

Operator Performance Evaluation of Fault Management Interfaces for Next-Generation Spacecraft

Miwa Hayashi and Ujwala Ravinder

San Jose State University & NASA Ames Research Center

Brent Beutter, Robert S. McCann and Lilly Spirkovska

NASA Ames Research Center

Fritz Renema

Perot Systems Government Services & NASA Ames Research Center

Copyright © 2008 SAE International

ABSTRACT

In the cockpit of NASA's next generation spacecraft, most vehicle command will be performed via electronic interfaces instead of hard cockpit switches. Checklists will be also displayed and completed on electronic procedure viewers rather than on paper. Transitioning to electronic cockpit interfaces opens up opportunities for more automated assistance, including automated root-cause diagnosis capability. The paper reports an empirical study evaluating two potential concepts for fault management interfaces incorporating two different levels of automation. The operator performance benefits produced by automation were assessed. Also, some design recommendations for spacecraft fault management interfaces are discussed.

INTRODUCTION

During the time-critical, dynamic flight phases of launch, ascent, and entry, the spacecraft crew must monitor the systems' parameters on the cockpit interfaces carefully, so that they can react quickly when any problem occurs. Numerous sensors are installed throughout the spacecraft, and their readings are presented to the crew through the cockpit displays. This huge amount of information is difficult for any single human operator to thoroughly monitor without automated assistance.

In the Space Shuttle cockpit, a relatively simple Caution & Warning (C&W) system assists the crew in detecting system anomalies by issuing audio and visual alarms whenever a sensor reading exceeds its predefined limits. At the same time, a brief fault message is displayed for each out-of-limit sensor reading and associated parameters on the status displays turn to yellow (if caution) or red (if warning). These events will be collectively called *C&W events* in this paper. A major problem in such a C&W system is that the failure of one

critical item often causes many additional downstream components dependent on it to also cease functioning properly. This produces C&W events not only for the root cause, but also for the failures of each of the downstream components and connected systems dependent upon it, often resulting in a flood of C&W events [1]. It is then up to the crew to interpret the multitude of C&W events, figure out which one is the root cause, and work on mitigating the root-cause failure. Furthermore, after identifying the potential root cause, the crew must manually 1) locate the appropriate section of the paper checklist, 2) search for and find the appropriate checklist, and 3) execute the relevant checklist steps to perform the necessary system reconfiguration. These operations can be slow, inefficient, attention demanding, and error prone.

Transitioning from the Shuttle to the next-generation spacecraft, the Crew Exploration Vehicle (CEV) Orion, provides a great opportunity to introduce more automation technologies to the crew's fault management processes. The CEV will have much less interior volume than the Shuttle, and with little interior room for physical switch panels, virtually all vehicle commanding will take place through soft (electronic) switches provided on the displays. Also, paper checklists will be eliminated and replaced with an electronic version. The electronic checklists potentially offer opportunities for simple automation assistance not available on paper checklists, such as automatically highlighting the currently active line, checking off completed lines, skipping lines that belong to inapplicable branches of conditionals, and so forth. Furthermore, the electronic checklists can be integrated with the status displays and the electronic switch panels. For instance, the electronic checklists can automatically highlight the parameter or the switch associated with the current checklist line, thus quickly drawing the crew's attention to the right place.



Documents

Document Sharing Hub

This study examined some of the potential design options of advanced fault management interfaces, namely the Advanced Caution and Warning System (ACAWS) displays, which utilize an integrated electronic checklist. One of the major design options of interest was whether or not to include the automated root-cause diagnosis capability. It was reported that commercial airline pilots have been expressing the desire for real-time, onboard automated root-cause diagnosis capability to help save precious cognitive resources and time under high-workload, potentially life-threatening situations [2]. The same reasoning applies to spacecraft operations. The root cause information also can be utilized in the electronic checklists to automatically call up the proper checklist, saving the crew's time and effort to do so manually and reducing the probability of the crew selecting a wrong checklist. The downside of including such capability is the additional vehicle hardware and weight required to provide the increased computational resources. The development and maintenance of complex root-cause diagnosis algorithms also will be costly and time-consuming. In addition, there are some human factors concerns. For instance, what if the computer chooses an incorrect root-cause diagnosis? Will the crew be able to correctly identify the root cause, manually override the computer's recommendation, and call up the correct checklist?

