Design of fail-operate computer systems

CORBIN JACKSON

ELECTRICAL AND COMPUTER ENG
HOWARD UNIVERSITY

Introduction

- Fail Operate Computer Systems are hardware and software that prevent harm or damages done by a system if it were to malfunction. Terminating the process the system is going through until fixed.

Two Systems

Computer Control System

- Operator, computer , sensor and effector components of the computer.
- They control the safety critical application by continuously monitoring the system and issuing controls.

Computer Safety System

- Passively monitors a safety critical application. Issues controls when it senses the application has entered a hazardous condition.

Mishap and Mishap Risk

- In a ***Computer Control System*** a mishap can occur when the system is in a hazardous operating system and fails to operate.
- The mishap risk in a computer control system is a combination of the probability that the system is operating in that region and that it has failed to operate.

- In a ***Computer Safety System*** both event must happen. A hazardous event followed by a failure of a safety system controlling the event.
- Mishap risk is the combined probability that there has been a hazardous event and the safety system failed to control it

Requirements

- Reliability
- Availability
- Repairability
- Total component failure rate

Reliability

- The probability that an item will operate correctly for a continuous period of time.

- The unreliability is the exact opposite. Providing a percentage or amount of times that an item can or will fail.

Availability

- The probability that an item will operate correctly at a given time and under specific conditions.
- The probability that a computer safety rate would fail to operate and as a result not available to preform its safety function.

Repairability

- The ease and speed of which a failed system can be restored back to its original operating condition.
- When an error occurs the system can repair itself back to its original unfailed condition.
- The unreliability and unavailability can all be reduced with proper repairability. The system can repair components immediately after they fail.

Total Component Failure Rate

- The higher the component failure rate is the lower the unreliability and unavailability.

- The more components in a system gives it a higher chance of those components failing, but by having more components there are more to rely on and also more available for the system.

Additional Requirements and Constraints

- Redundancy management method
- Application Constraints
- Exposure Time
- Failure Responses

Redundancy Management Method

- Process of identifying failures, isolating them and reconfiguring the system to a fail-operate state.
- There's three ways:
  1. Automatically by resident hardware and software
     - When the mishap is too short for human intervention
  2. Manually by operator action
     - Human operator identifies and isolates failures then fixes the system
  3. Semi-automatic through a combination of both

Application Constraints

- Limiting the uses and functions of a system.
- With fail-operate computer systems there needs to be back ups for when something goes wrong in the system and is used to improve performance.
- Many times there will be back up power to compensate for electrical failure (ex: generator)

Exposure Time

- The longer a system has failed the more unreliable it becomes.
- Its "Exposure Time" determines how safe it will be and how the system can be repaired.
- Different systems have different levels of exposure time but once the time has been exceeded the system cannot be repaired immediately.

Failure Responses

- Two types of responses:
  - Transparent
  - Transient
- In a transparent response the failure is located and fixed with no outwardly observed behavior.
- In a transient response it is almost the opposite. There is a obvious disturbance in the system.

Example

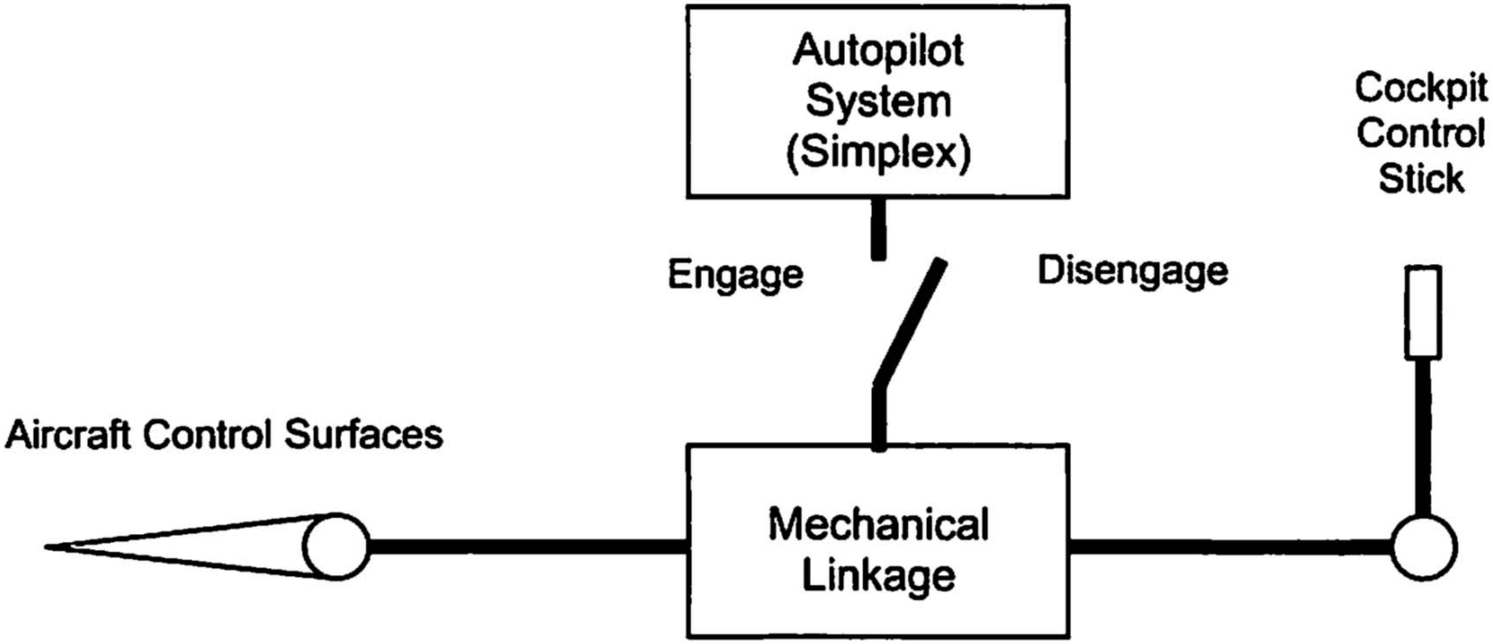

Figure 6.5 Aircraft Autopilot Example

Conclusion

- Fail-operate computer systems have many parts and many usages. They are complex in some ways but also very basic in other ways, but always necessary. A simple fail-safe can save many lives like the Therac-25 machine I mentioned in my last presentation. Even the airplane example I just gave. So fail-operate computer systems are just as important maybe even more important than the systems themselves.