NASA/TM—2018–219774

Managing Complex Airplane System Failures through a Structured Assessment of Airplane Capabilities

Randall J. Mumaw
San Jose State University Foundation

Michael Feary
NASA Ames Research Center

Lars Fucke
Diehl Aerospace

Michael Stewart
San Jose State University Foundation

Randy Ritprasert
San Jose State University Foundation

Alex Popovici
San Jose State University Foundation

Rohit Deshmukh
San Jose State University Foundation

March 2018

NASA STI Program…in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, and organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question via to help@sti.nasa.gov

- Phone the NASA STI Help Desk at (757) 864-9658

- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM—2018–219774

Managing Complex Airplane System Failures through a Structured Assessment of Airplane Capabilities

Randall J. Mumaw
San Jose State University Foundation

Michael Feary
NASA Ames Research Center

Lars Fucke
Diehl Aerospace

Michael Stewart
San Jose State University Foundation

Randy Ritprasert
San Jose State University Foundation

Alex Popovici
San Jose State University Foundation

Rohit Deshmukh
San Jose State University Foundation

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California

March 2018

Acknowledgments

This work has benefitted significantly from discussions with Jelmer Reitsma of Boeing, who was pursuing similar interests. We also want to thank a group of U.S. airline pilots who provided some early inputs on airplane capabilities. In addition, Captain Rob Koteskey of United Airlines provided valuable early reviews and advise on the prototype displays. Finally, we'd like to acknowledge valuable reviewer inputs from Loukia Loukopoulou and Mary Connors.

Available from:

NASA STI Program
STI Support Services
Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199

This report is also available in electronic form at http://www.sti.nasa.gov
or http://ntrs.nasa.gov/

Table of Contents

List of Figures

Acronyms and Definitions

AAL	American Airlines
AC bus	alternating current bus
AFM	Airplane Flight Manual
AH	abstraction hierarchy
APU	auxiliary power unit
ATC	air traffic control
CAS	crew alerting system or central alerting system
CPCS	cabin pressurization system
DSP	Display Select Panel
DST	decision support tool
ECAM	electronic centralized aircraft monitor
ECL	electronic checklist
ECS	environmental control system
EICAS	engine-indications and crew-alerting system
ETOPS	extended-range twin-engine operation performance standards
EWD	ECAM warning display
FMC	flight management computer
ft	feet
GPS	global positioning system
IFR	instrument flight rules
ILS	instrument landing system
inop	inoperable
KBFI	Boeing Field (Seattle)
KOKC	Oklahoma City airport
kts	knots
LDG PERF	landing performance
LNAV	lateral navigation
LOC	localizer
LRC	long-range cruise
MALSR	medium intensity approach lighting system plus runway alignment indicator lights
MEL	minimum equipment list
MFD	multi-function display
NASA	National Aviation and Space Administration
NNC	non-normal checklist
NOTAM	notice to airmen
OEB	Operations Engineering Bulletin
OEM	original equipment manufacturer
OIS	Onboard Information System
ORD	Chicago O'Hare Airport
QRH	quick reference handbook
RAT	ram air turbine
RNAV	area navigation
RVR	runway visual range
RVSM	reduced vertical separation minima
SD	Systems Dsplay
TCAS	traffic collision avoidance system
VNAV	vertical navigation
V_{ref}	reference touchdown speed

Managing Complex Airplane System Failures through a Structured Assessment of Airplane Capabilities

Randall J. Mumaw[1], Michael Feary[2], Lars Fucke[3], Michael Stewart, Randy Ritprasert, Alex Popovici, Rohit Deshmukh

Executive Summary

This report describes an analysis of current transport aircraft system-management displays and the initial development of a set of display concepts for providing information about aircraft system status. The new display concepts are motivated by a shift away from the current approach to aircraft system alerting that reports the status of physical components, and towards displaying the implications for mission capability.

Specifically, the proposed display concepts describe transport airplane component failures in terms of operational consequences of aircraft system degradations. The research activity described in this report is an effort to examine the utility of different representations of complex systems and operating environments to support real-time decision making during off-nominal situations. A specific focus is to develop display concepts that provide more highly integrated information to allow pilots to more easily reason about the operational consequences of the off-nominal situations. The work can also serve as a foundational element to autonomy-supported decision making since we are developing ideas for integrating information from the airplane and the operational environment to support decision making.

1. Introduction

Throughout the history of aviation, the approach to managing airplane system failures has been tied to sensing and reporting on failures of physical airplane components (e.g., an electrical bus). This approach requires the flight crew, with the aid of procedures, to sort out how the airplane is affected in terms of continued safe flight and landing. This can be a complex task for flight crews in modern jet transports and, in a number of cases, flight crews have managed it poorly (e.g., AAL 268, September 2008; https://www.ntsb.gov/_layouts/ntsb.aviation/brief2.aspx?ev_id=20081007X03940&ntsbno=CHI08IA292&akey=1). This issue is taking on increasing importance because recently developed transport airplanes have more complex and interconnected systems that significantly increase the difficulty of anticipating how component failures will affect system operations. While more intensive pilot training could reduce the impact of the increasing complexity of systems, it is highly unlikely that airplane systems training will be increased sufficiently to support pilots in reasoning through airplane system failures.

[1] San Jose State University Foundation; NASA Ames Research Center, Moffett Field, California.

[2] NASA Ames Research Center, Moffett Field, California.

[3] Diehl Aerospace; Hamburg, Germany.

We describe a new approach that attempts to translate physical system components directly into airplane "capabilities," which is the set of airplane functions required for operations. Ideally, these capabilities—when combined with other information that can be taken from the operational environment (e.g., current weather)—can present information to the flight crew that is closely aligned with the necessary operational decisions.

This report documents the work we have done to date on identifying airplane capabilities and designing display concepts that present these capabilities to the flight crew in a way that conveys airplane state and helps them make operational decisions. The report begins with a description of flight crew activities and decisions that are part of managing a non-normal event tied to airplane system failures. Section 3 describes the flight deck displays in the most-advanced commercial jet transport airplanes to show how airplane system failures are being addressed now. Section 4 describes how changes in airplane system architectures have made managing airplane system non-normals more difficult and that the existing solutions may have limitations. Section 5 describes the process we used for defining airplane capabilities, which moves away from traditional descriptions of physical airplane component states and toward functional descriptions. In Section 6, we describe the results of our work on defining new display concepts and their contents. A number of display concepts are presented with a description of how they could be coordinated for managing non-normal events. Section 7 presents a set of prototype displays that are linked to two fictional cases and two actual cases (the Qantas 32 accident and an American Airlines incident). In the last sections we identify potential next steps to further this work and present a summary of our conclusions.

2. Managing System Failures: From Failures to Operational Decisions

Airplane systems are responsible for supporting the full range of functions in a jet transport aircraft; examples are navigation, communication, pressurization, moving flight control surfaces, and stopping after landing. While airplane systems are generally highly reliable, they can fail or be damaged during a flight, and when this occurs, the flight crew needs to manage those failures for continued safe flight and landing. The flight crew activities tied to managing these failures are generally the following three steps:

- *Step 1: Manage the immediate threats to the flight*. The sub-goals are to identify the immediate threats, take action to remove them or manage them, and achieve a safe, stable, and flyable airplane. The following immediate threats, at minimum, should be considered:
  - fire
  - airplane depressurization
  - engine failure
  - damaged or non-functioning flight control surfaces
  - ground proximity
  - potential for traffic or obstacle collision
  - windshear conditions
  - take-off configuration
  - stall (or approaching a stall)
  - overspeed
  - unusual attitude
  - autopilot disconnect

These immediate threats are typically alerted at the Time-Critical Warning level to indicate the highest level of urgency. It is critical to have a safe, stable, and flyable airplane, under control, before any further activities should be pursued.

- *Step 2: Contain system failures and restore system functions*. Airplane system failures are annunciated through an alerting system, typically through a set of short alerting system messages. Examples of these messages are PACK L, HYD PRESS C, or ELEC AC BUS. These messages typically indicate a failure or non-normal state has been sensed in some airplane system component. Many, but not all, messages are also a link to a non-normal checklist (NNC) that contains actions for the flight crew to take in response to the failure. These actions are designed to do some or all of the following:
  - Contain the system failure. For example, to close fuel system valves when there is a known leak from a fuel tank. By reconfiguring the fuel system, a pilot may be able to prevent further fuel loss.
  - Restore system functions. For example, to engage a new source of power when one source of power was lost, such as starting the auxiliary power unit (APU) or ram air turbine (RAT) when electrical power was lost from another source. Ideally, by reconfiguring airplane systems, it becomes possible to restore lost or degraded functions. However, it may not be possible to restore everything.
  - Mitigate system failures. For example, to change airplane or airplane systems operation to accommodate a failure, such as descending to a lower altitude when it is no longer possible to pressurize the airplane adequately to support operations at a high altitude.

  The NNCs are designed to try to achieve these three objectives. However, these actions are "packaged" in NNCs that are tied to each failure, and when there are multiple airplane system component failures (and multiple messages), the flight crew must determine which NNC to apply, and in what order NNCs will be performed. In some cases, the flight crew will understand the nature of the failure and that will aid them in setting priorities for performing NNCs.

  Note that in the more-detailed view of this task (Figure 2), there is also a need to determine very early—prior to systems management—whether an emergency landing is needed.

- *Step 3: Revise mission as needed*. Another consideration in responding to airplane system failures are changes to the operational limitations of the airplane. The airplane system failures may lead to, for example, limitations in airspeed, flap settings, or the need to manually deploy the landing gear.

  When failures are more significant, there may be a need to revise the mission; that is, it may not be possible to safely fly to the planned destination. The flight crew needs to determine if there is a need to revise the mission, and if so, in what way. Further, this assessment can be on-going as there may be changes to weather or, perhaps, continued degradation of airplane systems, such as a fuel leak.

These three types of activities are captured in Figure 1 at a high level. On the left are the three steps for managing immediate threats. When that objective has been met, it is possible to move to the two performance cycles, one for each of the other two activities.

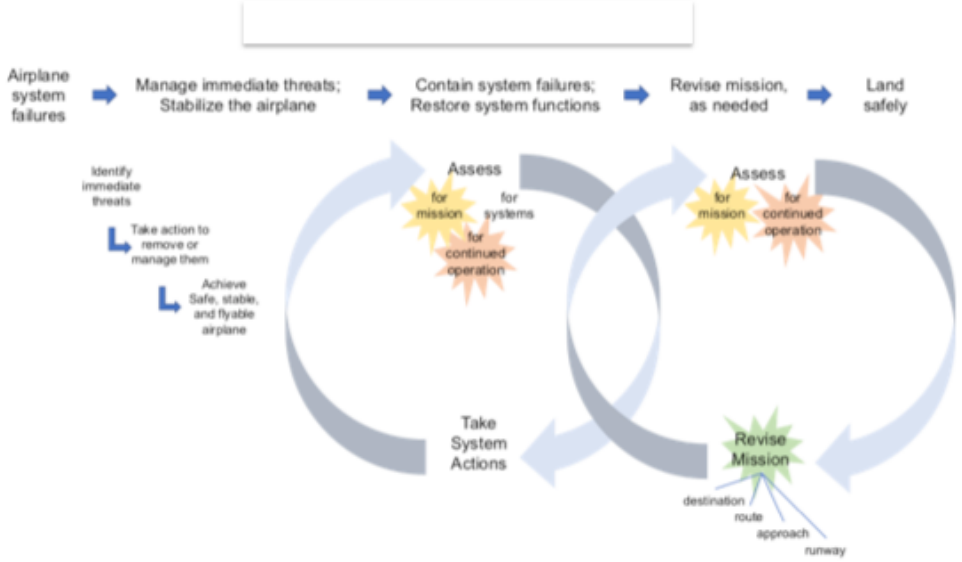


Figure 1. Managing airplane system failures.

For the middle performance cycle, the flight crew can, ideally, assess the situation to determine if it makes sense to continue on with the mission, if the airplane systems would benefit from further actions, and what limitations there are for continued flight (Note that the items with the colored "splat" under them [e.g., "for mission"] are items that are addressed by the work described here.) Figure 2 provides a more detailed view of these.

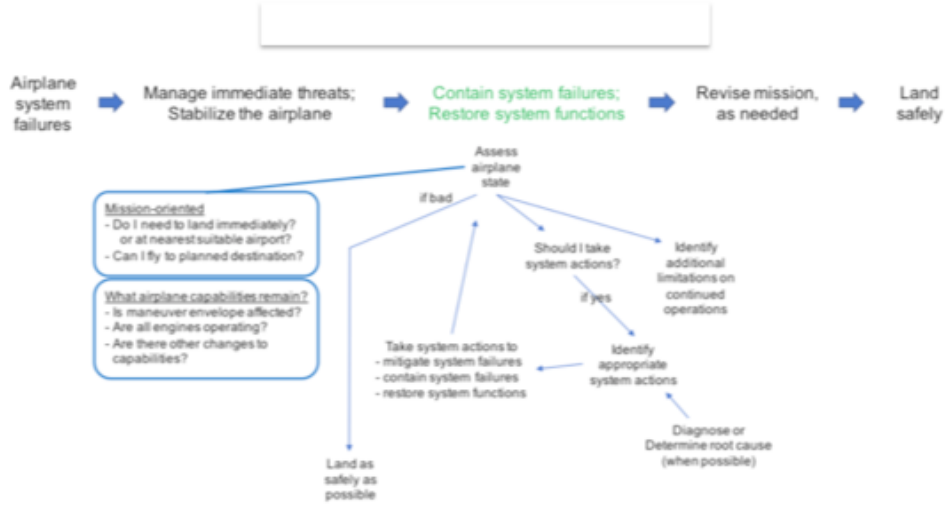


Figure 2. Managing airplane system failures (detail 1).

For the right-hand cycle, the flight crew has done all they can with actions on airplane systems, and they are now more focused on the mission. Assessment continues for determining if the mission can still be supported and additional limitations for continued flight. This assessment serves to revise the mission, if needed. These revisions can be minor (a change to the approach) or major (a diversion to a different airport). Figure 3 provides a more detailed description of this activity.