Another major design option considered in this study was whether the interface should present all the detailed system information or just a summary of it suppressing the details that the computer thinks less important to the crew (the suppressed details are always available when the crew takes an action to call them up). Another design option examined was whether the switches should be accessed via a virtual switch panel with switch icons resembling hardware switches, or the switches should be integrated with the system line-diagram and directly accessible via the switch symbols within the diagram. In the former option, the virtual switch panel is presented over the line diagram due to the limited display space, while in the latter option, the switch symbols are in the line diagram, and thus, the line diagram is always visible, enabling the crew to immediately observe the effects of a switch throw on the system.

This paper reports the results of a simulator study examining the impacts of several ACAWS display design options on operator performance. Two prototype ACAWS displays, called Elsie and Besi (not acronyms), were designed for fault management of the Electrical Power System (EPS) and Environmental Control and Life Support System (ECLSS). The EPS and ECLSS used in the study were simplified versions of those of the Shuttle. The two systems are tightly interconnected because EPS supplies electrical power to the ECLSS loads (e.g., fans, pumps). Therefore, when an ECLSS component indicated an out-of-limit sensor reading and generated C&W events, the root-cause could lay in either the ECLSS itself or in the EPS. The participants' task was to identify the root cause and perform the

proper procedure using the ACAWS displays. Elsie displayed detailed EPS/ECLSS information, had virtual switch panels separate from the system line-diagram, and did not provide automated root-cause diagnosis. Besi summarized EPS/ECLSS information, had switch symbols integrated in the system line-diagram, and provided automated root-cause diagnosis. In short, Elsie was somewhat similar to current Shuttle displays with the exception of electronic switches and checklists, while Besi had more automation assistance. The EPS-related displays and ECLSS display for Elsie and Besi were developed for this study, and the other displays were similar to those of the Space Shuttle Cockpit Avionics Upgrade (CAU) display suite [3]. (CAU is sometimes pronounced as "cow;" thus, the ACAWS displays used in this study were named after cow names.)

In addition to the EPS/ECLSS fault management tasks, the participants were asked to concurrently monitor the flight variables on the Primary Flight Display (PFD) to measure their ability to divide their attention between the fault-management and flight-monitoring tasks. At different times, one of the five major flight variables of the CEV changed its color from white to yellow, and then to red. The participants were asked to respond to the color change by touching the flight variable that had the color change. If the participant missed a color change, that indicated that the EPS/ECLSS task had caused attention tunneling (i.e., a tendency to focus very hard on only one thing, ignoring surrounding information, often observed under high-stress situations [4]).

This study analyzed and compared the participants' EPS/ECLSS fault-management performance accuracy, fault resolution times, PFD task misses, eye movements, subjective workload scores, and subjective preference ratings between Elsie and Besi. The primary goals of this study were to provide empirical data of the performance benefits provided by Besi's automation, as well as to provide generic design recommendations for the ACAWS displays.

METHODS

SIMULATOR - The CEV cockpit simulator consisted of an HP XW9300 workstation with two dual-core 2.4GHz AMD Opteron processors, 2GB of system memory, and an NVIDIA Quadro FX3450 video card with 256MB of memory running Windows XP Professional. The workstation was used for PFD and ACAWS display graphics generation, data collection, and sound control. The video card drove two 20-inch touch-sensitive Apple Cinema displays, one of which was used by the experimenter and the other by the participant. Figure 1 shows the display used by the participants (the display unit on the right was not used). The top half showed the PFD and the bottom half showed the ACAWS display. The experimenter's terminal was located outside the simulator room. The simulator included a speaker system to generate background engine noise and issue auditory alarms.



Figure 1: CEV Simulator

Another HP XW9300 with a similar configuration was dedicated to real-time computation of the EPS and ECLSS parameters with Matlab (version 7.4.0) and Simulink (version 6.6.1). In Besi trials, this workstation also ran automated model-based root-cause diagnosis software, Hybrid Diagnostic Engine ("HyDE") [5]. Simulated CEV flight parameters were computed real-time on the third workstation, a Sun Fire V40z Server, with two dual-core 2.4Ghz AMD Opteron processors and 16GB of system memory. The flight dynamics were based on a CEV flight model developed at NASA Johnson Space Center.

