Fault-tolerant design

Design

Fault tolerance the property that enables a system to continue error free operation in the event of unexpected failure of some of its components. If it's operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naively designed system In which even a small failure can cause total breakdown. Fault tolerance Is particularly sought after In high-availability or life-critical systems. Fault tolerance Is achieved by Incorporating It In a system at he design stage of development. . A fault-tolerant design enables a system to continue its intended operation, possibly at a reduced level, rather than failing completely, when some part of the system fails. The fault tolerant system design enables a system to be operational with a reduction In throughput or an Increase In response time In the event of some partial failure. That Is, the system as a whole Is not stopped due to problems either In the hardware or the software. Fault tolerance design leads to system redundancy I. E it makes a system redundant. 3.

Fault tolerance in system design enables a system to anticipate exceptional conditions and cope with them aiming for self-stabilization, so that the system converges towards an error-free state. However, if the consequences of a system failure are catastrophic, or the cost of making it sufficiently reliable Is very high, a better solution may be to use some form of duplication. 4. Recovery from errors In fault-tolerant systems can be characterized as either roll-forward or roll- back. When the system detects that it has made an error, roll-forward recovery takes he system state at that time and corrects it, to be able to move forward.

Roll-back recovery reverts the system state back to some earlier correct version / checkpoint and moves forward from there. Roll-back recovery requires that the operations between the checkpoint and the detected erroneous state can be made Idempotent. Some fault tolerant systems make use of both roll-forward and roll-back recovery for different errors or different parts of one error. 5. The internet is a good example of fault tolerant design where there is reliable two-way communication between the endpoints of the communication nodes inspire of data packet loss, duplication, re- ordering and corruption.

These conditions do not damage data integrity but only reduce throughput by a proportional amount. Fault-tolerant system design ultimately alms to achieve redundancy of system operation. AIM 6. The alma of this service paper Is to discuss fault tolerant design concept and Its incorporation in indigenously developed avionic systems. REDUNDANCY 7. The goal of fault tolerant system design is redundancy. Redundancy is the provision of functional capabilities that would be unnecessary in a fault-free environment. Redundancy allows either to detect or to mask a fault.

This can consist of backup components / systems which automatically come online should one and time redundancy. Space redundancy provides additional components, functions, or data items that are unnecessary for fault-free operation. Space redundancy is further classified into hardware, software and information redundancy, depending on the type of redundant resources added to the system. In time redundancy the computation or data transmission is repeated and the result is compared to a stored pop of the previous result. DEPENDABILITY 8.

The ultimate goal of fault tolerance in design is to enhance dependability of system. Dependability is the ability of a system to deliver its intended level of service to its users. It depends on the following:- (a) Attributes: The properties which are mandatory required in a system. These are reliability, availability and safety. (I) Reliability R(t) is the probability that a system operates without failure in the interval [O, t], given that it worked at time O. It is a measure of continuous delivery of erect service. Fault tolerance design improves the reliability of a system. It) Availability A(t) is the probability that a system is functioning correctly at the instant of time t. The reliability depends on an interval of time but availability is taken at an instant of time. A system can be highly available yet experience frequent periods of being nonproliferation as long as the length of each period is extremely short. (ill) Safety is the probability that a system will either perform its function correctly or will discontinue its operation in a safe way. B) Impairments: The reasons for a system to cease performing its intended function due to fault, errors and failures.

Fault is a physical defect, imperfection or flaw that occurs in hardware or software of a system / sub-system. Error is a deviation from correctness or accuracy in system / sub-system performance. Failure is a non-performance of some action by a system / sub-system that is due or expected I. E deviation from compliance specifications. Faults can result in errors and errors can lead to system failures. (c) Means: The methods and techniques to develop a fault tolerant system for:- I) Fault avoidance. (it) Fault tolerance. (iii) Fault masking. (iv) Fault forecasting.

Fault tolerant design of a system / sub-system should ensure:- (a) No single 9. Point of failure. If a system / sub-system experience a failure, it must continue to failing component. When a failure occurs, the system must be able to isolate the failure to the offending component. This requires the addition of dedicated failure detection mechanisms that exist only for the purpose of fault isolation. (c)Fault containment to prevent propagation of the failure. Some failure mechanisms can cause a system to fail by propagating the failure to the rest of the system.

Fault tolerant design prevents failure propagation. (d) Availability of reversion modes. In a fault tolerant system providing spare components addresses fault 10. Tolerance in three ways:- (a) Replication. Providing multiple identical instances of the same system or sub-system, directing tasks or requests to all of them in parallel, and choosing the correct result on the basis of a quorum. (b) Redundancy. Providing multiple identical instances of the same system and switching to one of the engaging instances in case of a failure. C) Diversity. Providing multiple different implementations of the same specification and using them like replicated systems to cope with errors in a specific implementation. The flight data recorder must survive highly destructive forces over a broad 11. Range of aircraft accident scenarios. The conventional crash hardened design concept is for a container to withstand the severest crash scenarios while installed inside an airframe where it endures severe impact, fire and other forces in a crash.

In pursuance of fault tolerant design for SUFFERS a deployable recorder unit / data acquisition unit deploys and falls away from the aircraft thus avoiding the crash environment. This can be achieved by placing the

recordable units in an aerodynamic lifting body or aerofoil which is affixed to the exterior of the airframe. Crash sensors activate a release mechanism which automatically releases the airfoil during accident, delivering it safely away from the aircraft impact site. The objective of such a design is to achieve maximum survivability of the recorded information.

Survivability of the memory storage media ensures that the information is retained and the consequent analysis of this data allows corrective action to be taken to prevent accidents recurring and improve the safety of future aircraft operations. 12. Fault-tolerant design's advantages are obvious, while many of its disadvantages are not:- (a) Interference with fault detection in the same component. (b) Interference with fault detection in another component. When fault tolerance in one component prevents fault detection in a different component.

For example, if component B reforms some operation based on the output from component A, then fault tolerance in B can hide a problem with A. If component B is later changed (Tao less fault-tolerant design) the system may fail suddenly, making it appear that the new component B is the problem. Only after the system has been carefully scrutinized will it become clear that the root problem is actually with component A. (c) Reduction of priority of fault correction. Even if the operator is aware of the fault, having a fault- tolerant system is likely to reduce the importance of repairing the fault.

If the faults re not corrected, this will eventually lead to system failure, when the fault-tolerant component fails completely or when all redundant components have also failed. (d) that the backup components are functional.

The only way to verify this is through bringing backup system online and which can be disastrous if the backup system is UN-serviceable. (e) Cost. Both fault-tolerant components and redundant components tend to increase cost. This can be a purely economic cost or can include other measures such as weight, size, power consumption and time to design. (f) Inferior components.

A fault-tolerant design may allow for the use of inferior components, which would have otherwise made the system inoperable. While this practice has the potential to mitigate the cost increase, use of multiple inferior components may lower the reliability of the system to a level equal to, or even worse than, a comparable non- fault-tolerant system CONCLUSION 13. A fault-tolerant design enables a system to continue its intended operation, system fails. Fault-tolerant design enhances the dependability of a system / sub- system due to increased availability. Thus improving the system / sub-system liability.

It also ensures safety by ensuring that in the event of total failure system will discontinue its operation safely. Providing fault-tolerant design for every system / sub-system is normally not an option. Associated redundancy brings a number of penalties such as increase in weight, size, power consumption, cost, time to design, verify and test. A number of options have to be examined to determine which components / system / sub-systems should be fault tolerant based on criticality, susceptibility to fault and cost involved in making component / system / sub-system alt tolerant.