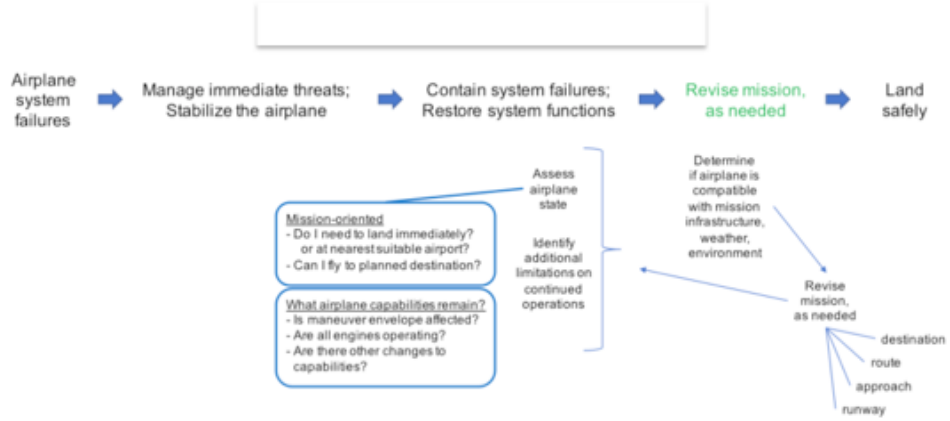


Figure 3. Managing airplane system failures (detail 2).

In the next section, we look at existing jet transport airplanes to see how well they support these activities.

3. Current Schemes for Managing Non-Normals

We looked at recently-produced flight decks from each of the major airplane manufacturers (OEMs) to identify the following in terms of how the interface supports managing non-normals:

- What interface displays are used?
- Are non-normal (alert) messages reduced or consolidated in an attempt to identify issues more central to the failure?
- How are messages prioritized?
- Can the flight crew easily see the full set of alert messages?
- Can the flight crew select any NNC they think is most important?
- Does the system generate any information about operational consequences?
- How are changes to operational limitations or consequences presented to the flight crew?

3.1 Boeing 787

What interface displays are used?

- The EICAS (engine indications and crew alerting system) is used to display non-normal (alert) messages (see Figure 4; specifically, the display just to the right of the narrow NAV display).
- The ECL (electronic checklist) display. This is where the non-normal checklists are displayed and executed. When there is a non-normal message that has an associated checklist, and the pilot presses the CHKL button on the Display Select Panel, the checklist is automatically presented on a multi-function display (MFD). If multiple EICAS alerts are displayed with associated checklists, when the CHKL button is pressed, a queue of checklists is presented for the pilot to choose among.
- Synoptic displays. These displays, which provide a schematic of the airplane system, can be selected onto one of the MFDs. There is no requirement to use a synoptic when performing a non-normal checklist.

Figure 4. Boeing 787 displays.

Are non-normal (alert) messages reduced or consolidated in an attempt to identify issues more central to the failure?

- EICAS messages are not eliminated or reduced, but there can be reductions in the messages that have an NNC associated with them. For example, the NNC called ELEC GEN DRIVE L1 contains the command, "Do not perform ELEC GEN OFF checklist." Thus, the ELEC GEN OFF NNC is removed from the ECL queue when ELEC GEN DRIVE L1 message is active. The ELEC GEN OFF message will remain in the EICAS queue but the square icon, which indicates an NNC exists, will be removed.

How are messages prioritized?

- Alert messages are assigned one of the following levels:
  - Warning: The highest level of failure indicating a condition that requires immediate flight crew awareness and action. This failure indication is color-coded red and has an associated continuous aural warning (Master Warning) that can be cancelled manually.
  - Caution: This failure indication defines a condition that requires immediate flight crew awareness, but may not require immediate action. It is color-coded amber with a single-occurrence aural warning (Master Caution).
  - Advisory:This failure indication is also color-coded amber but is indented to the right from the Caution-level messages; there is no associated aural alert. An advisory-level message requires awareness and may require flight crew action.

These levels drive prioritization such that, in the EICAS queue, all warnings are presented above cautions, and cautions are presented above advisory messages. As EICAS messages occur (i.e., are added to the queue), they are presented with the most recent at the top of the queue but only within each alerting category.

Can the flight crew easily see the full set of alert messages?

Yes, all messages can be viewed. If there are more than 12 EICAS messages, they are put on a second page and it requires paging down to see them.

Can the flight crew select any message (NNC) they think is most important?

Yes, the flight crew can select any NNC from the ECL queue (or select an ECL not in the queue). When an EICAS message is displayed, a white square (a checklist icon) appears next to it if there is an associated checklist to be accomplished. When the pilot presses the CHKL button on the Display Select Panel (DSP), the checklist is automatically presented on an MFD. If multiple EICAS alerts are displayed with checklists for accomplishment, when the CHKL button is pressed, a list of checklists (the NNC queue) is presented for the pilot to choose among. These are presented in the order of the EICAS messages.

Does the system generate any information about operational consequences?

Yes. Within each NNC there are "operational notes" which (generally) identify on-going consequences of the failure or changes to the operational limitations for the airplane.

How are changes to operational limitations or consequences presented to the flight crew?

There is a section called NOTES and all operational notes from each active NNC are collected and can be displayed at any time. There is a NOTES softkey on the ECL display.

3.2 Airbus A380

What interface displays are used?

There is a central display called the ECAM Warning Display (EWD) (top display in Figure 5), which is the lower half of the engine indications display. The EWD provides an area for showing ECAM (electronic centralized aircraft monitoring) messages and the associated NNC steps. On the EWD, 18 lines are available for the display of ECAM messages (or steps of the associated checklist).

A downward green arrow appears at the bottom of the EWD display to indicate the presence of ECAM messages of a lower priority when more alerts and checklist items exist than can be displayed (i.e., more than 18 lines worth of information). As displayed items are accomplished and their associated alerts cleared, the lines below scroll up on the display.

Below the EWD is a Systems Display (SD) (lower display in Figure 5). System synoptics are automatically displayed in the SD, which show the status of the malfunctioning system and the effect the crew actions are having on it as checklist steps are accomplished. Although a system synoptic is displayed automatically when an alert for a specific system is displayed, the pilots can also manually select a synoptic to be displayed.

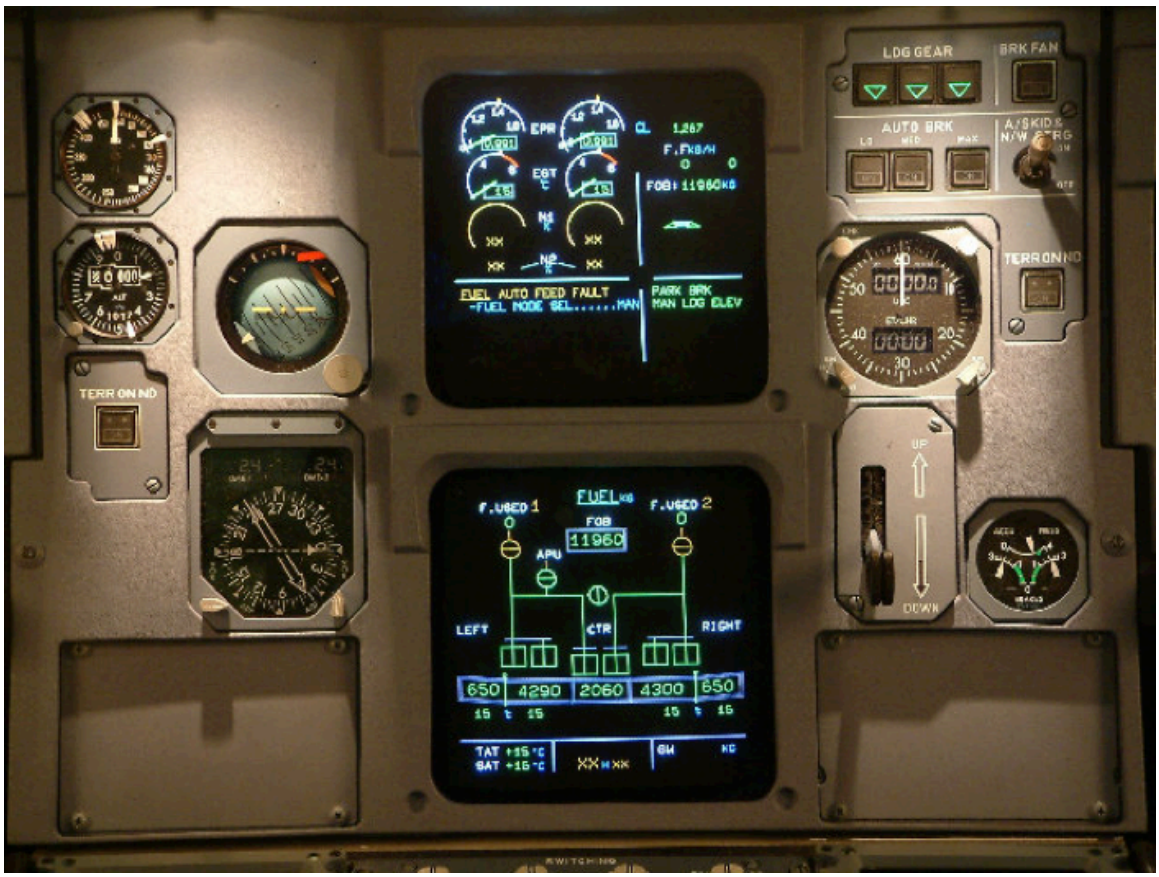


Figure 5. Airbus ECAM displays.

Are non-normal (alert) messages reduced or consolidated in an attempt to identify issues more central to the failure?

Yes, alert messages that would be generated from actions in another NNC will be inhibited. For example, when an ELEC GEN failure occurs, the ELEC GEN FAULT alert message will be displayed on the EWD. And, the associated ELEC GEN FAULT NNC will be displayed just below the alert message. That particular NNC requests that the Generator be turned to OFF. In this case, because that was an action from the NNC, the EWD will inhibit the ELEC GEN OFF message from the EWD. Normally, if the Generator were OFF, there would be an alert message on the EWD.

How are messages prioritized?

When airplane system failures occur, they generate a message at one of the following levels:

Level 3: The highest level of failure indicating an impact on the safety of the aircraft. This failure indication is color-coded red and has an associated aural warning (Master Warning) along with illumination of the Master Lights (red). The recommended crew action is to respond immediately to the warning.

Level 2: This failure indication defines an abnormal condition. It is color-coded amber with a different aural warning to that of a Level 3 failure (Master Caution), also with the Master Lights (amber). The recommended crew action is to be aware of the condition and then take appropriate action.

Level 1: Defined as a degradation in an aircraft system, this failure indication is also color-coded amber but there is no associated aural or visual alerting. The recommended crew action is to be aware of the condition.

When there are several failures, they are displayed in order of priority, determined by the level of the alert and its importance within that level. Airbus operational philosophy means that each NNC, in order of importance, should be completed by the flight crew before they move onto the next NNC. If the flight crew were performing actions from an NNC for a lower-priority alert when a higher-priority alert occurred, actions associated with the higher-priority alert would be displayed and actions associated with the lower-priority alert would be pushed down in the queue for later completion.

More generally, the flight crew is supposed to apply actions in the following order (unless they determine this is not appropriate):

- memory items
- Operations Engineering Bulletin (OEB)
- sensed ECAM, which produce ECAM messages on the EWD
- not-sensed ECAM, which do not produce ECAM message
- Quick Reference Handbook (QRH); the paper-based version of any non-normal checklist

Can the flight crew easily see the full set of alert messages?

For the A380, the flight crew is not able to look beyond the current ECAM messages that are presented to them on the EWD. They can see only the set of ECAM messages that can be displayed in the 18 lines, but if there is more information, they cannot look further down the queue. The A350 makes it possible to scroll down through the ECAM messages, and this upgrade may be applied to the A380.

Can the flight crew select any message (NNC) they think is most important?

For the A380, the flight crew is expected to work through the NNCs in the order they are presented, and the NNC is only displayed for the top-most alert message. However, it is possible for the flight crew to skip past an alert/NNC to perform a later NNC and then recall the alerts that were skipped.

Does the system generate any information about operational consequences?

Yes, via the STATUS page (see Figure 6). The STATUS page provides an operational summary of the aircraft status after the EWD has displayed a failure. It provides:

- deferred procedures and the phases in which they apply
- limitations
- information on any degraded aircraft system
- inoperative systems
- list of active alerts that have an impact on the landing distance or landing
- indication that a STATUS MORE page exists, in order to provide additional information related to the flight crew about the aircraft status (system redundancy losses, cautions cancelled, or MORE INFO to a procedure)

Note also, the Onboard Information System (OIS) helps identify changes to landing distance. The LDG PERF (landing performance) application for the computation of landing performance following in-flight failure is driven by the ECAM. In other words, the ECAM automatically feeds the LDG PERF computation with the faults affecting landing distance.

How are changes to operational limitations or consequences presented to the flight crew?

Through the various elements of the STATUS page (see above), shown in Figure 6.