The simulator was also equipped with a head-mounted eye tracker (ISCAN ETL-500, ISCAN, Inc., Burlington, MA) integrated with a head tracker (FasTRAK, Polhemus, Colchester, VT) to measure the participants'

gaze locations. The eye-tracking system was mounted on a baseball cap as shown in Figure 1. The display area subtended a visual angle of 30.2° horizontally and 47.2° vertically at a viewing distance of 20 inches. The sampling rate of the eye-movement data was approximately 60 Hz, and the spatial resolution was approximately 0.5 inches.

EPS/ECLSS MODEL - Figure 2 shows our EPS model. It contained three batteries (A, B, and C) capable of supplying power to the ECLSS loads connected to the two load banks (L1-L7 on Load Bank A, and L1-L8 on Load Bank B). Switches are shown as pairs of two circles with a short line in between (their names are also underlined), and circuit breakers as coaxial double circles. Figure 2 illustrates the initial configuration of the EPS at the beginning of each trial, where Battery A powered Load Bank A, and Battery B powered Load Bank B. Battery C was a backup battery. For each load bank, L1 through L6 were AC Loads, and L7 and L8 were DC Loads. Loads L1 and L2 on each load bank were the primary critical loads necessary for crew survival, loads L3 and L4 were non-critical loads, and loads L5 and L6 were backup critical loads for the other load bank's critical loads. Load L7 on Load Bank A was a primary critical DC load, and load L8 on Load Bank B was the backup for Load Bank A's L7. In the initial configuration, the load switches for the backup loads were off (open).

The participants were instructed to resolve any malfunctions by calling up the appropriate checklist (i.e.,

