

The Human Element in a DRE System

Robert Hanmer
Lucent Technologies
2701 Lucent Lane
Lisle, IL 60532 USA
+1 630 979 4786
hanmer@lucent.com

A Distributed Real-Time Embedded system is typically one that will be acting on its own for some portion of its operation. During this time period it is expected to handle faults and other unexpected events on its own, without the involvement of its user. Systems that fit this description range from aerospace or space vehicles to telecommunications systems to embedded systems found throughout the home. In order to support extended independent operation, the system must *Minimize Human Intervention*.

Many new system designers fail to recognize that this is an important constraint on the design of their system. In order for the system to achieve the goal of independent operation, it cannot ask for help at every opportunity.

The following pattern, *Minimize Human Intervention*, addresses this issue. This version was mined and thus expressed in terms applicable to several telecommunications switching systems designed and built by Lucent Technologies.

This pattern is tightly entwined with a number of other strategies and mechanisms that have been documented in pattern form. For example, In order to help *minimize human intervention*, the system should be able to *Ride Over Transients* as this eliminates false alarms and conditions that could not be isolated. It is also entwined with general patterns for input and output that in some way restrict output or direct its propagation, see "An Input and Output Pattern Language: Lessons from Telecommunications" in PLOPD-4.

1. PATTERN: MINIMIZE HUMAN INTERVENTION

Problem

History has shown that people cause the majority of problems in continuously running systems (wrong actions, wrong systems, wrong button).

Context

High-reliability continuous-running digital systems, where downtime, human-induced or otherwise, must be minimized.

Forces

Humans are truly intelligent; machines aren't. Humans are better at detecting patterns of system behavior, especially among seemingly random occurrences separated by time. (PEOPLE KNOW BEST)

Machines are good at orchestrating a well thought-out, global strategy, and humans aren't.

Humans are fallible; computers are often less fallible.

Humans feel a need to intervene if they can't see that the system is making serious attempts at restoration. Human reaction and decision times are very slow (by orders of magnitude) compared to computer processors.

A quiet system is a dead system.

Human operators get bored with ongoing surveillance and may ignore or miss critical events.

Events, normal processing or failures, are happening so quickly that inclusion of the human operator is infeasible.

Solution

Let the machine try to do everything itself, deferring to the human only as an act of desperation and last resort.

Resulting Context

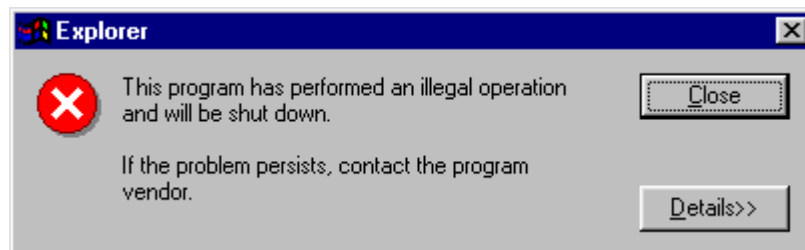
A system less susceptible to human error. This will make the systems customers happier. In many administrations, the system operator's compensation is based on system availability, so this strategy actually improves the lot of the operator.

Application of this pattern leads to a system where patterns such as RIDING OVER TRANSIENTS, SICO FIRST AND ALWAYS and TRY ALL HARDWARE COMBOS apply to provide the system with the ability to proceed automatically.

Rationale

Empirically, a disproportionate fraction of high-availability system failures are operator errors, not primary system errors. By minimizing human intervention, the overall system availability can be improved. Human intervention can be reduced by building in strategies that counter human tendencies to act rashly; see patterns like FOOL ME ONCE, LEAKY BUCKET COUNTERS and FIVE MINUTES OF NO ESCALATION MESSAGES.

Avoid asking the user to get involved if there is any chance that the system can resolve the problem itself. This reduces a human's impact on the system reliability equation. Another detrimental aspect of asking the user to get involved is the slow response time of users-- they might not be looking to the system to notice that they should do something. (See also ALARM GRID).



Avoid This:

Notice the tension between this pattern and PEOPLE KNOW BEST.

Author

Robert Hanmer, Mike Adams, 1995/03/23

Workshopped at PLoP/95

Referenced Patterns:

<u>Pattern</u>	<u>Source</u>	<u>Intent</u>
PEOPLE KNOW BEST	PLOPD 2 Chapter 33	Assume humans know more than the machine.
FOOL ME ONCE	PLOPD 2 Chapter 33	Keep watch on the requests to clear history information.
LEAKY BUCKET COUNTERS	PLOPD 2 Chapter 33	Decrement error counts periodically, if they aren't increasing.
FIVE MINUTES OF NO ESCALATION MESSAGES	PLOPD 4 Chapter 23	Don't confuse craft with too frequent messages.
RIDING OVER TRANSIENTS	PLOPD 2 Chapter 33	Give transients time to clear up on their own.
SICO FIRST AND ALWAYS	PLOPD 2 Chapter 33	Integrity considered first and always vigilant.
TRY ALL HARDWARE COMBOS	PLOPD 2 Chapter 33	Explicitly enumerate and try all configurations.