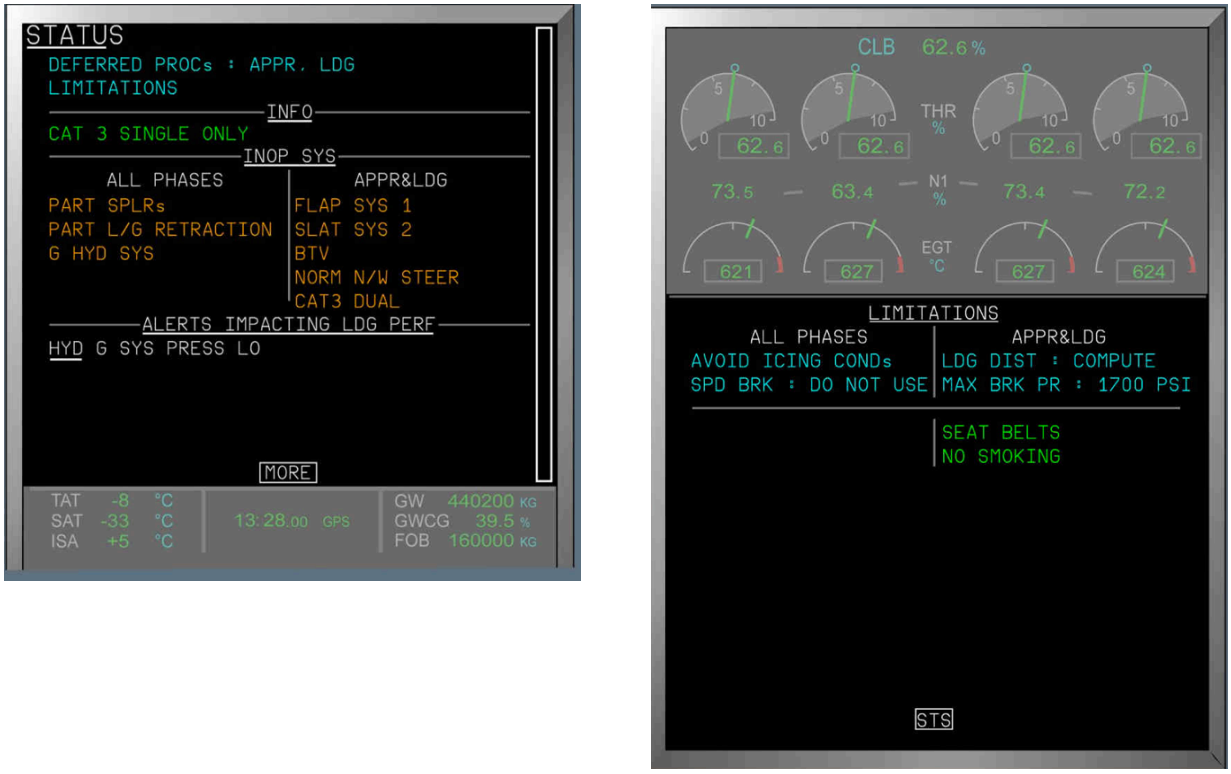


Figure 6. Airbus STATUS displays.

3.3 Embraer ERJ 170/190 (First Generation Primus Epic)

What interface displays are used?

There is a single central EICAS screen that contains a crew alerting system (CAS) field, which displays alerting messages. The glareshield of the instrument panel contains two Master Warning pushbuttons and two Master Caution pushbuttons. These provide flashing illumination concomitant with EICAS Warnings and Cautions, as well as the means to acknowledge and cancel such indications.

The ECL display and system synoptic pages can be displayed on MFDs. Each display is equipped with tabs that provide access to specific items. For the ECL display, a pilot can access normal, non-annuciated, abnormal, emergency, and user-defined checklists.

Are non-normal (alert) messages reduced or consolidated in an attempt to identify issues more central to the failure?

Systems malfunctions that generate multiple consequential messages are displayed with an accompanying chevron to indicate that they are "root" EICAS messages.

How are messages prioritized?

The categories of CAS message prioritization are as follows, in descending order of urgency:

- Warning: Annunciated in flashing inverse red video on the EICAS, synoptic page, and ECL, and accompanied by the two flashing Master Warning lights, recurring triple chime, and possible additional aural indications. Warnings are serious malfunctions or conditions that require immediate crew action to avoid potential loss of life and/or destruction of the aircraft.
- Caution: Annunciated in flashing inverse amber video on the EICAS, synoptic page, and ECL, and accompanied by the two flashing Master Caution lights and a recurring single chime. Cautions are categorized as conditions that require immediate crew awareness and crew action, but not necessarily an immediate response.
- Advisory: Annunciated in flashing inverse cyan video on the EICAS for five seconds. Advisory messages indicate operational or airplane conditions that require crew awareness. Subsequent or future crew action may be required.
- Status: Annunciated in flashing inverse white video on the EICAS for five seconds. A status message indicates the status of a system of which the crew might wish to be aware.

All messages of the most urgent category of priority are displayed at the top of the EICAS, followed by all messages at the next lower level of urgency, and so on. Within a prioritization category, the most recent message is displayed at the top.

Can the flight crew easily see the full set of alert messages?

Yes, but if there more than 22 CAS messages, scrolling is required to see the messages that are out of view. The number of off-screen messages is listed at the bottom of the CAS field.

Can the flight crew select any message (NNC) they think is most important?

In the ECL, checklists for abnormals appear in the same order as on the EICAS screen. A pilot can select an ECL checklist related to any particular abnormal in order to deal with a situation that has been assigned a higher priority.

Does the system generate any information about operational consequences?

We were unable to get information from Embraer about this capability

How are changes to operational limitations or consequences presented to the flight crew?

We were unable to get information from Embraer about this capability

3.4 Bombardier C-series

What interface displays are used?

There is an EICAS display that presents all non-normal messages. There is an ECL page that can be called up (on a multi-function display) to work through normal or non-normal checklists. There is a Synoptic page, which has the following pages that can be displayed: STATUS, AIR, DOOR, ELEC, FLT CTRL, FUEL, HYD, AVIONIC, INFO and CB.

The ECL page has several tabs. It defaults open to the SUMMARY tab, which has an upper and lower half. The upper half shows the set of normal checklists for the current phase of flight, and identifies which have been completed and which should be performed next. The lower half presents the set of Warning and Caution checklists to be performed (at the top of the lower half), and the history of what has been performed (lowest part) and any limitations.

The ECL has a NORMAL tab, which lists all of the normal checklists and shows whether they have been started or completed. It also shows any limitations. The pilot can select any normal checklist to perform.

The ECL has a NON-NORMAL tab, which provides a listing of systems and shows, through red or amber color-coding, which systems have non-normals. For example, if there is an engine fire, the text "Power Plant" (in the list of systems) would be red (for Warning). Clicking on Power Plant shows all of the Power Plant-related EICAS messages, and ENG FIRE would be in red. Clicking on ENG FIRE would open the ENG FIRE checklist. Note, also, that the ENG FIRE EICAS message would also be on the lower half of the SUMMARY tab. The NON-NORMAL page would also list limitations at the bottom of the page.

Are non-normal (alert) messages reduced or consolidated in an attempt to identify issues more central to the failure?

Yes. When an NNC will accomplish the actions of a secondary NNC, the secondary NNC is removed from the EICAS messages.

How are messages prioritized?

Alert messages are of one of the following levels:

- Warning: The highest level of failure indicating a condition that requires immediate flight crew awareness and action. This failure indication is color-coded red and has an associated aural warning (Master Warning).
- Caution: This failure indication defines a condition that requires immediate flight crew awareness, but may not require immediate action. It is color-coded amber with a different aural warning to that of a Warning (Master Caution).
- Advisory: There are no pilot actions required for Advisory messages.

EICAS messages are listed in the order of most recent at the top of the queue. Also, all warnings are presented above cautions, and cautions are presented above advisory messages. This prioritization emphasizes urgency.

There is a "priority" pointer (on the SUMMARY tab) that "recommends" an NNC for performance. The pilot can select another NNC instead of the one with the priority pointer. Priority is determined primarily by urgency but there are other factors as well.

Can the flight crew easily see the full set of alert messages?

Yes. The EICAS display shows all messages and the pilot can scroll/page down to see them all. They also appear on the SUMMARY tab.

Can the flight crew select any message (NNC) they think is most important?

Yes. The SUMMARY tab shows all of the NNCs, and the pilot can select one for the ECL to perform. Further, the NON-NORMAL tab will also list all of the EICAS messages, under their system names, and the pilot can select one from there for execution.

Does the system generate any information about operational consequences?

Yes. Operational limitations are presented on the SUMMARY tab and on the NON-NORMAL tab.

How are changes to operational limitations or consequences presented to the flight crew?

The SUMMARY tab has a section that lists all of the operational limitations that have been identified through performing the NNCs. These are arranged by NNC on the SUMMARY tab. Operational Limitations come from each NNC and there is no attempt to resolve redundant or conflicting items. The pilot needs to resolve any conflicting or redundant items.

Note that if the pilot does not complete an NNC, the operational limitations items from that NNC will not go to the SUMMARY tab. Also, there are "notifications" in the NNCs that call out issues, such as implications for increased landing distance or speed restrictions. These do not get passed to the SUMMARY tab but they do get passed to subsequent normal checklists, such as Before Landing.

3.5 Gulfstream G500

What interface displays are used?

There is a CAS that presents alerting messages; this information is typically on a centrally located display (Figure 7; display #3 is circled; the upper left 1/6 of the display is where the CAS would be presented). The ECL display can be also be placed on any 1/6 window. Typically it is on display #3, lower 1/6 window. Only normal checklists are displayed through the ECL display at this time (future software will put non-normal checklists in ECL). The ECL does not always have to be displayed. Non-normal checklists can only be accessed via the Airplane Flight Manual (AFM), in either paper or electronic form (iPad). Thus, there is no interaction between CAS and the non-normal checklists.

Synoptic displays can be viewed using one of the MFDs (display #2, display #3). There is no requirement to use a synoptic when performing a non-normal checklist.

Figure 7. Gulfstream displays (from a G500). © Gulfstream Aerospace Corporation.

Are non-normal (alert) messages reduced or consolidated in an attempt to identify issues more central to the failure?

Yes, some sets of messages are consolidated through an umbrella message, which is an alert message that is presented in lieu of two or more alert messages that share a common cause (see FAA AC 25.1322-1). More specifically, umbrella messages identify CAS messages that are downstream consequences of a primary failure, so that it shows the "parent" failure but suppresses some of the "children" messages. Umbrellas CAS messages are denoted with "(U)" at the end of the message; e.g., APU Fire (U).

Some of the "children" (consequential) messages may be presented with the umbrella message. If they are, they are denoted with ">" at the beginning of the message; e.g., >APU Fail. However, consequential alert messages are only displayed when they are judged to provide useful information to the flight crew regarding failures in one of the following areas:

- flight envelope
- flight or ground controls
- cabin pressurization system (CPCS) or environmental control system (ECS)
- loss of annunciations or alerts

Consequential alert messages that are not tied to those types of failures are inhibited on the CAS. However, the non-normal checklist in the AFM will show the full set of consequential messages so the ones that were inhibited on the CAS will be revealed in the AFM.

How are messages prioritized?

Alert messages are of one of the following levels:

- Warning: The highest level of failure indicating a condition that requires immediate flight crew awareness and action. This failure indication is color-coded red and has an associated three-bong aural warning (Master Warning) that can be cancelled manually via the Master Warning push button. The CAS message will flash continuously until acknowledge via the Master Warning push button.

- Caution: This failure indication defines a condition that requires immediate flight crew awareness, but may not require immediate action. It is color-coded amber with a double-bong aural warning (Master Caution).
- Advisory: This failure indication is color-coded cyan and has an associated single-bong aural warning. An advisory-level message requires awareness and may require flight crew action.
- Status: This indication is color-coded white and has no associated aural warning; e.g., PARKING BRAKE ON.

These levels drive prioritization such that all warnings are presented above cautions, cautions are presented above advisory messages, and advisory above status. As CAS messages appear (i.e., are added to the queue), they are presented with the most recent at the top of the queue (but within the Warning/ Caution/Advisory/Status categories).

Can the flight crew easily see the full set of alert messages?

Yes, all messages can be viewed. The CAS window is sized to accommodate 13 lines. It will expand as required to accommodate 17 lines. If there are more than 17 alerts, the "overflow" messages can be seen by scrolling down. The umbrella CAS will collapse (removing any consequential messages) to show only the warning messages if needed to ensure all red messages are viewable in the window.

Can the flight crew select any message (NNC) they think is most important?

Yes, the flight crew can select any non-normal checklist, which can be found in the AFM. The ECL display does not yet cover non-normals.

Does the system generate any information about operational consequences?

No, CAS does not generate this information. Within each NNC in the AFM there are operational notes, cautions and warnings, which (generally) identify operational consequences of the failure or changes to the operational limitations for the airplane.

How are changes to operational limitations or consequences presented to the flight crew?

The CAS does not generate this information. Within each NNC in the AFM there are operational notes, cautions and warnings, which (generally) identify on-going consequences of the failure or changes to the operational limitations for the airplane. These items are not brought to the flight crew; the flight crew will only find them by working through the NNCs.

3.6 General Characteristics of the Current Systems

While there are some differences across OEMs, there are many similarities in the current non-normal alerting and management systems, which can be characterized with the following statements:

- *Non-normal messages (airplane system alerts) are presented to the flight crew in terms of failures to airplane system components*. In addition to the Boeing 787 interface description described above, we also reviewed the almost 450 Warning, Caution, and Advisory messages used in that airplane. All but 19 of those messages are about failures or losses in physical systems; e.g., a hydraulic system. The remaining 19 are related to losses in airplane capability or functionality; e.g., loss of autoland capability. Further, a recent accident investigation (see ATSB, 2013) revealed that, in the A380, system alerts are

sometimes at a very low level of system description. For example, a Qantas event generated messages such as:

- A-ICE ENG 1 VLV OPEN
- HYD Y ENG PMP A PRESS LO

That is, these messages, in some cases, are reporting changes at the level of individual pumps and valves. Thus, while there are examples in which recent airplanes report a few failures from a more functional perspective, the overwhelming set of messages are tied to airplane system components.

- *When multiple failures occur, flight crews are required to address these failures one at a time*. With a few exceptions (e.g., the Gulfstream G500/600), which does try to suppress some messages when they are judged to be consequential (downstream) of another failure, non-normal messages are presented in a queue to be addressed one at a time. In fact, in the Airbus A380, the flight crew is forced down a path to work through the NNCs in the order they are presented (there is a way around that requirement, but it is more cumbersome). Other airplanes are not so restrictive in determining order. Generally, however, the primary philosophy is to perform these NNCs in the order in which they are presented.However, a review of all of the messages can sometimes provide better information about which non-normal checklist should be performed first.

- *The non-normal message system (alerting system) is linked with electronic checklists that allow the flight crew to identify and perform the appropriate NNCs*. Other than the Gulfstream, these airplanes have largely removed the need to pull out a large, paper binder (QRH) to find the appropriate NNC, which improves efficiency and eliminates the chance that the wrong NNC will be used. However, there are differences in whether the ECL version can be tailored for each operator. Boeing allows operators to edit/tailor the NNCs within the ECL. Airbus does not allow operator tailoring and, therefore, in some cases, individual operators require their flight crews to work through the generic ECL version and then also work through a more operator-tailored QRH version, which is paper-based.

