



## Measuring Safety - BBBB (Bonus)

*Safety Instrumented Systems Verification: Practical Probabilistic Calculations* by William Goble and Harry Cheddie

Reviewed by Nick Sands

Following close on last fall's approval of the new safety instrumented systems standard *ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) Functional safety: Safety Instrumented Systems for the process industry sector*, the new book by William Goble and Harry Cheddie is the right book at the right time. *Safety Instrumented Systems Verification: Practical Probabilistic Calculations* is a well written and useful reference for anyone working with safety systems. Both Goble and Cheddie have written other safety related books for ISA. Dr Goble, currently a principle partner at Exida, has over 30 years of experience and holds degrees from Penn State, Villanova, Eindhoven University of Technology. He is an ISA Fellow, a PE, and a Certified Functional Safety Expert (CFSE). Cheddie, also currently a principle partner at Exida, has many years of experience. He is certified by ASQ as a quality software engineer and a reliability engineer, a PE, and a CFSE.

This book starts with a very clear overview of the safety lifecycle, which gives a picture of how the different tasks related to safety systems fit together according to IEC61508 and S84/IEC61511. Next is an explanation of what a safety instrumented system (SIS) is and how it is different from a basic process control system (BPCS), a good thing to understand. The following chapters build up a basic understanding of the reliability engineering terms and calculations used in SIS verification. The failure modes, safe and dangerous, undetected and detected, also impact the verification calculations. Another consideration for the calculations is the demand mode; continuous, high demand, or low demand. Depending on the demand mode, testing can make a significant difference in the calculations, but the authors show some very interesting limits to testing credit

After understanding the basic calculation methods to determine the probability of failure on demand (PFD), there remains the question of what numbers to use and the SIL claim limits for devices and architectures. The authors give guidance on where to get the magic numbers for the calculations and how to develop numbers for sensors, logic solvers, and valves. The discussions set the stage for the industry examples that demonstrate the iterative process of design and calculation.

The final chapter covers the contentious issue of separation, not performing safety functions in a control system, but performing control functions in a safety system. There are also eight appendices that provide background and extensions on topics including statistics, probability, and architectures. The appendices are as well written as the chapters.

Goble and Cheddie have done an excellent job with this book. In short, well written chapters, they explain the language and math of safety systems. The step by step breakdown of the complicated verification calculations makes not only a great guide, but an excellent resource that will be useful for years to come. The appendices also provide an excellent reference. Unless you have a PhD in reliability like Dr. Goble, this is a more than a must buy, its a bonus book. You can find it at ISA for \$89, member price.