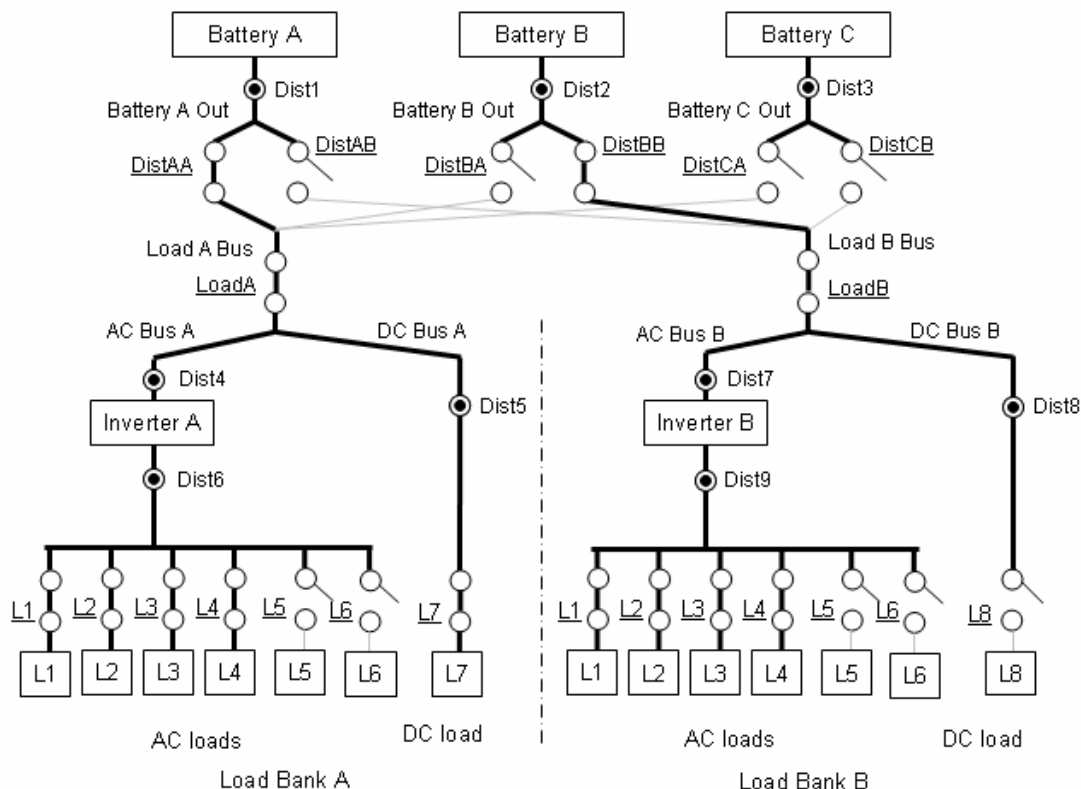


Figure 2: Electrical Power System (EPS) in initial configuration



performing from memory was not allowed). The process to select the appropriate checklist was different between Elsie and Besi, and described in the ACAWS Displays section. Once the checklist was opened, the procedure usually started with diagnosing the problem by troubleshooting and/or cross-checking related system parameters. After the diagnosis steps were completed and the problem was verified, the checklist instructed recovery steps to reconfigure the system (e.g., activate proper backups). For instance, for a failed-open switch (i.e., stuck at an open position), the first steps in the checklist consist of a diagnosis of the problem by cycling the switch. If cycling restores the switch, the problem is resolved. If not and the switch is verified to be un-restorable, the checklist instructs additional switch throws to activate the appropriate backup components.

Participants were instructed to follow these rules for switches:

- Before cycling a switch, all the ECLSS loads connected to the switch must be turned off. This prevents damage to the loads by a high inrush current later.
- One load bank should not be powered by more than one battery at any moment.
- *The load-shedding rules:* To avoid exceeding the maximum power capacity limit of a single battery, one or two non-critical loads (L3 or L4) must be turned off before turning on a backup critical load (L5 or L6).

These rules are complex, but strictly following the checklist procedures insures that these rules are satisfied, except for the load-shedding rules. Because the number of the primary critical loads lost may be different in each case (especially when there was a previous malfunction that disabled some of the primary critical loads), the checklist did not specify how many non-critical loads had to be shed. Thus, the participants needed to determine which non-critical loads had to be shed each time.

ACAWS DISPLAYS - The bottom half of the Apple Cinema display presented the ACAWS display (Figure 1). The participants interacted with the ACAWS display through a commercial hand controller manufactured by Nostromo (Figure 3). The rationale of using this type of hand controller was to simulate a dynamic flight phase situation (e.g., ascent), where large G-forces and vibration require the crews' arm to be restrained. This

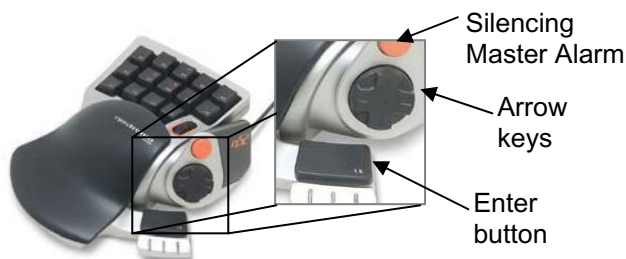


Figure 3: Nostromo hand controller

requires the use of a hand controller installed near the arm rest to interact with the display. The arrow keys were used to move the cursor among edge keys and other selectable items in the display, and the Enter button was used to select the item. Pressing the orange round button silenced the Master Alarm sound.

Elsie – Figure 4 shows Elsie. In this figure, the main area (the large square area) shows the EPS Summary (EPS Sum) display. The checklist area is on the right side, and the fault message area is below the main area. The red edge key at the lower left corner is the Master Alarm. As mentioned earlier, Elsie presented detailed system information to the crew. The information was organized by several displays within Elsie: the EPS Sum showed the EPS diagram (Figure 4), EPS Main showed all the EPS parameters in a table format (Figure 5), and EPS Loads showed the status of the load switches in a table format (not shown). The ECLSS parameters were presented on the ECLSS display (not shown). All of these displays, as well as the EPS switch panels (Figure 6 shows an example), were accessible via the edge keys. All of these displays appeared in the main area.

