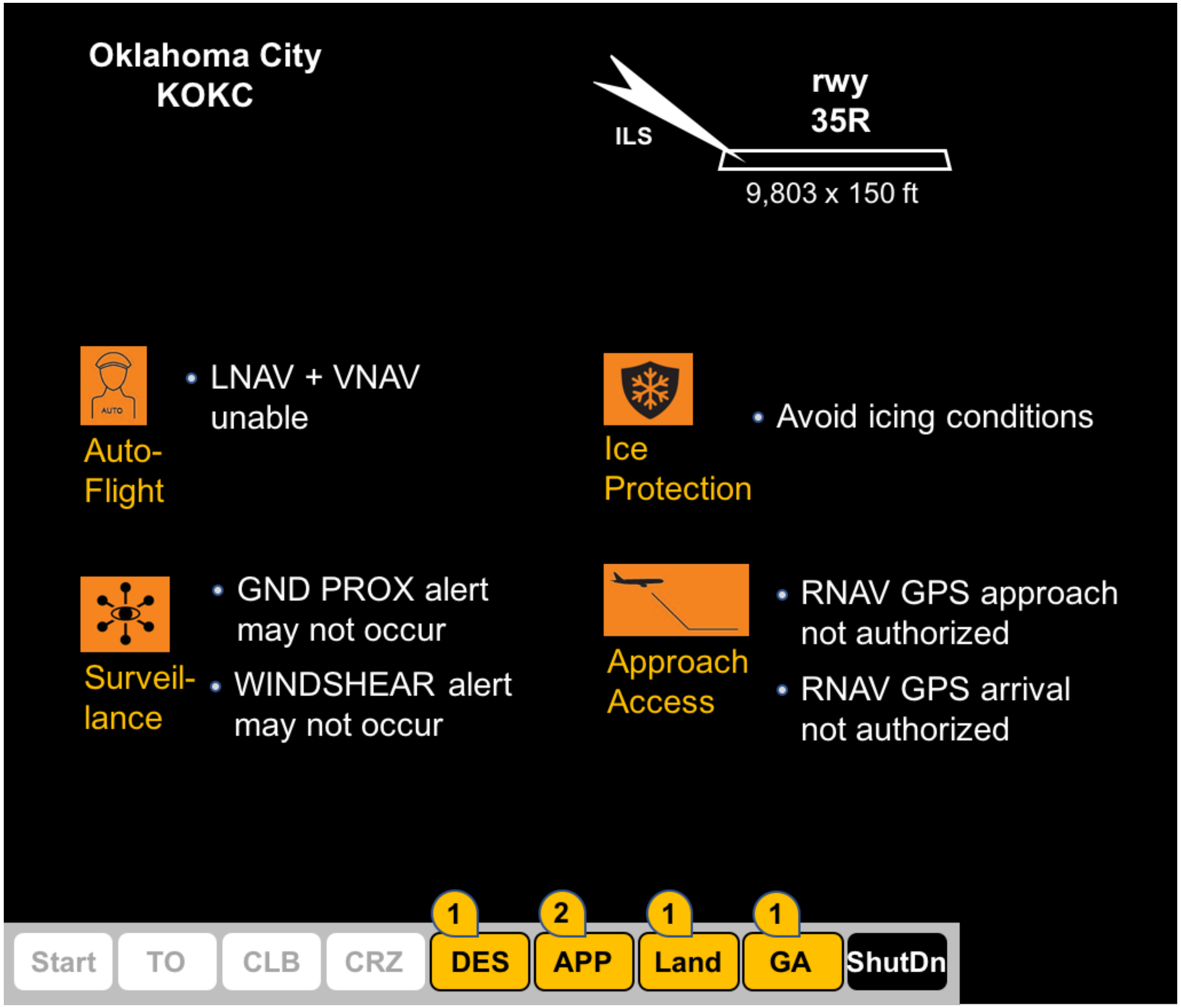
Case 2: AC Bus Failure



Operational limitations are organized by phase of flight.

Also, it shows origin of limitation.