- *Generally, flight crews can select any NNC to perform*. Alerting systems, with the exception of the Airbus, allow the flight crew to identify which NNC they should perform, based on their assessment of what is most appropriate. There is an ordering tied to level (Warning/Caution/Advisory or 3/2/1) but flight crews can deviate from that ordering if they judge a different order to be more effective. (Note that the Airbus system also makes this change of order possible but it requires more actions from flight crews who want to deviate from the prescribed order.)

- *Changes to operational limitations are generated out of NNCs but not integrated with mission information*. In each airplane's alerting scheme, the NNCs identify changes to the airplane's operational limitations tied to the failures. Some systems pull limitations together and make them easier to find. However, these limitations are generated from each NNC and are not integrated; more specifically, there is no attempt to resolve conflicting guidance or remove redundancies across NNCs. In the case of Airbus, these limitations are linked to a phase of flight and are easier to apply to operations, but for other OEMs, they are tied to the checklist that generated them. It is still the role of the flight crew to manage the integration of the different sets of limitations and to determine how these limitations affect continued safe flight and landing. Shifting more toward a larger set of operational

decisions, recent Airbus airplanes have done a better job of linking failures to changes in landing distance, but, more generally, that analysis is left to the flight crew.

The approach to reporting and managing airplane system faults that is characterized by these five statements is driven by a number of factors:

- There is a long history of reporting at the level of airplane system components. At one time, this is all that was possible, and it was easier for pilots to use that information. Airplane systems were simple, and pilots had detailed knowledge of those systems. Pilots wanted to know which system components had failed because they were able to reason through the system to determine the operational consequences. As we describe in Section 4, however, there have been significant changes to the complexity of transport airplane systems and to the typical pilot's understanding of those systems.
- The technology was not in place to integrate information from the operational environment with airplane system information so that operational decision making could be better supported. Notice to Airmen (NOTAM), weather information, and information about the various resources in the world existed only on paper.
- Diagnosis of airplane system faults is complex. Looking at the various reported failures and determining what occurred to generate them all is difficult. It is even more difficult when the initial failure is the result of something external to the airplane, such as a bird strike or uncontained engine failure. Certainly, some progress has been made in identifying the "root" messages, but this can fall short of identifying root cause.

This difficulty has created a gap that flight crews try to fill. The OEM philosophy is typically that the airplane system alerts are to be addressed one at a time, in the order they are presented. However, pilots eventually learn that, if they have enough experience or a good understanding of the system, it may be possible to identify the optimal checklist to perform. In some cases, the best NNC may be one that is not listed. There is at least one case in an older Boeing airplane in which a failure led to six engine-related EICAS messages, but the optimal reponse from the flight crew was to perform an "unannuciated" checklist (Engine Fail)—that is, an NNC that is not indicated by the EICAS. So, in this case, the flight crew should not perform any of the NNCs associated with the EICAS messages, but should perform a different NNC.

This minor dilemma can be more broadly described as tension between:

- relying on the engineering analysis and following the procedures that the alerting system provides vs
- understanding what is happening in the system and selecting the best response to that system state

Research from a process-control setting has shown that system operators, despite having no encouragement to do so, will attempt to develop their own understanding of how the system is being affected and use the non-normal procedures to address the problems as they understand them (see Roth, Mumaw, & Lewis; 1994; Vicente, 1999).

The foregoing characterization represents the most recently designed transport airplanes, and it reveals that OEMs, generally, have taken steps toward better integration of failures into an operational framework. However, the primary language of these alerting systems is still airplane

system components. The effort described here is an attempt to replace that framework with a different one that more directly flows from operational functionality.

4. Technology Changes and New Challenges

Every pilot is required to be trained on airplane systems. At one time, several decades ago, these systems were fairly simple and had few interactions between sub-systems. For these systems, many pilots could use their training to reason through the system and determine what airplane system component failures meant for how to operate the airplane.

However, recently developed transport airplanes (e.g., Boeing 787, Airbus 350, Gulfstream G500, Bombardier C-Series) have a dramatically different system architecture. There are more shared resources that interact with multiple systems and the systems themselves are more interconnected. For example, an air data sensor failure can lead to the airplane dropping into a "degraded" operational mode, such as from normal law to alternate law, which changes system performance in a number of ways. These changes lead to an exponential increase in complexity for pilots trying to reason about the operational consequences of airplane system failures.

Unfortunately, it is probably not possible to increase pilot training on airplane systems adequately to compensate for this additional complexity. We believe that the pilots of these new airplanes will be unable to anticipate how airplane system failures will propagate through systems and affect airplane performance. In fact, we are already seeing this.

The following cases illustrate how pilots are sometimes unable to understand the consequences of system failures:

- *Incident: American Airlines 268, Boeing 757; Sept 22, 2008*. On a flight from Seattle to New York, during cruise, an electrical system alert appeared on EICAS: STANDBY BUS OFF. The flight crew followed the relevant QRH procedure and turned the standby power selector to the BAT position (battery). The QRH procedure also stated that, "The battery will provide bus power for approximately 30 minutes." The airplane systems stabilized with several items inoperative and the captain contacted maintenance technical support and subsequently elected to continue the flight on battery power. The flightcrew then reviewed the MAIN BATTERY CHARGER procedure referenced in the QRH.

  Approximately 1 hour and 40 minutes later, still in cruise flight, the battery power was depleted at which time several cockpit electrical systems began to fail. The airplane was over western Michigan and the captain elected to turn around and divert to Chicago (ORD). The battery depletion led to the loss of a number of systems, including the cabin public address, making it impossible for the flight crew to call the cabin crew; elevator and standby elevator trim systems; and automatic deployment of the thrust reversers and spoilers. The airplane landed at ORD, failing to stop on the runway. The airplane was evacuated but the crew was unable to shut down the engines. None of these failures was anticipated by the flight crew or the American Airline (AAL) maintenance support.

- *Multiple incidents: 787 error messages*. In the first several months of entry into service for the Boeing 787-8, the new airplane operators were getting many EICAS (alert) messages tied to the airplane's computer systems. While these messages did not have any operational implications—the airplane could operate normally—pilots were uncertain about the importance of the messages. In many cases, the flight crew chose to do a turn back or not

perform the mission. While this was not a safety issue, it was a significant expense to the operators because they did not understand the significance of the messages.

- *Accident: Qantas 32, Airbus A380; Nov 4, 2010*. This four-engine airplane took off out of Singapore, headed to Sydney. During the climb out, engine #2 exploded due to an internal crack in an oil line. The explosion sent virtual shrapnel into the left wing and left side of the airplane, damaging a number of other airplane systems. Over a period of the next hour, there were more than 80 ECAM (alert) messages generated. Fortunately the flight crew that day was supplemented by several Check Captains, resulting in a total of five experienced pilots on the flight deck.

  Due to the nature of the A380 ECAM system (see Section 3), there was no opportunity to get a "big picture" view of all of the airplane system failures. Generally, they had to work through NNCs one at a time. The airplane, although badly damaged and leaking fuel, was flyable. However, the flight crew became frustrated that they did not have a good understanding of what had failed and what was working. The Captain, Richard DeCrespigny, at one point said, "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'". Over a period of almost two hours, they were able to get a sense of what they had and were able to return to Singapore and land, stopping with little room left on the long runway.

- *Accident: Northwest Airlines 1495; Douglas DC-9; May 10, 2005*. The DC-9 had a failure, leading to low pressure on the right hydraulic system, but continued to the planned destination and was able to land safely. After landing and crossing the runways, one of the pilots shut down the left engine as they were taxiing. Braking, steering, and the thrust reversers are powered with the hydraulic system, which in turn, is powered by the engines. Shutting down the left engine removed power to the left hydraulic system, which was the only remaining hydraulic system. Thus, from the engine shut down, they lost braking, steering, and, eventually, the thrust reversers. They were unable to stop forward progress and ran into (in slow speed) another airplane. Due to a fuel leak from the other airplane into the DC-9, they had to evacuate the airplane.

5. Derivation of Airplane Capabilities

There has long been a distinction made between the physical components of a system and the functions that those components perform (Rasmussen, 1983); for example, the safety parameter display system developed in nuclear power plants (Woods, Wise, & Hanes, 1982) that showed how well the plant was achieving essential operational goals, such as nuclear core cooling. An aviation example is the function of stopping an airplane after landing. To achieve this function, many transport airplanes use three airplane systems for slowing and stopping an airplane after it has landed: mechanical braking on the wheels, thrust reversers on the engines, and spoilers on the wings. Each of these airplane systems can contribute to the function of stopping the airplane. Airplanes, however, do not currently offer a functional view.

This distinction between physical and functional is useful for system operations because one can use the mapping between the two to solve system problems. When a system failure occurs, it is essential to understand how system functions are affected. The pilot's goal is to restore critical functions, and it is therefore important to understand what functions have been degraded or lost when a physical component fails and which backup or alternative system components can be employed to meet those

functions. Thus, if there is a failure to deploy the thrust reverser, the pilot needs to determine whether brakes and spoilers can stop the airplane before it runs out of runway.

To a large extent, the NNCs are designed to do this mapping for pilots. When a failure occurs, the NNC identifies the system actions needed to reconfigure airplane systems to restore the affected functions (among other things). In cases where the functions cannot be restored, the NNC informs the pilot that some functions are degraded or lost, saying, for example, that stopping will take more runway distance. Then, the pilot can revise the planned approach and manage the airplane to achieve a safe landing.

The NNCs use an implicit analysis of functions, but these functions are not communicated directly to the flight crew and applied to the mission. The primary language of the flight deck displays for managing non-normals is a language of physical components. So, an important element of our task here was to find a language for describing functions, or airplane capabilities, to pilots. We explored two different paths for developing that language.

5.1 Airplane System Functions

During transport airplane system design and certification, engineers and pilots conduct an analysis to determine how system failures are likely to affect airplane functions and how well the airplane can be reconfigured (or flown) to avoid a bad outcome. This analysis is typically applied to many single failures as well as to likely combinations of failures that could be tied to certain catastrophic outcomes. There is an explicit consideration of system functions in this analysis, which serves as a check on completeness for assessing operational effects on the airplane. The airplane functions that are typically considered for this analysis are (at a high level) the following:

- control and stabilize the airplane
- generate and control energy
- provide awareness of the airplane for the operators
- navigate
- communicate
- surveillance
- manage the environment in the aircraft
- support response to emergencies (such as fire extinguishing)

Airplane system designers work through this analysis to ensure that airplane system failures can be managed or mitigated through pilot actions (specifically, pilot actions that a typical pilot is capable of performing). In the final analysis, the designers try to make a case that the indications, alerting schemes, and operational procedures are sufficient to aid a trained pilot in managing or mitigating the full set of failure cases.

Important to the current discussion is that the system designers work from a set of system functions that are appropriate for any jet transport airplane. These functions capture the essential capabilities that any jet transport airplane should support. Thus, this function set serves as a starting point for the types of airplane capabilities that pilots could also use.

5.2 Abstraction Hierarchy

The Abstraction Hierarchy (AH) is a framework for representing the operation of a complex system (Rasmussen, 1983; Vicente, 1999). This framework provides an explicit mapping between the physical system components and their functional purpose. There are five levels of abstraction:

1. *Physical form*. This level of system description captures the physical components of the system, their appearance, condition, and location. For example, pump #23 is located in hydraulic circulation system B.
2. *Physical function*. At the next highest level, is a description of the state of each physical component; for example, the valve is open, the heater is on, or the tank is empty.
3. *Generalized function*. This level describes states and behaviors of the subsystems formed as individual components work together. Examples are a liquid or gas flowing, creating thrust, or applying pressure through a hydraulic system to move control surfaces.
4. *Abstract function*. This level captures a more abstracted representation of the generalized functions. It captures how subsystems support the overall system purpose. For example, if the overall system purpose is transporting people or cargo, the system needs to be able to climb to a height where flight is efficient, it requires methods for modifying airspeed, it requires methods for sustaining life at high altitudes.
5. *Functional purpose*. At the highest level, this is a description of the purpose of the system in the domain. For a nuclear power plant, one purpose is to generate electricity. For a transport airplane, the primary purpose is to transport people or cargo.

One might think of lower AH levels as describing "what," middle levels as describing "how," and the top levels as focusing on "why." What is important about the AH is that it shows how physical systems and their operation get mapped to system functions. One intent of the AH is to provide a representation of the system that allows operators to relate the various AH levels (Vicente, 1999).

System interface designs for older systems (airplanes, nuclear power plants, etc.) were focused on the lower levels of the AH. That is, they showed the physical functions, which are states of physical system components (e.g., valve open, pump on) and the generalized functions, which are the operation of subsystems. Therefore, the work motivated by AH has attempted to offer effective representations at the higher levels, as well as attempts to bridge the levels; it asks, "How can you represent a physical system more in terms of the functions it is to perform and how well that function is being achieved?"

Dinadis & Vicente (1999) applied AH in a narrow way to only the engine/fuel systems to capture their purpose and the links between expected performance and system component failures. This effort was focused primarily on the latter aspect (links between physical and functional) to allow pilots to understand why airplane performance was not as expected after a component failed.

A recent project by Reitsma (2016) attempted to characterize jet transport systems at the higher abstraction levels. At the highest level, Reitsma identified two purposes: efficient air transport and safe air transport. It is not unusual for a high-level characterization of a system to identify these complementary purposes: "produce" and "operate safely." An AH analysis for a nuclear power plant is very similar at the top level. Indeed, sometimes these two purposes are treated as antagonistic; that is, ensuring safety may reduce or end productivity.

At the next level down, the abstract functions, Reitsma offers three functions:

1. Perform desired flight path, which reflects the physical constraints on the airplane's performance (or the operating space).
2. Accommodate payload, which reflects the constraints tied to the payload (passengers and cargo); e.g., maintaining a livable environment.
3. Emergency management, which reflects the airplane's ability to ensure survivability after an emergency has occurred.

The generalized functions, at the next level down, represent the subsystem functions that support the abstract functions. Interestingly, this function set is largely the same as the product of the systems engineering effort described in the last section. The abstract functions level is the bridge between the subsystem functions in a way to support the functional purpose; it should be a more operational view of how those individual systems are employed.

5.3 Function Framework

Our objective is to better support pilots in managing airplane system non-normals, and we need to develop a framework for describing functions. Using the AH language, the highest level of description is the functional purpose. The traditional AH functional purpose (for a transport airplane), as described here, is probably best expressed as "transport people and cargo." This highest-level purpose captures the system's purpose for all operations. However, for our effort, we chose to cast the system's purpose more narrowly, stating it in terms of *compatibility with the current mission*; e.g., "Am I able to fly from Boston to Chicago?".