When there was no system malfunction to work on, such as during the beginning of the trial, the participants were instructed to bring up the Fault Summary (Fault Sum) display (Figure 7) in the main area to monitor the overall health of the EPS and ECLSS. Once any out-of-limit sensor values were detected, the C&W system issued the C&W events, including a visual alarm (red Master Alarm), auditory alarms, color changes of the affected parameters on the Fault Sum display (yellow for caution, red for warning), and fault messages. The participants used the Fault Sum display information to judge which system, EPS or ECLSS, was likely to contain the root cause. It was also recommended for the participants to go check the EPS Sum display (if the suspected component was in EPS) or the ECLSS display (if it was in ECLSS) to quickly assess which specific component likely had the root-cause failure.

Then, the participant checked the fault messages displayed in the fault message area (lower part of Elsie). This area displayed only the first five messages. If there were more, the participant needed to go to the Fault Log display to view the entire list (Figure 8). The Fault Log had three pages, each of which could list up to eighteen messages, or 54 in total, in chronological order. To determine which message was associated with the root cause, the participants were instructed to look for, first, any “switch mismatch” fault message (i.e., the commanded position and sensed position of the switch did not match). If there was no such message, then, second, they looked for the volts-related message coming from the most upstream part of the system (for example, the “Load A volts low” message is upstream of the “DC Bus A volts low”; see Figure 2). In Elsie, the participant must go through the fault messages and find the one that was associated with the potential root cause, because that fault message was also the item on the checklist to be selected.