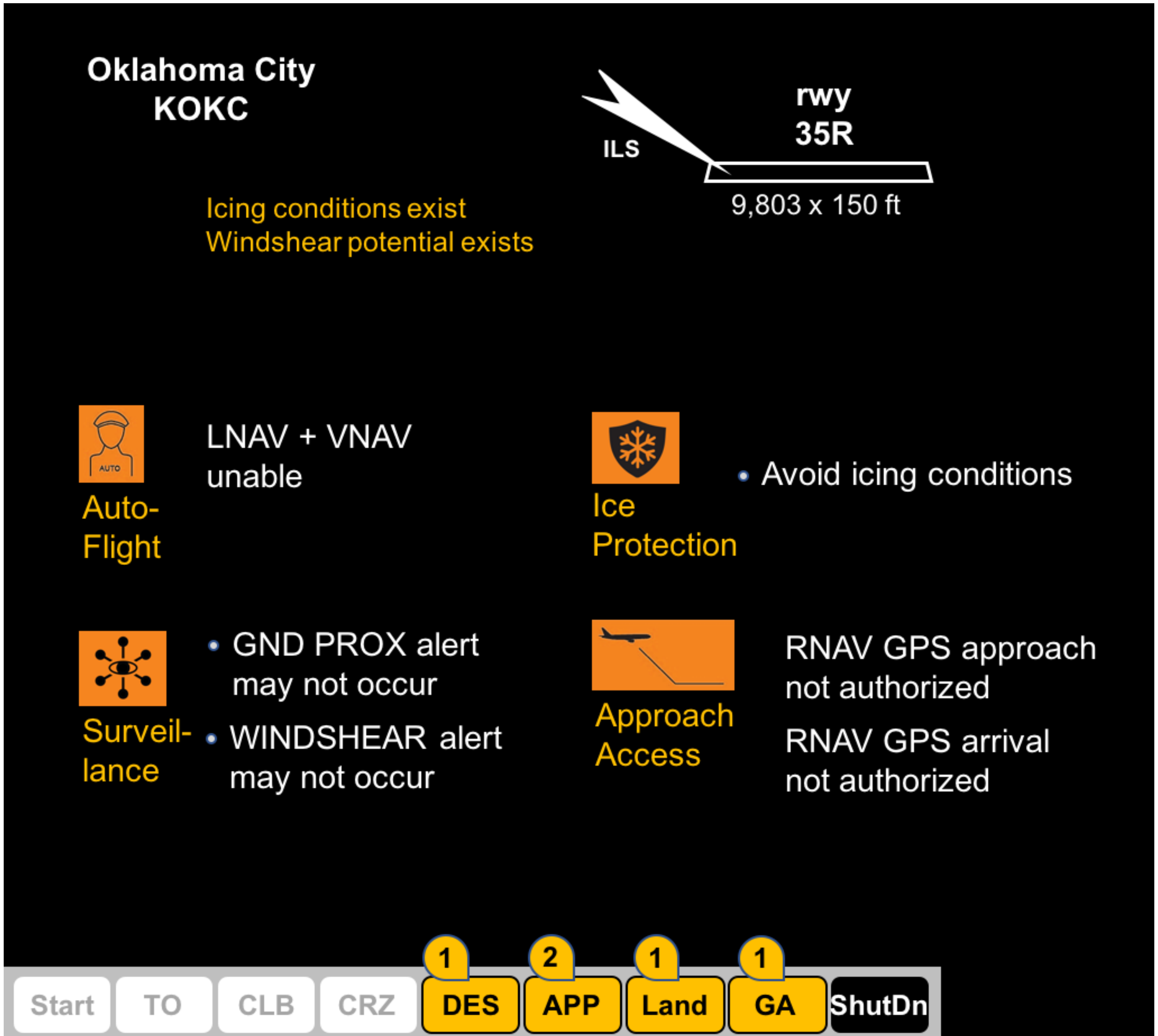
Case 2: AC Bus Failure



New approach selected.

Everything is good.

