The computer has become the design component of choice in realizing control and monitoring systems for applications in aerospace, ground transportation, oil and chemical processing, medical electronics, and many other industrial sectors where the safety of life, property, and the environment are at risk. This is a practical, how to technical book that will show the reader how computer systems work and how they must be designed to make them safe. The text explains workings of all the principal components in the system including computer hardware (microprocessors, microcontrollers, PLCs, industrial controllers, etc.), software (from machine language through high level functional diagrams and ladder logic), field instruments (sensors for pressure, temperature, switch contacts, etc.), control elements (actuators, valves, motors, etc.), digital and analog and data communication interfaces, power sources (electrical, hydraulic, pneumatic, etc.), and human operator including man-machine interface. Addressing the safety-critical application, the book shows how these hardware, software, and human components and their interfaces fail and how and where protective safety devices are designed into the system to protect against the effects of the failures. The full range of system safety devices is discussed including hardwired interlocks, computer hardware safety devices (self-tests, watchdogs, end-arounds, etc.), software-implemented safety routines (sensor checks, analytical redundancy, actuator wraparounds, safety assertions and permissives, etc.), as well as high-level protective measures (overpressure devices, limit switches, check valves, etc.). The book shows the reader how hardware redundancy and software redundancy are built into a system to make it fault tolerant and how one defines (or selects from a vendor) the correct redundant architecture (e.g. backup, dual, or triplex, structure) for the application at hand. Emphasis is placed on the often ignored, but crucial, workings and limitations of the redundancy management algorithms resident in user or vendor fault tolerant architectures. Once
hardware and software safety devices and redundancy have been incorporated in a design, the burden falls on the designer and safety analyst to show that these collective measures will produce a system that meets required levels of safety as defined in the applicable safety standard (such as IEC 61508, ISA 84 series, MIL-STD-882D, etc.) The book shows the reader how to systematically verify (using failure mode analysis, fault tree analysis, and risk estimation) that the designed-in safety measures will cover all causes that can lead to catastrophic failure and that overall safety requirements (stated in the standards in terms of acceptable risk and availability) can be satisfied. To assist the reader, the book provides a checklist which can be applied to any real life safety-critical computer system design to verify that all necessary safety measures have been taken. The book is illustrated throughout with examples and figures and includes numerous engineering tables that can used in designing and analyzing real-life systems.

My Personal Review:
This text provides a high-level introduction to the concept of system safety for the engineer involved in embedded control/computer controlled systems.

The first 100 or so pages of the text are simplistic and of little value to anyone already involved in designing a safety-related system but do serve to introduce the example systems to be used throughout the remaining text and the concepts of how such systems typically fail.

Things get complicated quickly after those first hundred or so pages - Dunn basically introduces every failure mode evaluated and every mitigation technique employed by me in my latest project within about 30 pages. It is because of this rapid introduction of concepts at a high level that I suggest this text as introductory rather than as a reference.

The inclusion of 882 in an annex almost appears to be filler. If anything I would suggest removal of the 882 annex and inclusion of a discussion of how to pull a safety case together for a regulatory authority/ISA that complies with 882 or 61508.

This is not light reading. If you skim you will miss important concepts - Dunn's writing style is efficient and seemingly minor statements are, in fact, fundamental concepts of safety-related design that the developer needs to conduct further research in to.

For More 5 Star Customer Reviews and Lowest Price: