Crossing the Digital Divide (v147)

Redundancy

by Joseph Feigon

for the Observer

In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe, or to improve actual system performance, such as in the case of GNSS receivers, or multi-threaded computer processing.

In many safety-critical systems, such as fly-by-wire and hydraulic systems in aircraft, some parts of the control system may be triplicated, which is formally termed triple modular redundancy (TMR). An error in one component may then be out-voted by the other two. In a triply redundant system, the system has three sub components, all three of which must fail before the system fails. Since each one rarely fails, and the sub components are expected to fail independently, the probability of all three failing is calculated to be extraordinarily small; often outweighed by other risk factors, such as human error. Redundancy may also be known by the terms "majority voting systems" or "voting logic".

A suspension bridge's numerous cables are a form of redundancy.

Redundancy sometimes produces less, instead of greater reliability – it creates a more complex system which is prone to various issues, it may lead to human neglect of duty, and may lead to higher production demands which by over stressing the system may make it less safe.

This week’s message is about the level of redundancy you can control, and what you “need” to keep safe.

For most of us, the need for hardware redundancy might be limited to charge controllers and solar batteries, or a small server for your business, with a battery backup. For the small business, having a “backup” PC is often more cost effective than enterprise, server class hardware is, provided of course, there’s a valid, current backup of whatever data you need.

For most of us, Information redundancy means replicating data. A backup to USB, backup to a network addressable storage system (NAS), or backup to the Cloud (Dropbox, Amazon, One Drive…), must be kept current. Anything you need that cannot be easily replaced should be backed up. There are many ways to make this simple, and if it’s simple enough, and repeated often enough, a hardware failure, power failure, or Internet access outage will not result in non-recoverable loss.

Whatever needs to be backed up, needs to be tested. Experience has proven, equipment will fail, networks will have outages, software bugs will surface.

Control those things you can, and keep the surprises to a minimum.