Case 2: AC Bus Failure



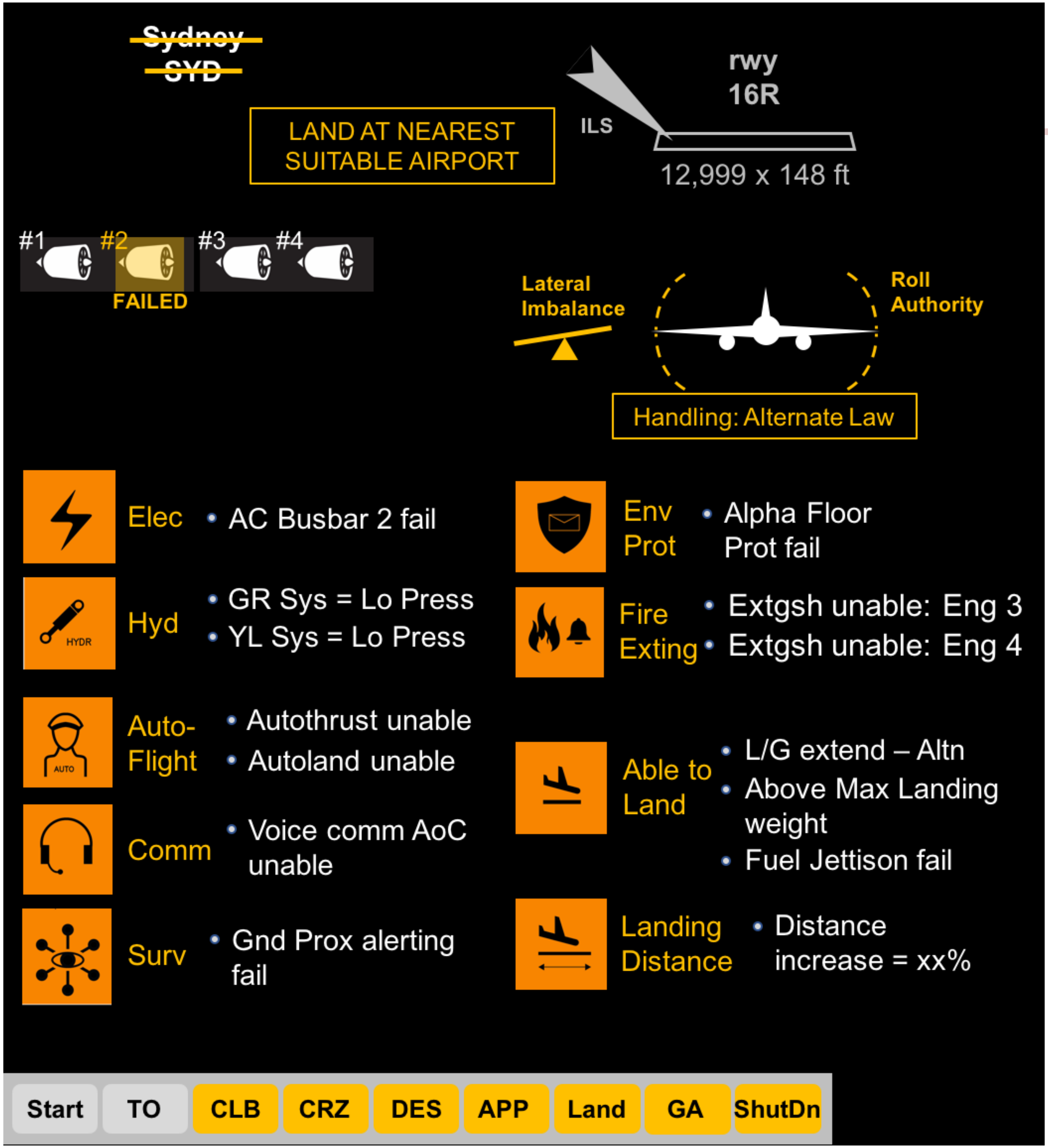
Again, weather changes

Explosion of Alert Messages

Qantas A380 Uncontained Engine Failure

- QF 32; Singapore to Sydney; 469 people on board
- 4 minutes after Take-off, engine no. 2 bursts, severely damaging other equipment
- 43 ECAM messages in first 60 seconds; many additional later
- 50 minutes to sort through the non-normal checklists (NNCs)

“It was hard to work out a list of what had failed; it was getting to be too much to follow. So we inverted our logic: Instead of worrying about what failed, I said ‘Let’s look at what’s working.’”   *A380 Captain*



Qantas 32

Lots of stuff going on.

Does this provide a useful overview? Contrast to >80 ECAM messages that came one at a time.

Design Decisions / Trade-offs

- All capabilities vs Those remaining vs Those lost/degraded
- All capability information vs Only what is relevant to the mission
- Keep EICAS and supplement it vs Replace it (final goal depends on how much automation will come to system management)
- Rely on estimates from engineering analysis (model-based) vs Relying on pilots to reason through the system
- Integration vs Elements (Lost capabilities + airport or environmental conditions)

Reasons for Using System Displays (Synoptics)

We stayed away from ideas to support system actions

- Identify options for restoring a capability
    - what is lost
    - what is available

    [use simple models to map physical components to airplane capabilities]

