Abstract

Software Failure Modes and Effects Analysis (SFMEA) is a traditional system safety analysis technique which is widely used in the aerospace, automotive and other safety-critical intensive systems. However, traditional FMEA methods are difficult to identify and analyzing the failure modes which caused by the dynamic logical information between interfaces or functions, such as software-hardware interaction. To intuitively assume the effects of module failures in a system, numerous approaches have been proposed. This work addresses the use of SFMEA by using an experiment for safety-critical embedded control systems. The work presented here provides a general example illustrating how SFMEA can be effectively applied to an 8-bit micro-controller (Chip 89S52) based computer control system having little or no hardware protection. This paper also describes Functional FMEA, interface FMEA, and detailed software FMEAs. The experimental results of SFMEA also found the hardware failures and memory faults. The safety analysis reveals several design deficiencies and physical faults for which modifications are needed. This paper also found that, when properly implemented SFMEA at
the right point in the Software Development Life cycle, it makes requirements, design and code reviews more effective. It also identifies single point failures due to software.

References

Index Terms

Computer Science  Control Systems

Keywords

BPCS, Software Safety, SFMEA