The display we are imagining is meant to support pilots who have a specific mission and need to understand if that mission can be achieved. The mission may change—for example, a diversion for weather—and, if it does change, the new mission will become the new system purpose.

At the level below the functional purpose for Reitsma, there was a set of three abstract functions. We also tried to identify a relatively small set of functions that could quickly characterize the airplane's operational capability. The various attempts tended to hover around the types of descriptions that Reitsma used: airplane performance, range, ceiling, which are the elements that compose any mission. We failed to identify a small set that we believed would provide a useful characterization.

Working from the lower level of the AH—the integration of simple subsystem functions into more operationally relevant functions—we gravitated toward the larger set of functions that were used in the airplane systems safety analysis (Section 5.1). The status of these functions, such as stopping on the runway, comprise the characterization of the airplane below the mission level. This characterization captures *how well the airplane can perform any mission*. A guiding question for defining a capabilities set was: "If something fails, what are you not able to do that you would want to do relative to flying the mission?"

Because the mission may change, the pilots should have a display that reveals the ways in which the airplane is limited for performing other missions, if needed. Note that the limitations captured in this lower-level display may not be relevant to the current mission, which is why this display is secondary. For example, an airplane may no longer be capable of landing in a strong crosswind; but, if the weather in Chicago is calm, this limitation is not relevant to that mission.

Our framework, then, is a primary focus on compatibility with the current mission, and, secondarily, a characterization of how well the airplane can perform any mission. The next section describes a set of displays to support this framework.

6. Example Display Concepts for Supporting Assessment and Decision Making

To flesh out the framework, we developed a set of prototype displays concepts for five operational objectives. The first three are imagined as elements of a Mission Overview display. The next two could be implemented on a separate display that is easily accessed.

6.1 Mission Compatibility

The focus of this display is to show how compatible the airplane's current capabilities are with the specifics of the planned destination, as defined by what is in the flight management computer (FMC); this is the functional purpose. In some cases, the software will need to translate airplane system failures into operational consequences; e.g., airplane range or landing distance. This is not a trivial problem, but the focus here is on how to present information that is most meaningful to pilots, and not on solving those computational problems.

Specifically, the Mission Compatibility display creates an opportunity to identify incompatibilities in the following areas:

- *range/endurance:* determines whether the airplane is likely to be capable of reaching the airport for a safe landing. When it is judged that the planned destination cannot be reached (or should not be attempted), an appropriate message will appear:
  - land immediately (or land as soon as possible)
  - land at nearest suitable airport
  - XXXX [airport specifier] may be out of range
- *landing distance:* determines whether the airplane is likely to be able to stop prior to reaching the end of the runway; this will be expressed as a difference between estimated stopping distance and runway length.
- *approach/Departure/Arrival:* determines whether the airplane is capable of performing the departure and arrival and approach in the FMC.
- *airspace along the route:* determines whether the airplane is capable of the level of navigation required for using a certain type of airspace.
- *airport:* determines whether a specific airport is compatible with the airplane's capabilities.
- *runway:* determines whether a specific runway is compatible with the planned approach and landing distance.

For situations in which the airplane is judged to be compatible with the mission as defined in the FMC, this display provides graphical elements or text (in white) (see Figure 8a) to show basic mission information:

- airport
- runway
- approach
- departure or arrival (if it requires specific airplane capabilities)

The current prototype design shows incompatibilities or concerns about the ability to perform the mission, with corresponding display elements in amber (to reveal a concern) or a text specifier struck through with amber lines (to reveal that it is not available) (Figure 8b). Further, when there are changes that are relevant to the planned destination (from a source different than a compatibility), those will be shown through text messages (Figure 8c). Primarily, these will be changes related to weather or infrastructure that remove options or increase risk; for example, an ILS for the planned runway is out. In these cases, the display also identifies the source of the change information.

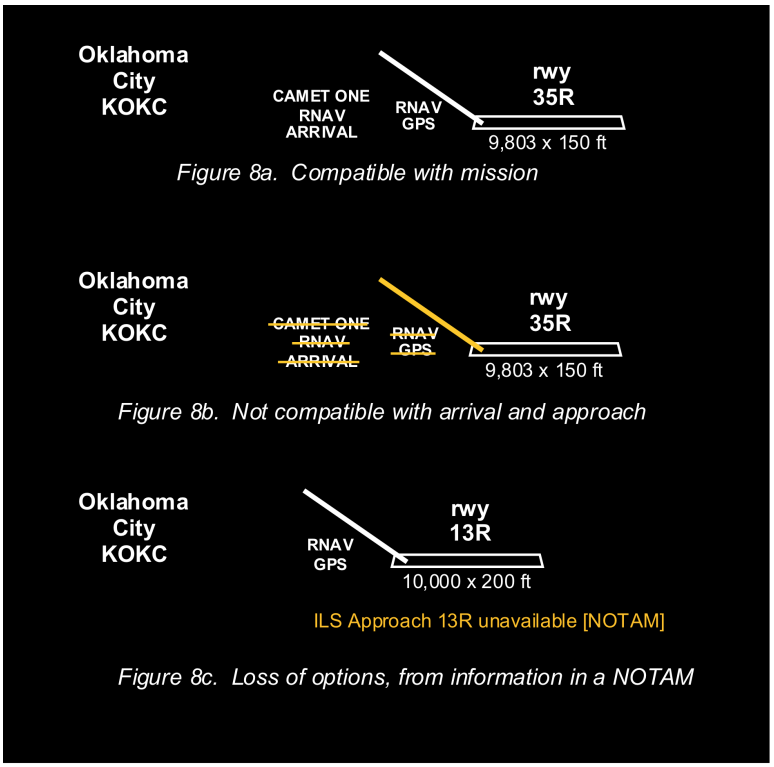


Figure 8. Compatible with (8a); not compatible with arrival (8b); loss of options (8c).

6.2 Airplane Capabilities

Airplane capabilities are intended to capture changes to the airplane's ability to perform essential functions. These capabilities are independent from the mission, and represent the abstract functions level of the AH. For example, if an airplane cannot maintain a survivable pressure and temperature in the cabin or cannot extend its landing gear, this will be true no matter the planned destination. The derivation of capabilities was described in Section 5.

One distinction to capture in specifying a loss of a capability is the difference between unable to perform vs not authorized to perform (from a regulatory perspective). For example, if an airplane loses one of two global positioning systems (GPS), it is not authorized to fly an area navigation (RNAV) approach, but it is still able to fly that approach. Therefore, in showing changes to capabilities, the display will use Unable or Fail to show the capability is lost because of equipment or system failures, and will use Not Authorized to indicate that a regulatory requirement is not met but the capability may still be available.

The following are the initial airplane capabilities that we examined for operational decision making with the prototype interface (note that it is not an exhaustive list):

- Autoflight. This is concerned with changes to the autopilot/autothrust/autoland capabilities. Potential messages are:
  - Autoland unable
  - Autopilot unable
  - Autothrottle unable
  - LNAV/VNAV unable
- Navigation. This is concerned with the navigation system's ability to determine a precise position for the airplane. Potential messages are:
  - Position precision unable
  - Required navigation performance standard unable
- Communication. This is concerned with changes in the ability to communicate with groups. Potential messages are:
  - Communicate flight deck unable
  - Communicate cabin/pressure altitude/crew intercom unable
  - Voice communication ATC unable
  - Data communication ATC unable
  - Voice communication Airlines Operations Center/Dispatch unable
- Land. This is concerned with the ability to land the airplane in the ideal configuration. Potential messages are:
  - Max landing weight exceeded
  - Landing gear retraction unable
  - Landing gear alternate extension
  - Jettison fuel unable
- Take Off. This is concerned with the ability to take-off. Potential messages are:
  - Take-off not configured-xxx, where xxx could be
  - Doors
  - Flaps
  - Gear
  - Gear steering
  - Parking brake
  - Rudder
  - Spoilers
  - Stabilizer
  - Insufficient fuel
- Approach Access. This is concerned with the ability to perform arrivals and approaches that may be required. Potential messages are:
  - RNAV GPS approach unable
  - RNAV not authorized
  - instrument landing system (ILS) approach Category I/II/III unable
- Airspace Access. This is concerned with the ability to use certain types of airspace. Potential messages are:
  - Reduced vertical separation minima (RVSM) airspace unable
  - RVSM airspace not authorized
  - Oceanic airspace unable
  - Oceanic airspace not authorized

  - Extended-range Twin-engine Operational Performance Standards not authorized (can only appear prior to take-off)
- Cabin/Cargo Environment. This is concerned with the ability to manage temperature, pressure, and air flow in the cabin or cargo area. Potential messages are:
  - Control temp cabin unable
  - Control temp cargo unable
  - Control pressure cabin unable
  - Control pressure cargo unable
  - Air flow cabin reduced
  - Air flow cargo reduced
  - Air flow cabin unable
  - Air flow cargo unable
- Ice protection. This is concerned with changes in the ability to protect against icing. Potential messages are:
  - Avoid icing conditions: engine
  - Avoid icing conditions: wing
  - Avoid icing conditions: window
- Landing Distance. This is concerned with capturing increases in landing distance. It is always expressed as an estimated increase in landing distance on a dry runway. Note that the mission compatibility display will integrate runway conditions and assess compatibility regarding landing distance. Potential messages are:
  - Landing distance increase = xx%
- Directional Control Runway. This is concerned with changes in the ability to steer the airplane on the ground. Potential messages are:
  - High-speed steering reduced
  - Low-speed steering reduced
- Fire Detection/Extinguishing. This is concerned with changes in the ability to detect and extinguish an on-board fire. Potential messages are:
  - Detection unable: xxx (where xxx is a region of the airplane)
  - Extinguishing unable: xxx (where xxx is a region of the airplane)
- Surveillance. This is concerned with changes in the ability to detect external threats. Potential messages are:
  - Windshear alerting fail
  - Traffic Collision Avoidance System (TCAS) alerting fail
  - Ground prox alerting fail
- Fuel Supply. This is concerned with the ability to get fuel to the engines. Potential messages are:
  - Fuel use unable
- Electric Power. This is concerned with the ability to provide electrical power. It shows when an electric power source is lost (or will be lost) or cannot be distributed. This is a "resource" item that can lead to changes in operational capabilities. Potential messages are:
  - Bus fail (specific bus)
  - Load shedding
  - Bus on battery power
- Hydraulic Power. This is concerned with the ability to provide hydraulic power. It shows when hydraulic power is lost (or will be lost) or cannot be distributed. This is a "resource" item that can lead to changes in operational capabilities. Potential messages are:
  - Hydraulic system x lost

  - Hydraulic system low pressure
- Pneumatic Power. This is concerned with the ability to provide pneumatic power. It shows when pneumatic power is lost (or will be lost) or cannot be distributed. This is a "resource" item that can lead to changes in operational capabilities. Potential messages are:
  - Pneumatic power lost
- Equipment Cooling. This is concerned with the ability to cool equipment, which will eventually lead to equipment failures. This is a "resource" item that can lead to changes in operational capabilities. Potential messages are:
  - Equipment cooling unable

Note that the last four capabilities, which are referred to as "resource" items, may be considered less important elements for supporting operational decisions. They are included because they aid in the flight crew's understanding of the "downstream" effects on operational capabilities, and it can be useful to understand that a source of power, such as hydraulic, has been lost. Having knowledge of the likely causes of a capability loss may help the flight crew be more effective in taking system actions to restore lost capabilities. For example, if equipment cooling failed, eventually there would be failures in systems such as the navigational computer. Instead of just showing the anticipated loss of a navigational capability, we are also showing the resource loss that precedes it to tell a more complete story.

There is also value in allowing the flight crew to understand in more detail why an airplane capability has been degraded or lost or is not authorized. The display allows the flight crew to either pull up the relevant system synoptic for cases of equipment losses, or to click for a pop-up box to reveal more detail about a loss of authorization. These activities are also an element of performing system actions in an attempt to recover the capability.

When airplane system failures lead to changes in capabilities, the appropriate messages will appear on the Mission Overview display next to an icon that was developed for its functional area (see examples in Section 7). An on-going design discussion is whether the description of the larger set of capabilities should be displayed at all times or only when those changes become relevant to the mission. On one hand is the belief that pilots should maintain an awareness of what airplane capabilities have been lost or degraded in case a mission change is needed. This awareness can guide pilot decision making in assessing possible mission changes (i.e., diversion airports). On the other hand is the push to minimize displayed information. A design philosophy that has had a significant role in shaping cockpit displays (as well as displays used in other modes of transportation) is the "quiet, dark cockpit" design principle (Sexton, 1988; Wiener, 1989). The "quiet, dark" approach tries to minimize active display data in normal operations so that indications of any off-nominal conditions stand out.

6.3 Maneuver Envelope

A major component of airplane capability is the airplane's ability to maneuver, or its maneuver envelope. The Maneuver Envelope display (see Figure 9) sets this capability apart from the other airplane capabilities. Specifically, this display element will show when airplane system failures lead to limitations in the following:

- maximum altitude, for example, due to an inability to pressurize
- airspeed (should not exceed a value, should not be less than a value)
- roll rate or roll authority
- bank angle
- pitch control
- elevator authority
- thrust
- thrust change rate
- slowing (e.g., inability to use the speedbrake)

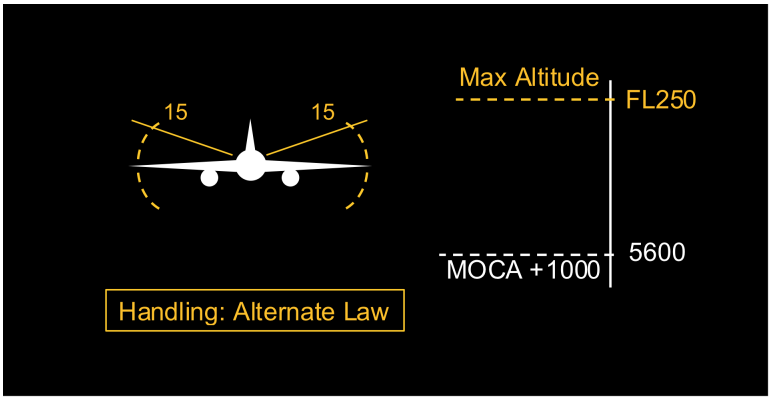


Figure 9. Maneuver envelope changes.