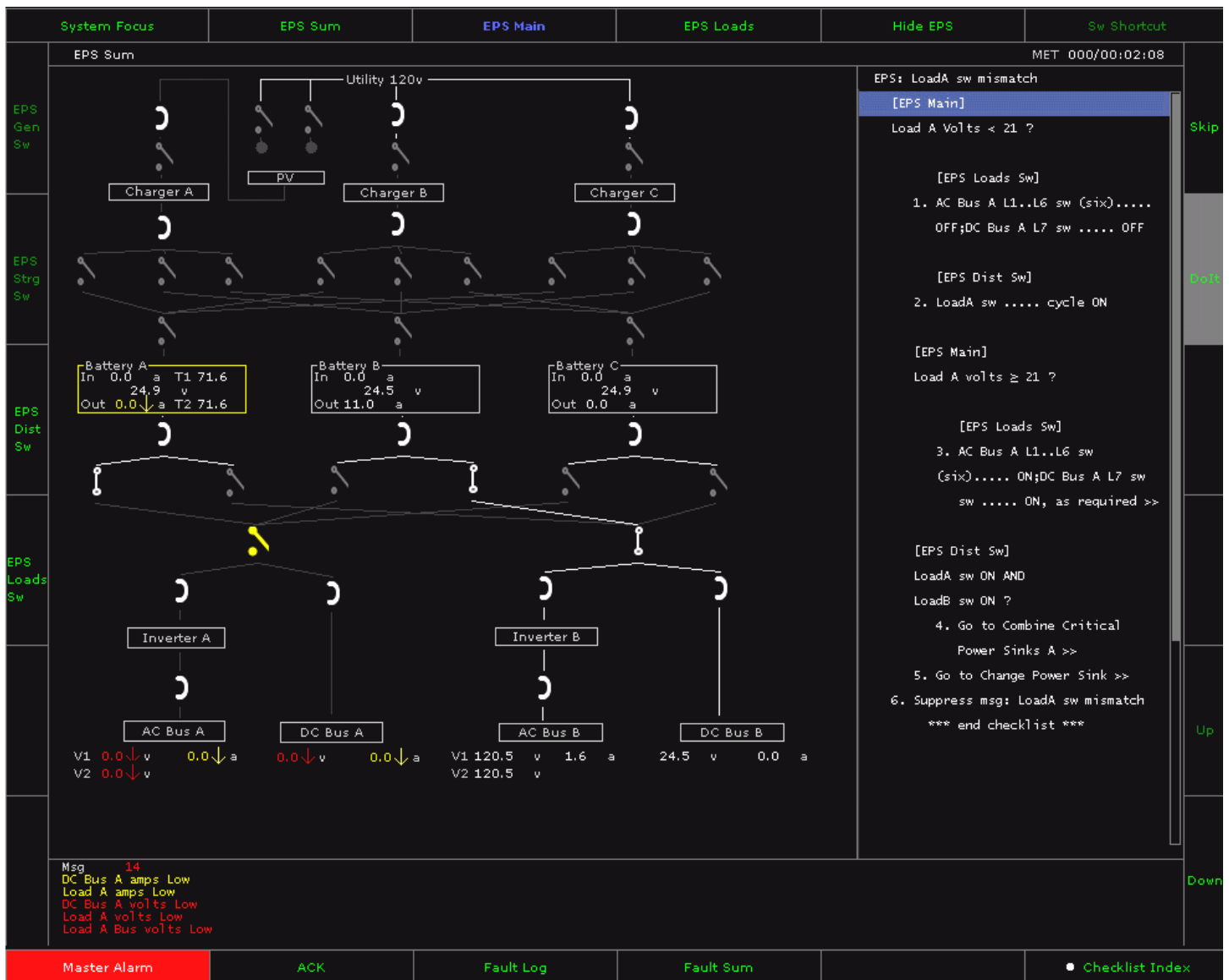


Figure 4: Elsie. The main area is showing the EPS Sum display.

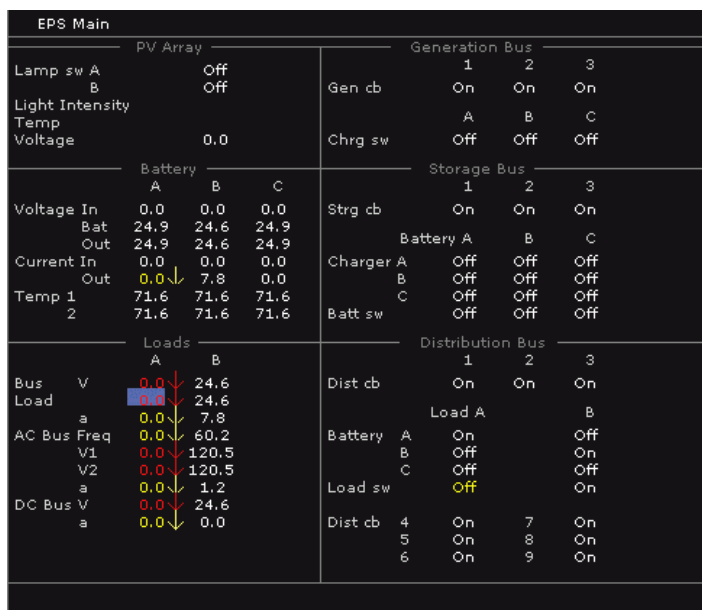


Figure 5: Elsie - EPS Main

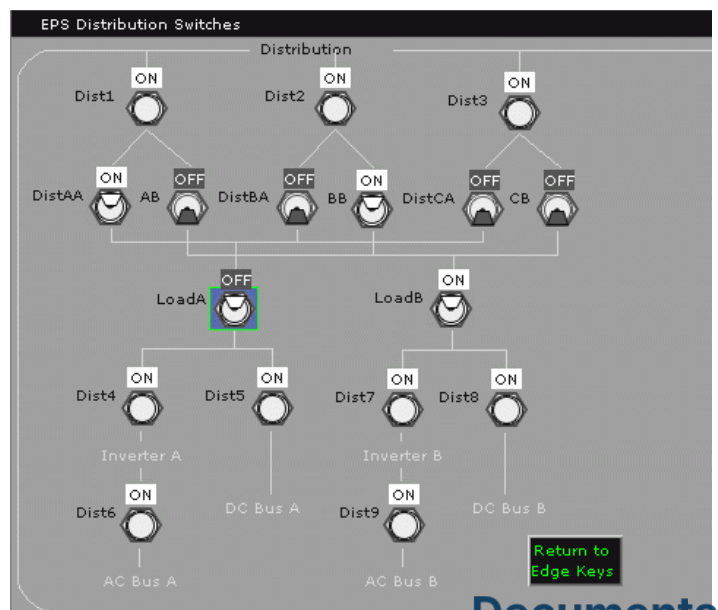


Figure 6: Elsie - One of EPS switch panels