4.3.2.3 Fault Tolerance

Return to Reliability

About

Return to the Top

Fault Tolerance is the ability of a system (computer, network, cloud cluster, component, etc.) to continue functioning correctly without interruption during failures. Fault Tolerant systems (or components) prevent disruptions to a system that is considered Safety-Critical System (SCS), Life-Critical System or Mission Critical System. Usually, this requires an understanding of the single points of failure through the multiple critical execution paths in a running system.

The system characteristics of Fault Tolerance High Availability are related in that to achieve high availability, a system must address Fault Tolerance of components on the systems critical paths.

Fault Tolerant systems use redundant (i.e;, spare, backup) components to automatically become available in the event of a component failure to ensure there is no loss of service or data. The ability to use Failover mechanisms to quickly, smoothly and transparently transition to the redundant or backup systems requires a well designed system, with contingency plans and special management processes, hardware or software to ensure the transition. There are some Failover components which are acquired. For example:

- **Power sources** are ruggedized as fault tolerant by incorporating alternative sources and backups like Uninterruptible Power Supply (UPS) and backup generators. A good description of this is provided in the Tactical Microgrid Standard (TMS) use case,
- **Hardware systems** are made Fault Tolerant by deploying identical or equivalent systems that can either be used instead of the original system or use in conjunctions with the original system used as an alternative. For example, a server can be made fault tolerant by using an identical server running in parallel, with all operations mirrored to the backup server.
- **Networks** designed as Fault Tolerant by supporting multiple networks paths between any two endpoints within the Local Area Network (LAN) or Wide Area Network (WAN) are possible but the actual endpoint also needs to be duplicated (i.e., two Network Interface Cards (NICs)). It is also possible to use two different networks such as a wired, Wireless Fidelity (Wi-Fi), Bluetooth, or ZigBee.
- **Software** systems or components become fault tolerant when multiple instances of the software are running in parallel using either operating system threads or even more modern containers such as Docker or orchestration software such as Kubernetes. For example, a database can be continuously replicated to other machines. If the primary database goes down, operations can be automatically redirected to the second database. Another example, would be use of orchestration software such as Kubernetes to automatically use an alternate application container on the same or different machine.

Fault Tolerance needs to be considered in all disaster recovery plans or strategies. For example, Fault

Tolerant systems can use the cloud for backups allowing critical systems to quickly be restored. Although these backups are not true immediate failovers, they can offer a longer timeline for fault tolerance recovery. **Note:** often these backup plans are not geographically local which is particularly important during natural or even human disasters. [1)]

DIDO Specifics

Return to the Top

1)

Mariah Timms, AT&T outage: Internet, 911 disrupted, planes grounded after Nashville explosion. Get the latest updates, Nashville Tennessean, 5 January 2012, Accessed: 8 January 2021, https://www.tennessean.com/story/news/local/2020/12/25/att-outage-internet-down-hours-after-nashville-explosion/4045278001/