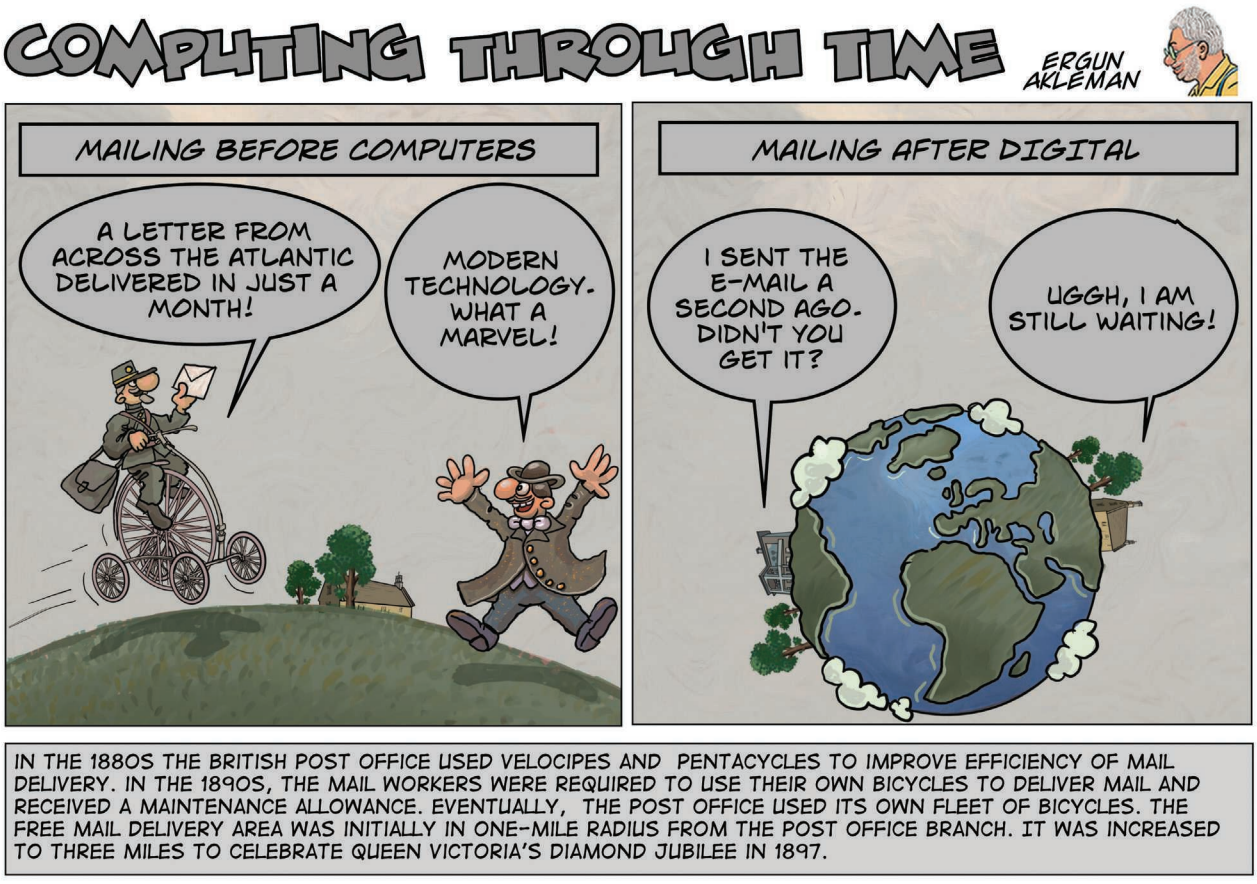

Digital Object Identifier 10.1109/MC.2022.3150933
Date of current version: 8 April 2022

Understanding Fault Tolerance and Reliability; Arun K. Somani et al. (p. 45) "Future systems will be more complex and so more susceptible to failure. Despite many proposals in the past three decades, fault tolerance remains out of the reach of the average computer user. The industry needs techniques that add reliability without adding significant cost. ... Systems fail for many reasons. The system might have been specified erroneously, leading to an incorrect design. Or the system might contain a fault that manifests only under certain conditions that weren't tested. The environment may cause a system to fail. Finally, aging components may cease to work properly. It's relatively easy to visualize and understand random failures caused by aging hardware. It's much more difficult to grasp how failures might be caused by incorrect specifications, design flaws, substandard implementation, poor testing, and operator errors." (p. 50) "Once a fault-tolerant system is designed, it must be evaluated to determine if its architecture meets reliability and dependability objectives. There are two ways to evaluate dependability: using an analytical model or injecting faults." *[Editor's note: The five articles that follow this analysis of fault tolerance and reliability describe different approaches to increase reliability and availability in systems of different mission critical requirements. I will only briefly describe each of them as much of what is said there is still needed and used today.]*

Toward Systematic Design of Fault-Tolerant Systems; Algirdas Avizienis (p. 51) "The greater the benefits these systems bring to our well-being and quality of life, the greater the potential for harm when they fail to perform their functions or perform them incorrectly. ... At the same time, threats to dependable operation are growing in scope and severity." (p. 52) "Here I summarize the most mature version of the guidelines for bottom-up fault tolerance. An abstraction of observed design processes in which steps often overlap, it is offered as a way to minimize the probability of oversights, mistakes, and inconsistencies that may occur during the implementation of fault tolerance. The first three steps—specification, implementation, and evaluation—deal with the building of a new system. Implementation and evaluation are concurrent. Step four—modification—addresses the repair or