Another important element of the maneuver envelope for modern jet transports are changes to fly by wire, envelope protection or stability augmentation, which can result in the following types of issues:

- handling quality changes
- loss of alpha floor protection
- loss of bank angle protection

Ideally, these changes to the maneuver envelope would be presented through the primary flight display so that they are closely tied to relevant flight instruments. For the current prototyping, which assumes a retrofit into the existing flight deck displays, however, we are limited to indications on a separate display. The goal of this display element is to present the changes to the maneuver envelope in a compact manner.

This display element is not shown unless and until there are changes to the airplane's capabilities. Figure 9 illustrates the types of changes that could be captured; for example, a maximum altitude of 25,000 ft or a limit of 15° of roll. The element that has changed is shown in amber. The goal is to use separate display elements to show changes to airspeed, altitude, roll authority, pitch authority,

etc. In some cases, a message is needed to show the reason for the change in performance, such as a change in handling due to a drop into Alternate Law.

6.4 Operational Limitations by Phase of Flight

Airplane system failures can not only lead to changes in the airplane's ability to perform essential functions; these failures can also change the operational limitations on the airplane for continued safe flight and landing. The flight crew needs to understand the ways in which they should continue operating so they do not create additional problems for the airplane.

Traditionally, as illustrated in Section 3, NNCs identify only necessary changes that are tied to failures. The following are examples of operational limitations that are typically found in NNCs. They are arranged here by the relevant flight phase:

- Descent
  - Do not exceed 250 kts below 10,000 ft.
- Approach
  - Require runway visual range (RVR) more than 4000 ft.
  - Use flaps xx and V_{ref} xx on final approach.
  - Plan more time for slower flap operation.
- Land
  - Manual braking is required on landing.
  - Do not arm the speedbrake lever. This prevents inadvertent in-flight speedbrake extension. Manually extend the speedbrakes after landing.
  - Use normal flaps for landing. Maintain airspeed at or above 130 kts.
  - Position the flap lever to 1 and use V_{ref} 30 + 40 for landing. This ensures the slats are extended.
  - Do not land in a crosswind of more than 10 kts.
- Go-around
  - Use flaps xx for go-around.
  - The slats will extend beyond midrange when the airspeed is below 225 kts. For go-around, do not exceed 225 kts until the slats retract to midrange.
  - Limits on climb performance.
  - After gear is extended, it cannot be retracted.
- Taxi/Shutdown
  - Flap retraction is inhibited on the ground. Do not move the flap lever after landing.
- General not specific to a phase of flight)
  - Use long-range cruise (LRC) speed for diversion. Do not use FMC fuel predictions.
  - Move the thrust lever manually. Do not exceed the reduced thrust setting for the rest of the flight.
  - Do not exceed exhaust gas temperature (EGT) caution limits.
  - Run the engine at idle for the rest of the flight.
  - Do not exceed 270 kts.

When there are multiple failures, there can be a number of these operational limitations. Current airplanes take various approaches to identifying these and making them available to the flight crew. In the worst case, the flight crew has to recall them from each NNC that was used. In the best implementation, these operational limitations are collected and presented by phase of flight.

Our initial prototype interface is similar to the Airbus approach in that it collects the various items and orders them by phase of flight. This display, when accessed, will show the operational limitations for the current and next flight phases (as well as see limitations that apply to all phases). However, the pilot can also select one additional flight phase that is further in the future; for example, there may be a desire to see what limitations will be in play for landing. This display also shows the total number of items in each flight phase (when that phase is not displayed fully). And, for each limitation, it identifies the NNC it is tied to.

Figures 10 and 11 provide examples. In Figure 10 the airplane is currently in the cruise phase of flight. The current phase and next phase (descent) are shown, along with any operational limitations that are tied to all phases of flight. The array of flight phases at the bottom of the display shows all phases of flight and indicates:

- which phases have occurred already (grayed out)
- which phases have not occurred but are not affected by changes to operational limitations (black with white letters)
- which phases have not occurred but are affected by changes to operational limitations (amber with black letters)

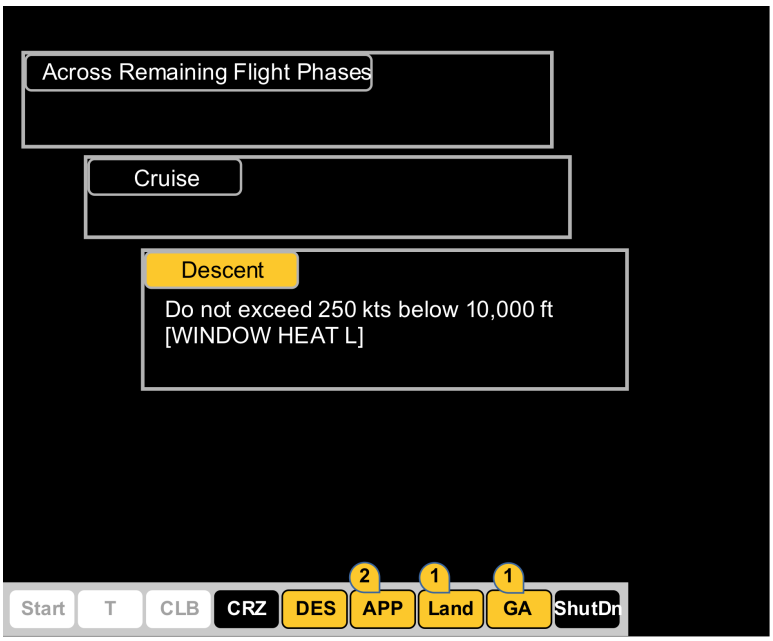


Figure 10. Operational limitations by phase of flight (example 1).

Figure 11 shows that the pilot can select a later phase of flight to also show the operational limitations in that phase. Generally, the limitation information can be located and accessed quickly because of the organization and phase of flight tabs.

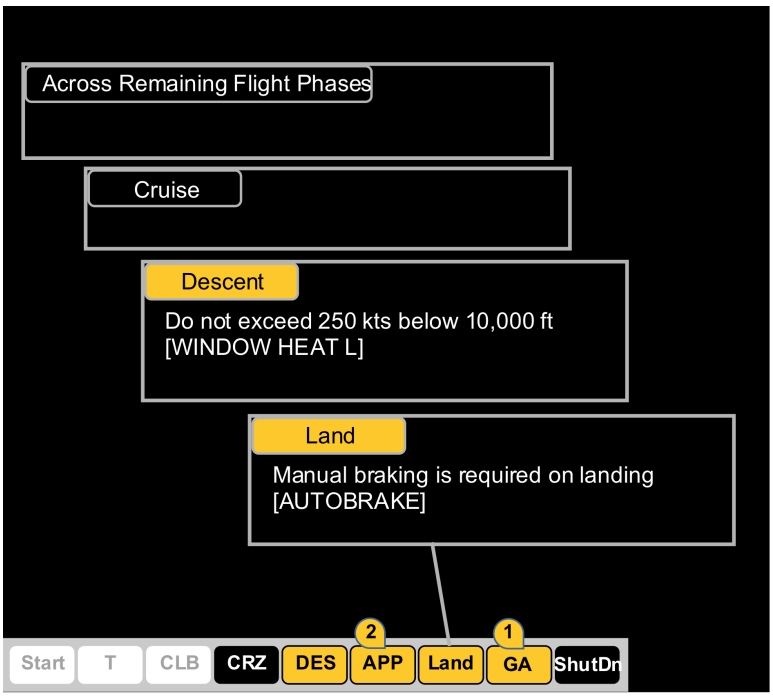


Figure 11. Operational limitations by phase of flight (example 2).

6.5 Mission Risks

Each flight (mission) has a set of risks associated with it, some anticipated and some that emerge during the course of the flight. Indeed, the shift in pilot training to a Threat and Error Management framework (Helmreich et al., 1999) highlights the fact that there is a range of risks tied to each mission. Examples include:

- Flight crew-related risks, such as:
  - fatigue tied to duty time
  - fatigue tied to operating through circadian lows
  - fatigue tied to crossing multiple time zones
  - no previous experience with a route or destination
  - low time in type
  - illness or incapacitation
  - personal stress related to a family (or other) situation
- Environment or weather-related risks, such as:
  - reduced visibility
  - icing conditions
  - nearby thunderstorms
  - moonless night
  - birds near a large airport
- Infrastructure-related risks, such as:
  - a recent change to an approach procedure
  - a change to taxiway markings
  - a change to a special use airspace near the destination airport

- Airplane-related risks, such as:
  - a high number of MELs

As part of the effort to pull together mission-related information to support operational decision making, we have developed a display space to keep track of these mission risks.

6.6 Support for Diversion Decisions

In addition to supporting operational decisions about the planned destination, this capabilities orientation can also aid flight crews in making decisions about diversions, when a diversion is needed. We discussed the Mission Compatibility (section 6.1) element that aids the flight crew in determining whether they can land at their planned destination. That same approach can be used to identify alternate airports that are compatible with the airplane's capabilities; i.e., within range, sufficient runway length, compatible approaches, etc.

Indeed, other efforts have shown that much of this selection process can be automated (e.g., Meuleau et al., 2009). The flight crew will need to make the decision to initiate a search for a diversion airport, and that decision could also specify the urgency of the need, including:

- land immediately/as soon as possible
- land at nearest suitable airport
- identify the best airport within the airplane's range (when the planned destination has been removed as an option)

To further guide the selection process, there may also be value in having the flight crew indicate if there are any specific needs to be met on the ground, such as medical or maintenance facilities. Previous efforts to automate elements of this process have pulled together information, such as weather and terrain, along with databases on relevant support services. The airplane capabilities analysis described here can supplement that effort to further optimize the identification of an appropriate diversion airport.

While the current effort has not developed and evaluated prototype displays to support diversion decisions, we believe that the capabilities-oriented assessment of the airplane can fit into a scheme for diversion selection. Further, we believe that a design for that type of DST should provide the following features:

- Present a single diversion recommendation, which benefits pilots when little time is available and they do not have time to sort through options.
- Provide a set of options to choose from when there is more time available, and provide a method for comparing that small set of "best" options.
- Present a description of the selected diversion airport so that the flight crew can quickly determine that the DST's information is correct (data transparency), or correct the information if it is not correct.
- Provide a "rationale" for both the airport that was selected and the airports that were not selected. This rationale should be presented in a short-hand to indicate the basis for selection or rejection (e.g., runway length), but there should also be more information available that can be accessed when time permits. When the flight crew believes they know which airport is best and the DST did not select that airport, there needs to be some transparency regarding the DST's rejection.

- Provide transparency regarding which airports were considered and allow the flight crew to add other airports that may not have been included in the initial set.
- Make it possible to see the options on a map that also shows the airplane's current location. Also, allow the flight crew to filter the full set of potential diversion airports for important features, such as maintenance facilities.
- Provide "negotiation" tools for the flight crew so that they can explore (when time permits) what is needed to change the selection of a diversion airport. For example, perhaps they can reduce (for just this flight) the amount of fuel reserves they are required to carry to increase their range enough to get to an airport that has important services. Other factors that might benefit from flight crew input are anticipated changes to weather, runway conditions, or use of thrust reversers on landing to decrease landing distance.
- Identify any operational risks tied to the diversion airport, such as weather, visibility, or terrain, and move those operational risks to the larger sets of risks already in play.

6.7 Display Integration

The displays, and underlying software, described here are intended to support the management of airplane system failures. Recall that the primary elements of managing non-normals (Figure 1) were:

- manage the immediate threats to the flight
- contain system failures and restore system functions
- revise mission, as needed

The displays described here support some elements of these activities but not the full set (e.g., there is no support for managing immediate threats). Specifically, our emphasis has been on integrating and presenting information to provide better support for operational decisions. A primary focus of these display prototypes is presenting a clear picture of the operational effects of airplane system failures (integrated with existing conditions in the world). Initial outputs are mission compatibility, maneuver envelope, airplane capabilities, and operational limitations.

The mission compatibility display is intended to translate the airplane system failures directly into an assessment of whether the airplane can still make the planned destination, or if there are any incompatibilities between the airplane's capabilities and the requirements of the mission.

The maneuver envelope display is intended to pull together all relevant information on changes to the airplane's maneuver envelope.

The airplane capabilities display identifies any degraded or lost airplane capability to convey succinctly the ways in which the airplane is limited in performing missions. Ideally, the language used in these displays has more meaning to pilots than the listing of failed airplane system components.

Finally, changes to operational limitations are presented in a format that is more mission-oriented (using a phase of flight organization), more accessible, and better integrated. The software should resolve conflicts between limitations coming from the different NNCs.

Again, these displays reveal the ways in which operating the airplane needs to be modified to complete the mission. In the case where a diversion is needed, the products of these displays can be passed to a DST to generate a recommendation.

6.8 Remaining Design Decisions

These prototype displays were developed to better understand how relevant operational information could be pulled together and integrated in a way that aids pilots. The following design issues remain until relevant user data can be gathered in an evaluation.

