Graduate Student Research Day 2012
Florida Atlantic University

COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Failure Patterns: A New Way to Analyze Failures

Ingrid Buckley

Department of Computer & Electrical Engineering and Computer Science, College of Engineering and Computer Science, Florida Atlantic University, Boca Raton, FL

Purpose: We propose the concept of failure patterns as a way to describe how faults lead to system failures. A failure pattern describes how a fault becomes a failure indicating how the fault propagates through the system units until it produces a system failure. The pattern explicitly shows how flaws in the system allow the propagation of faults. The information in these patterns is useful to evaluate and design reliable systems. The pattern also shows how to stop the failure or mitigate its effects. Background/Significance: Notable incidents have occurred due to failure in critical systems that fueled research efforts on reliability. A pattern is an encapsulated solution to a recurrent problem in a given context. Failure patterns embody the experience and knowledge of many designers, and when properly catalogued, they provide a repository of solutions for useful problems. Method(s): A failure pattern describes how a failure is propagated from a fault, identifies the components which are involved in the failure, the specific errors which allowed the failure to occur, and the effect of the failure on the system. If the failure was intentional (instead of produced by a fault), its propagation can also be described. It also provides a solution to stop this propagation in the form of reliability and security patterns, as well as a way to store and analyze the information collected at each stage of the failure. Due to their dynamic descriptions, failure patterns allow countermeasures to be included to mitigate the identified failures.

FLORIDA ATLANTIC UNIVERSITY
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Secure Systems Research Group

Failure Patterns: A New Way to Analyze Failures

Ingrid Buckley and Eduardo B. Fernandez

Department of Computer & Electrical Engineering and Computer Science, Florida Atlantic University, Boca Raton, FL – USA, 33431

Motivation

- Reliability is a key system characteristic that is an increasing concern
- Greater reliability is necessary due to the new ways in which services are delivered to the public Health care, government, telecommunications, tools, and products require greater reliability.
- Reliability is a property which allows some function/task/service to behave as intended when required.
- A pattern is an encapsulated solution to a recurrent problem in a given context. Reliability patterns provide solutions for reliability problems.
- Our objective is to increase the application of reliability in critical systems using reliability patterns.
- We have defined a series of basic successive steps to incorporate reliability in the development life cycle.

Failure Patterns

- Failure patterns are useful to understand how failures can manifest and propagate in the system
- Faults are manifested as errors, which in turn are manifested as failures
- The primary characteristics of a failure pattern can be summarized as:
  - It shows how a fault is manifested in a given system until it produces a failure
  - It helps to identify countermeasures to a avoid or mitigate failure
  - It allows for the reconstruction of a failure scenario by observing its effect in specific units
  - It provides a guide of application for software development to follow that helps to reduce failures.

- Benefits:
  - Shows direct relationship between the system structure, components and the failure
  - Can be used to understand and analyze different problems

- Challenges:
  - Software developers are not accustomed to designing reliability features during software development.

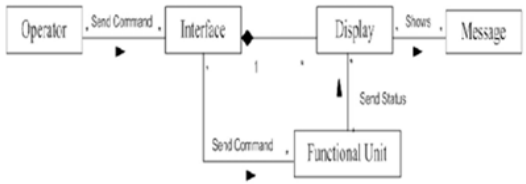
Failure Pattern: Incorrect Status Message in Safety-critical Systems

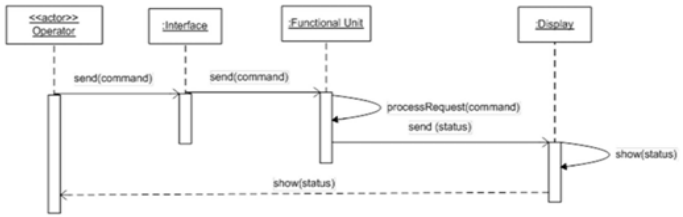
Intent – Many systems can endanger humans if their indicators fail, e.g., a radiation treatment machine or an airplane inflight. The operator may not realize that some operation occurred or not and can act on a given indication thus provoking a failure.

Context - Health care facilities that use systems to perform critical procedures on patients. These systems have status indicators that show if a operation has been applied. An example was described above. Aircrafts that display indications to operators to make critical decisions in flight.

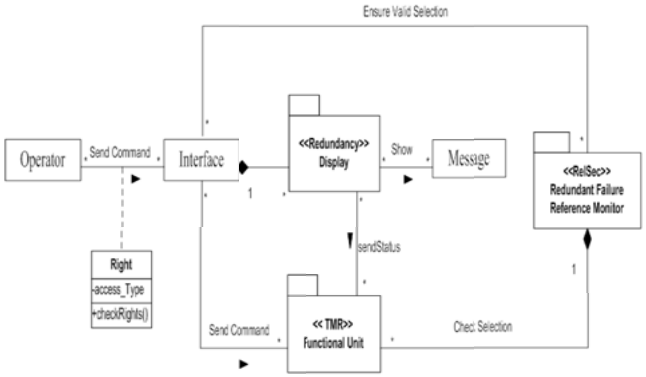
Problem - How erroneous operator message failures originate and propagate?

Solution - A hardware or software fault in the functional or control unit may send erroneous status indications to the display. A fault in the display, in the interface, or in the functional unit, may produce a similar effect.





Countermeasures and Forensics



Where to look for Evidence

- The classes which are most susceptible to failures:
  - The interface, functional unit, and display classes.
  - We can check what information was sent to the interface and functional units if these classes keep a record of their message history.

Conclusions

- We introduced the concept of failure patterns as a systematic description of the steps which lead to a failure as well as an indication of the countermeasures needed to avoid or mitigate those failures.
- Failure patterns are complementary to dependability patterns which prevent failures.
- They are effective when used for building machines that carry out crucial functions.
- Aids developers is identifying, tracing and handling failures in the system.