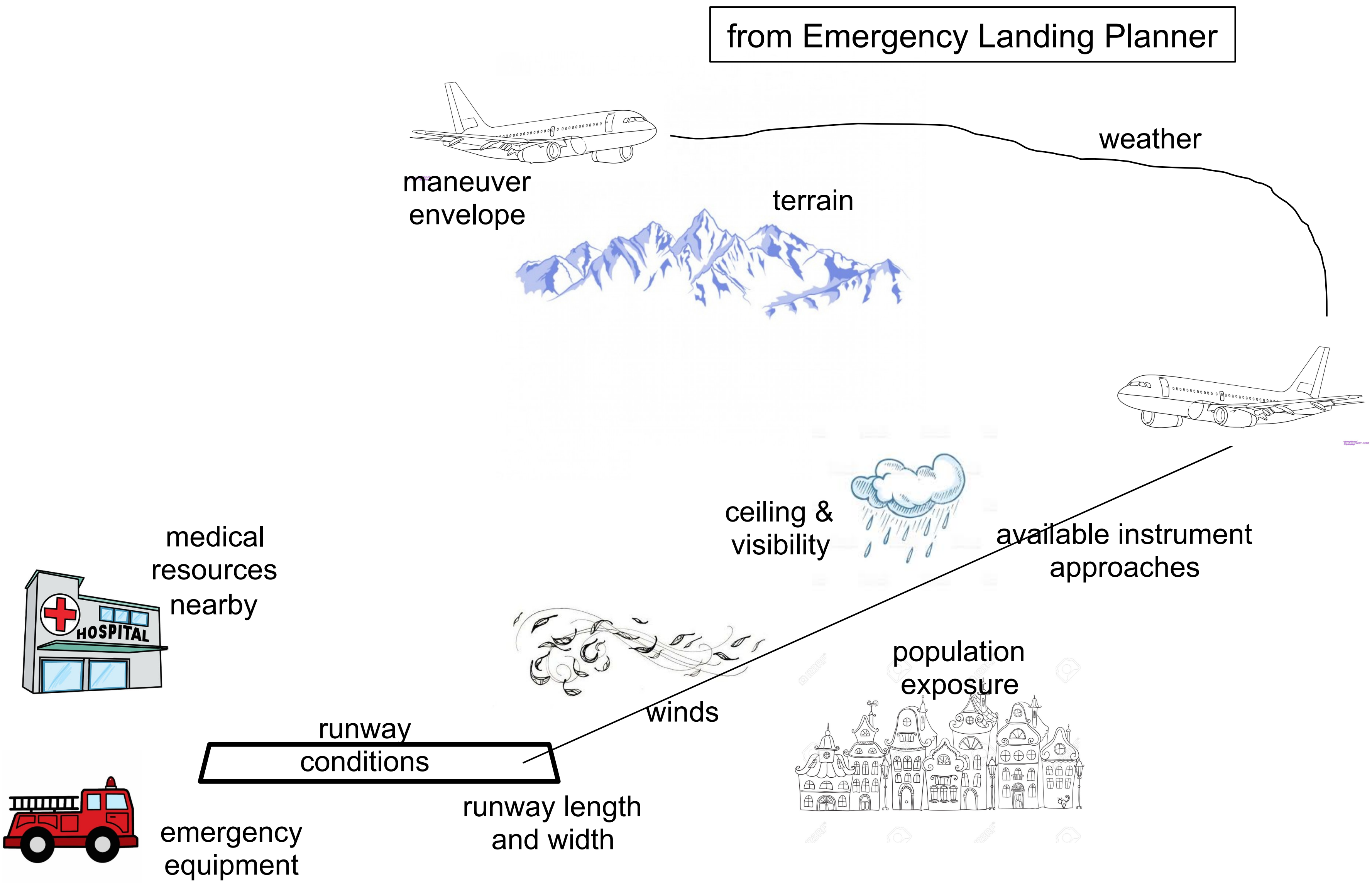
- Feedback on system actions
    - containing
    - restoring

- Illustrations of change in airplane capabilities (operational consequences) / Systems training

What Did We Learn?

- Current interfaces (and operational procedures) for managing system failures are evolving but are still tied to a language of system components.
- We understand it is not simple to generate accurate operational information from sensing component failures, BUT someone should be pushing hard to figure out what can be done.
- Airplane capabilities is just one critical input into operational decision making. Other relevant information is should also be included (weather, NOTAMs, flight crew risks . . .)
- Pilots would benefit from a more integrated approach to span from system failures to diversion decisions.
- While we have not been able to perform a large, formal evaluation, informal feedback from pilots has been very positive.

Mission Decision: Where Should I Land?



Mission Decision: Where Should I Land?