SAFETY SYSTEM FOR CRITICAL SITUATIONS

Mrs. Madhu Malini Khanna, Dept. of English

Dr. C.V. Raman University, Bilaspur

Abstract

Safety-critical systems are systems whose failure could result in loss of life, substantial damage to property, or environmental harm. In applications fields such as medical devices, aircraft flight control, weapons, and nuclear systems, there are many well-known examples. In a particular sense, many modem information systems are becoming critical of security because their failure can result in economic loss and even loss of lives. More prevalent and more effective will be future safety-critical systems.

Key words: Safety critical system, information system.

Introduction

For their right operation, many modem systems rely on computers. Of course, safety-critical systems are of the biggest concern because their effects of failure can be significant. There are many applications that have traditionally been deemed critical of safety, but the definition's range needs to be extended as computer systems continue to be introduced in many fields that influence our life. The future is likely to dramatically boost the amount of computer systems that we regard as critical to safety. Dropping hardware costs, improving hardware quality, and other technological innovations guarantee that in many fields fresh apps are sought. There are plenty of security-critical[1], [2] system definitions, but the intuitive concept actually works quite well. Intuitively and formally, the concern is with the effects of failure. If a system's failure[3], [4] could lead to unacceptable effects, then the system is critical to safety. In principle, when we rely on it for our well-being, a system is critical to safety. The consequences of this concept are discussed in this chapter in terms of the classes of systems that should be regarded as critical to safety.

Methodology

Development of hardware remains at a stunning pace with an apparently endless sequence of changes in processor speed, memory size, disk capacity and bandwidth of communication, and the

introduction of comparatively fresh capacities such as wireless. Notwithstanding these improvements, several technology fields have not evolved as rapidly. Energy storage remains difficult and limits the use of computers in critical security apps. Consider what would happen if an AA battery's capacity increased at the same rate as the disk drive capacity. We have the technology to use well-understood fission procedures to extract at least some of the energy in the plutonium. Owning extensive and compact power sources would enable the development of many precious, currently impractical, safety-critical apps.

A 2nd area where technology has not progressed to the extent that many other regions are communication among high-speed networks and local devices. We're talking about great communications capacity, but we don't have it in fact. There's no cost-effective way to get your home, vehicle, or PDA to a gigabit / sec. Prevalent, high-bandwidth communication would enable a range of new critical security apps[5] such as remote medical surveillance and action, remote car control, and military and police personnel's communication-intensive actions.

Scale will be a true challenge as technology progresses. More critical apps for safety will be viable and more figures will be available. Such systems will involve important breakthroughs in both software and system engineering design, growth and implementation.

Conclusion

We are moving quickly to a scenario where computers are "embedded" in both culture and traditional control systems, thus blurring what we mean by an embedded system. As a consequence, severe failure implications occur for all traditional safety-critical applications, but also for completely new applications. Furthermore, completely new failure modes such as denial-of-service attacks on networked information systems are developing. There are several specification elements that are not endorsed by any present method, and even where specification methods exist, there is still a lack of inclusion to allow the assessment of entire specifications.

References

[1] R. Turner, “Security,” in *Implementation and Applications of DSL Technology*, 2007.

[2] Homeland Security, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” *Ics-Cert*, 2016.

[3] T. Homer-Dixon *et al.*, "Synchronous failure: The emerging causal architecture of global crisis," *Ecol. Soc.*, 2015.

[4] J. Leners, T. Gupta, M. Aguilera, and M. Walfish, "Improving availability in distributed systems with failure informers," in *NSDI,* 2013.

[5] P. Singh, P. Tiwari, and S. Singh, "Analysis of Malicious Behavior of Android Apps," in *Procedia Computer Science*, 2016.