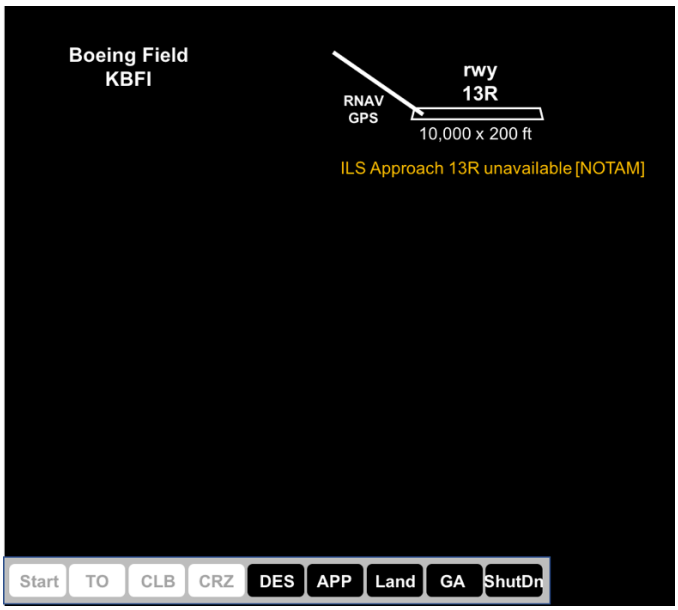
- *What is lost vs what remains*. The prototype displays described here generally show "losses." The alternative is to show what capabilities remain. Early versions of the prototype designs showed the full set of capabilities, and highlighted the ones that had been affected; an approach that also shows what you have remaining. However, there is a long tradition ("quiet, dark," described above) in aviation displays that advocates showing losses only. Largely driven by a desire to minimize the information presented to emphasize the ability to see "change," showing overall system status is discouraged. We eventually shifted to a loss-only display. At this time, we believe that the critical time for considering what remains is when selecting a diversion airport, and that approach described above, is driven by what remains (i.e., what is working). Pilot input is needed to further inform this decision.
- *Awareness vs just-in-time advising*. Somewhat related is the issue described above regarding whether all changes to airplane capabilities are presented on the display, or only those related to the current mission. At this time, we are showing all changes in the belief that we are supporting pilot awareness of the degraded airplane state, and that that awareness has the potential to support later decision making. Part of the justification for this approach is that we believe the set of changes to airplane capabilities will be relatively small in the vast majority of cases, and pilots will be able to manage the overall picture. Again, the intent is to shift away from a longer list of airplane component failures to a small set of changes in capabilities.
- *Some information is already available*. In a number of cases, the information described here is already available in many airplanes; e.g., operational limitations can be found in the NNCs; the FMC can indicate when you may not be able to get to the planned destination, etc. The focus for these prototypes is to not only identify information that could be useful for operational decision making, but to also think about better ways to present it to pilots (e.g., easier to access, faster to identify and process, organized around operational decisions).

7. Case Studies and Initial Prototype Interface

The following provides a set of case studies to illustrate how these display concepts might support decision making for specific airplane system failures:

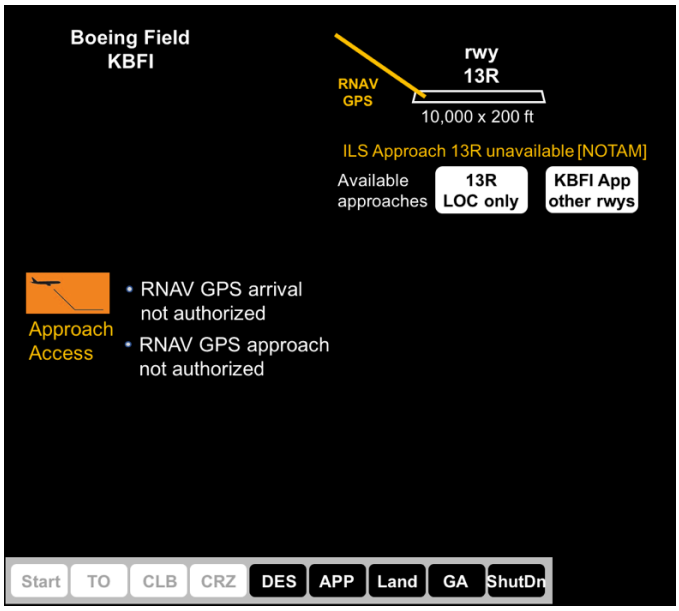
7.1 Case 1: A Single, Simple Failure that has Implications for Approach and Landing

A commercial jet transport is flying to Boeing Field (KBFI) in Seattle, which only has a single runway (for this airplane), 13/31. A NOTAM informs the flight crew that the ILS for runway 13R is inop. The flight crew, now on descent, is planning to fly the RNAV GPS approach to 13R. The mission overview display would look like this:



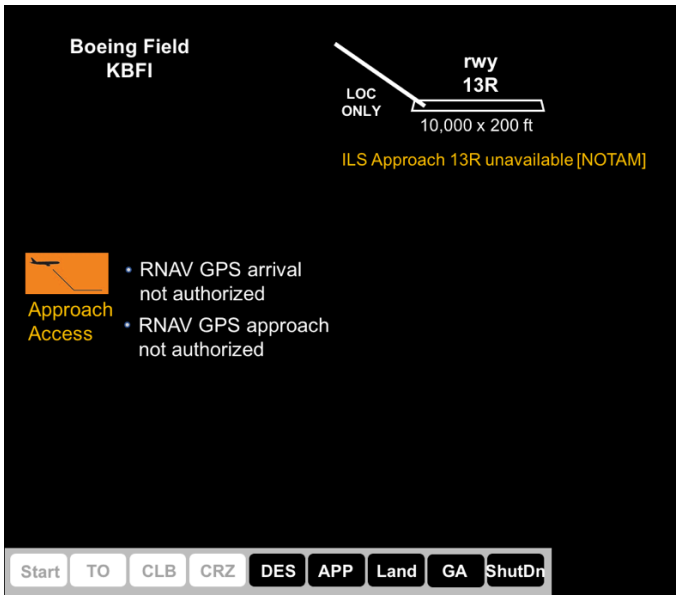
The loss of the ILS approach is indicated (with its source) and the color white shows that this plan is compatible with the airplane's capabilities. Note that the bottom of the display shows that there are no operational limitations in any of the remaining phases of flight.

Later in descent, there is a Radio Altimeter failure, which means that the airplane is no longer "legal" to fly the RNAV GPS approach. The mission overview display changes to this:

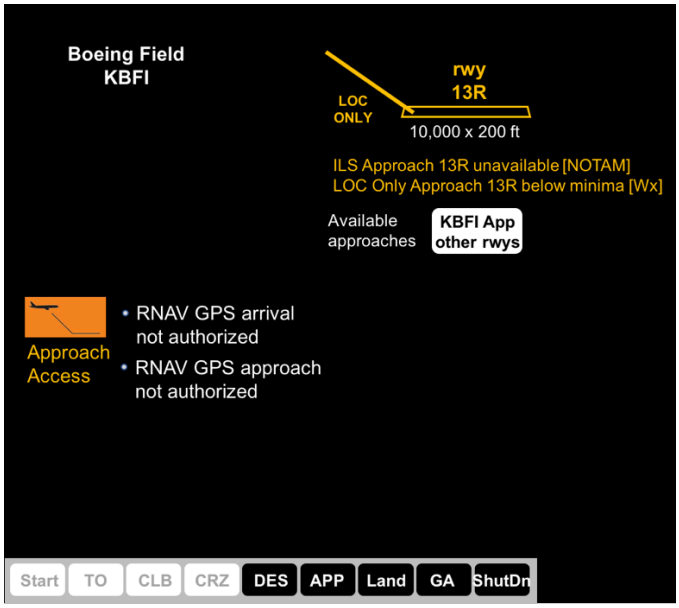


Note that the RNAV GPS approach has become amber to show an incompatibility (although not an actual loss of the approach). The display also shows the approaches that are currently available for this runway (in addition to a link to non-13R approaches). The change to airplane capabilities is indicated in the middle of the display with the Approach Access icon and messages to indicate that

RNAV GPS arrivals and approaches are not authorized. In this case, the flight crew should choose the LOC only approach, which leads to the next figure:



Compatibility has been restored (white). The changes to airplane capabilities remain for pilot awareness. The next event is that the weather at KBFI degrades to low instrument flight rules (IFR): overcast, 200 ft with ¾ mile visibility, which is below the minimums for the LOC approach (Category C aircraft require 1.5 miles visibility to perform LOC approach). The mission overview, with access to weather information, now changes to this:



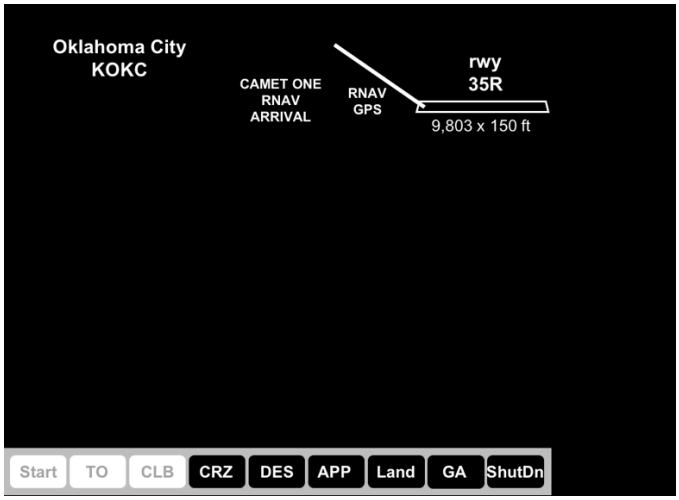
Again, amber is used for the approach to indicate that it is not totally compatible. The label for the runway is also now amber, given that there is no approach to 13R that is completely compatible. At this point, the flight crew will need to determine if they should approach from the other end, divert

somewhere, or fly one of the approaches to 13R with an understanding that they are not fully compatible with any of the approaches.

7.2 Case 2: An AC Bus Failure that Affects a Number of Airplane Systems

Electrical system failures can have far-flung effects. In this case, an Alternating Current (AC) bus failure leads to downstream failures to a number of components.

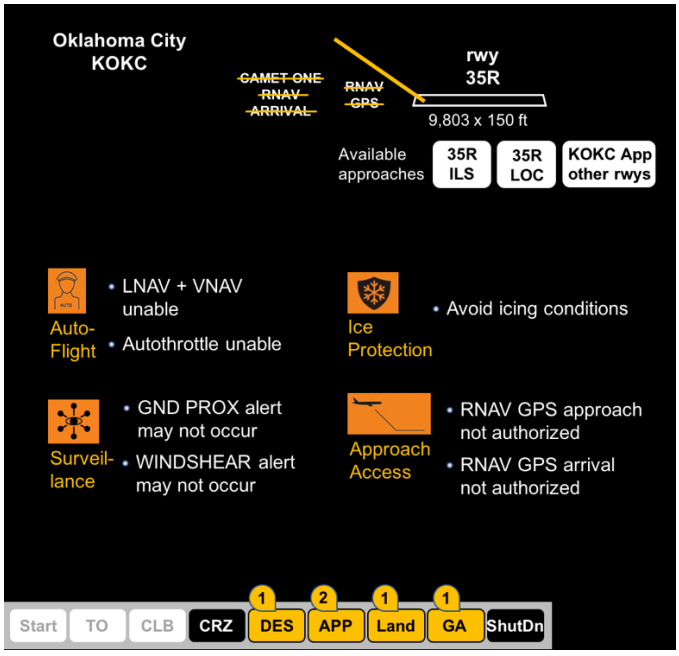
For this scenario, the commercial jet transport is flying to Oklahoma City (KOKC); in cruise and cleared to fly the RNAV arrival and approach to runway 35R. The initial mission overview display, which indicates compatibility with the mission looks like this:



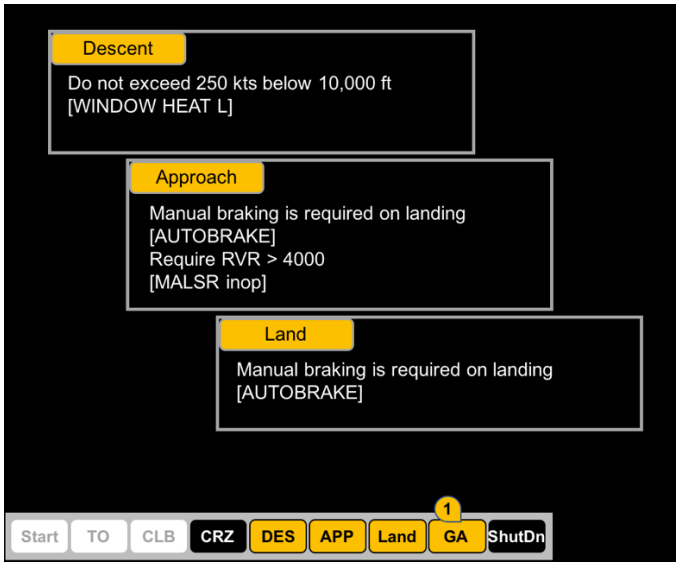
The AC bus failure occurs. In EICAS, it would generate the following diverse set of failure messages. (Note that these EICAS messages present a realistic example of what would be shown for a Boeing airplane.)

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

The effects are on the autothrottle, fuel pumps, alerting systems, probe heaters, environmental control, and the autobrake. Also, LNAV and VNAV are lost. This list gets translated to the mission overview in the following way:

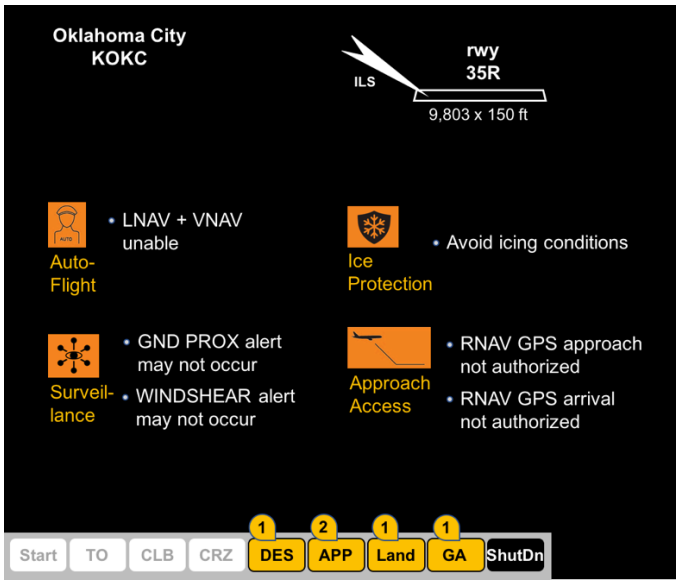


Because LNAV and VNAV are lost, the airplane is not able to fly the RNAV arrival and approach. As before, the other approaches to this runway are shown. The airplane capabilities section of the display shows the four functional areas that have been affected: autoflight, surveillance, ice protection, and approach access. This is a subset of the larger set of functional areas, and, ideally, aids the flight crew in making sense of what has been affected. Next, note that there have been changes to the operational limitations for four phases of flight. The display also indicates how many limitation items there are in each phase of flight. By clicking on that area of the display, you can navigate to another display that provides the detail on these limitations:



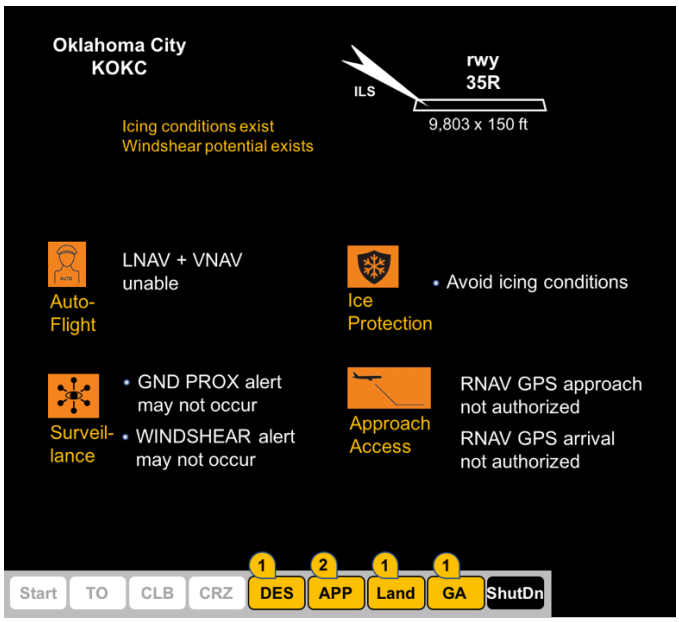
The display, in this iteration, does not expand every phase of flight. In this case, it details three of them. Note that the Medium intensity approach light system plus runway alignment indicator lights (MALSR) inop issue is from a NOTAM.

