



How Safe Are Your Systems? BBBB (Buy)

Safety Shutdown Systems: Design, Analysis, and Justification by Paul Gruhn and Harry L. Cheddle
Reviewed by Nick Sands

Gruhn and Cheddle's book, *Safety Shutdown Systems*, is an easy and informative read on a difficult subject. Paul Gruhn is a consultant for safety systems, a member of SP84, and a past director of the ISA Safety Division. Harry Cheddle is an Engineering associate with Bayer. Their book provides an excellent explanation of the terms, steps, and issues in safety systems design.

The first chapters cover the life cycle of a safety instrumented system, an interesting discussion on risk and risk measurement, and the difference between control systems and safety systems. Control systems are active, causing changes in the process that reveal most failures. Safety systems however, are passive, waiting for a demand before taking action, so failures may remain undetected until it is too late. It is the undetected dangerous failures that limit the safety performance of a system.

The next chapters cover protection layers, the safety requirements specification (SRS), and some methods for determining the safety integrity level (SIL). The SRS consists of the functional requirement specification or what the system does, and the integrity requirement specification or how well the system needs to do it. The SIL for an interlock is part of the integrity requirement specification. According to the UK's Health Safety Executive, approximately 44 percent of safety system accidents are caused by inadequate specification. (I would suggest that projects in general fall close to that mark).

The authors next compare different safety system technologies for safety and reliability, which are not the same thing. The safety of a system is related to its probability of failure on demand (PFD) to a dangerous mode which is related to the mean time to fail dangerously (MTBF_d). This can be stated in unit years: 1/1000 yrs means that if 1000 units operated for 1 year, 1 would fail. This is not quite the same as saying a single unit would operate for 1000 years before failure. The safer the systems the lower the PFD. But a system can be safer and less reliable. Reliability is related to the mean time between failure to a safe mode. While these failures may not directly create an unsafe situation, they often cause shutdowns and start-ups which are more dangerous operating states than normal operation. The authors show how to evaluate the safety and reliability of systems with several examples. Special attention is given to field devices since ~90% of system failures are associated with these components. Field devices with diagnostics can significantly improve the performance of a safety instrumented function.

The remaining chapters cover more aspects of engineering a safety system, the steps involved in installation, some discussion on testing, and a chapter on management of change for safety systems. Testing also impacts the PFD. In fact, a system that is never tested is doomed to fail (mathematically). There is also a chapter on justification that demonstrates a method for estimating the lifecycle costs and the benefit of reliability in SIS design. The last two chapters include a useful checklist that covers most of the SIS lifecycle and a case study showing most of the steps discussed in the book.

Safety Shutdown Systems is written in a conversational and sometimes even humorous style where the authors ask questions for the reader to consider. Gruhn and Cheddle also share many anecdotes about installed safety systems that give the reader pause. It is easy to see why this book was a winner of the Raymond Malloy award and a best seller for ISA, where it's available at the member price of \$69. Though the information is about 5 years old, it has not changed. I recommend this book as a strong buy (BBBB).