Flight crew application of NNCs can restore the autothrottle but all the other losses remain after NNCs have been performed. After the flight crew switches to the ILS approach, the mission overview display looks like this:



The flight plan for the ILS approach is now compatible with the airplane's capabilities. The operational limitations remain to be managed.

The last event we created for this scenario was for the weather at KOKC to change—specifically, thunderstorm activity nearby the airport. This weather information is picked up and used to generate a message because of the airplane's particular vulnerabilities (icing and windshear alerting):



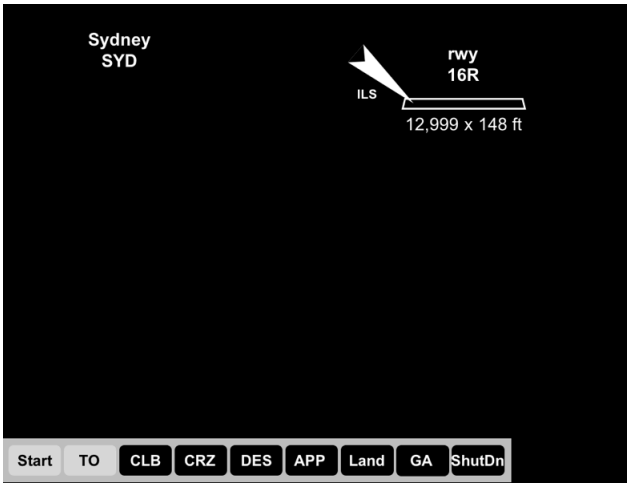
A remaining design issue is the combination of:

- vulnerability to a hazard/threat (due to degradation or loss of a capability)
- the presence of the hazard/threat

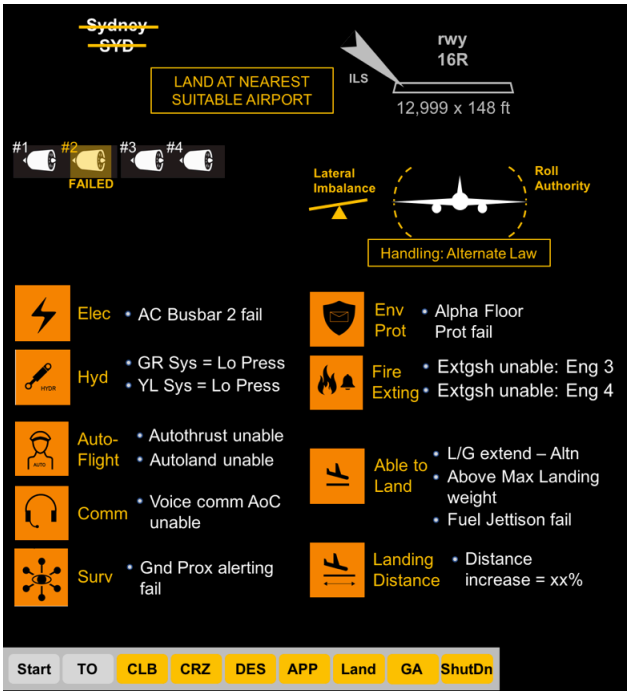
The primary question is: “Is there value in explicitly indicating the combination of the two?”. That is, is it enough to identify a lost capability (icing protection) and separately the presence of icing conditions? Or, should the mission compatibility display also point to the combination?

7.3 Case 3: The Qantas 32 (A380) Uncontained Engine Failure

As described above, this serious event generated more than 80 ECAM (alert) messages, which sometimes referred to components at a very low level (e.g., HYD Y ENG PMP A PRESS LO) and could therefore not be integrated in a manner that gave a complete picture of the situation. The highly experienced flight crew struggled to sort out the state of their airplane from the information they had. Based on the accident report (ATSB, 2013) and Captain DeCrespigny's personal account (DeCrespigny, 2012), we attempted to have the event play out using our prototype display. The initial mission overview display would look like this:



The crew were on their way to Sydney; they were in climb phase and everything was normal. After the uncontained engine failure occurred, the picture changed dramatically. The following captures many of the operational effects although we do not have enough detail to identify the specific changes to operational limitations:



First, significant damage to two hydraulic systems probably created the need to land at the nearest suitable airport. This airplane is not compatible with continuing on to Sydney. Therefore, we show that Sydney is eliminated as a destination, and the Sydney runway is grayed out. When a new destination and runway are selected, they will replace what is there now. Also, when there is a need to land prior to the planned destination, that is communicated clearly (i.e., Land at nearest suitable airport).

In this situation, the flight crew would, at some point, transition to the decision support tool (not prototyped here) to select a diversion airport. That DST would use what it knew about remaining airplane capabilities to make a recommendation about where to go (see the discussion in Section 6.6).

Next, we show an option for revealing engine state. This illustration is simpler than the actual QF32 situation, in which some of the other engines had degraded performance. However, the point here is to illustrate the idea of presenting engine state more simply and clearly than it is presented on current engine indication displays (e.g., see Sikora & Mumaw, 2004).

Also, new to this case study is inclusion of the maneuver envelope information. Recall that this information is not included unless there are changes. In this case, there were some significant changes to airplane performance and handling. It is difficult to capture them all from the reports, but there was a lateral imbalance caused by an inability to move fuel, a degradation in roll authority, and a transition into Alternate Law. The goal here is to use a combination of text and graphical elements to simply convey those degradations or losses.

The busiest part of the display is where the changes to airplane capabilities are listed. These almost fill the available space. Note that probably not all of these items were true immediately; some of them, such as the fuel imbalance, developed over time. While there are a large number of functional areas and messages listed, the hope is that this display is much more efficient and effective than the list of more than 80 ECAM messages (which required more than an hour to sort through). Note that the electrical and hydraulic functions are presented and are listed first; recall that the role of these icons is to tell a more complete story about the operational consequences.

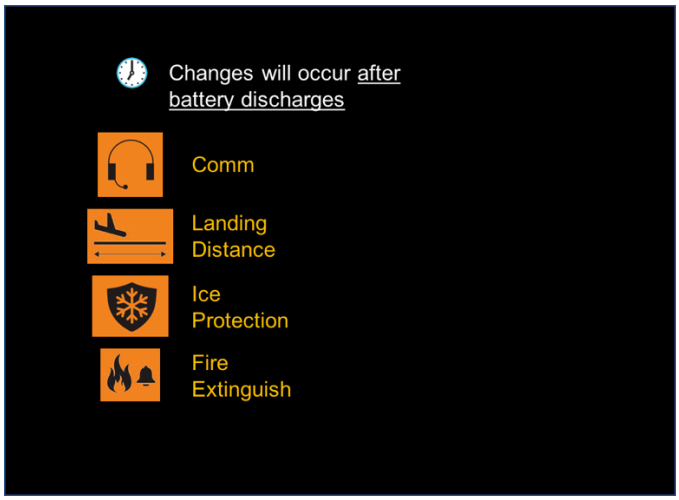
Missing from this display is the fuel leak that occurred after flying engine parts punctured the fuel tanks in several places. Currently, the display scheme would tie fuel loss into range (as do other airplanes) but since the display is not expecting Sydney as a destination and range is a mission-specific issue, range is not captured at this point in time. It would factor later, during selection of a diversion airport.

Finally, at the bottom of the display are the indicators that show which phases of flight have changes to operational limitations. While we do not have specifics here, there are enough changes to maneuverability that it is likely that most, if not all, phases of flight would have relevant items.

7.4 Case 4: The American Airlines Standby Bus Failure and Delayed Consequences

One interesting aspect of the AAL 268 incident (described in Section 4) was that a number of items were relying on a battery that was being depleted over time. So, the failure and transition to battery did not lead immediately to airplane capability losses. However, the capability losses were going to

happen if enough time passed. The airplane capabilities display could reveal this through something like the following:



A clock icon makes clear that after some time these functions will be affected. In the actual event, the flight crew was quite surprised about the capability loss, which occurred after quite a bit of time. When there are airplane resources that will be depleted over time, such as power or fuel, it may be useful to show specifically which functions will be affected.

8. Next Steps

As described above, this effort is in an early stage of development. The creation of prototype displays allows us to start articulating important questions and then seek input from airline pilots regarding the potential benefits (or liabilities) tied to these display concepts. We have identified certain types of information that we believe could be beneficial for managing non-normals but only pilots, working in a realistic scenario, can determine the true benefits.

The next stage of work is to get pilot feedback on the display prototypes to aid us in answering our design questions and refining these prototypes. After that refinement, we need to develop displays for specific cases or scenarios and then observe how pilots use those displays to manage a non-normal situation. Later studies will need to compare performance with displays developed out of this "capabilities" approach to the more traditional "airplane component" approach.

Another element of this work, mentioned briefly in the report, is the automated integration of other operational factors, such as weather or infrastructure, that also affect operational decisions. We are identifying ways to integrate airplane state information with weather data and changes to the larger airspace to support decision making. For example, in Case 1 above, we tied in information from a NOTAM regarding the loss of an ILS. Developing a system that can effectively support decisions about the mission and alternate destinations really requires having access to a wide array of data on the airspace system.

9. Summary and Conclusions

The work described in this report describes the need for a shift in the way airplane system information is conveyed to jet transport pilots and the development of a set of display concepts to support that shift. The prototype displays developed here move away from descriptions of physical airplane system components in favor of a more function-oriented characterization. Specifically, the goal is to aid the flight crew in understanding how system failures affect their ability to complete their current mission, or to divert, if needed. Second, the displays identify ways to further integrate information from outside the airplane to better support operational decisions. These displays were developed for a small set of failure cases.

A belief driving this effort is that airplane systems are becoming much more complex and that pilot training on airplane systems is (or will be) inadequate to support a pilot's ability to reason about the operational consequences of system failures. Further, pilots may not arrive to training with a good understanding of systems. Our intent is to remove some of the burden placed on the flight crew when trying to understand the systems during non-normal, sometimes even time-critical conditions.

A second driver of this work is a move toward more automated support of operational decisions. In the current design phase, we are trying to identify and integrate the information that supports operational decisions by the flight crew. In future phases of research, the work of supporting operational decision making may help to support the development of autonomous functions to aid the flight crew.

The primary results of this initial effort are:

- a set of display prototypes that illustrate how operational information can be better represented and integrated
- a set of design questions that will inform continued refinement of these display concepts

References

ATSB (2013). In-flight uncontained engine failure Airbus A380-842, VH-OQA. Aviation Occurrence Investigation report–Final (AO-2010-089). Canberra, Australia: ATSB.

DeCrespigny, R. (2012). QF32. Sydney, Australia: Macmillan.

Dinadis, N. & Vicente, K.J. (1999). Designing functional visualizations for aircraft systems status displays. The International Journal of Aviation Psychology , 9(3):241–269.

Helmreich, R. L., Klinect, J. R., & Wilhelm, J. A. (1999). Models of threat, error, and CRM in flight operations. In Proceedings of the tenth international symposium on aviation psychology (pp. 67–682).

Meuleau, N., Plaunt, C., Smith, D., & Smith, T. (2009). An emergency landing planner for damaged aircraft. 21st Conference on Innovative Applications of Artificial Intelligence.

Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols and other distinctions in human performance models. IEEE Transactions in Systems, Man, and Cybernetics, 13 (3), 257–266.

Reitsma, J. (2016). Decision-making support for non-normal events on highly integrated airplane systems. Unpublished Master's thesis, Technical University –Delft.

Roth, E.M., Mumaw, R.J., & Lewis, P.M. (1994). An empirical investigation of operator performance in cognitively demanding simulated emergencies. (NUREG/CR-6208). Washington, DC: Nuclear Regulatory Commission.

Sexton G.A. (1988). Cockpit-crew systems design and integration. In Human Factors in Aviation. (E.L. Wiener & D.C. Nagel, eds.). New York: Academic Press.

Sikora, J. & Mumaw, R. (2004). Making engine displays more meaningful to flight crews. Proceedings of the International Conference on Human-Computer Interaction in Aeronautics, Toulouse, France.

Vicente, K. (1996). Improving dynamic decision making in complex systems through ecological interface design: A research overview. System Dynamics Review, 12, 251–279.

Vicente, K. (1999). Cognitive work analysis: Toward safe, productive, and healthy computer-based work. Lawrence Erlbaum: Mahwah, NJ.

Wiener E.L. (1988). Cockpit automation. In Human Factors in Aviation. (E.L. Wiener & D.C. Nagel, eds.). New York: Academic Press.

Wiener E.L. (1989). Human factors of advanced technology ("Glass Cockpit") Transport aircraft. NASA Technical Contractor Report 177528. NASA Ames Research Center, Moffett Field, CA.

Woods, D.D., Wise, J.A., & Hanes, L.F. (1982). Evaluation of safety parameter display concepts. EPRI NP-2239. Palo Alto: EPRI.