Preface to the 1st Edition

With the introduction of electronic programmable systems in safety-relevant applications, "Functional Safety" has become a central concept. The term "Functional Safety" appears in titles of the international standards IEC 61508 and IEC 61511, which were published a number of years ago. These standards define how functional safety can be attained in safety-relevant applications using electrical, electronic and electronic programmable components and systems.

In general, functional safety means that a component or a system performs its safety-relevant task correctly and in accordance with the risk to be managed. The system either performs this function, even if internal faults or failures occur, or will assume a predefined safe state.

To fulfil this requirement, an understanding of safety engineering and a comprehensive knowledge of the existing standards are required. This begins with examining a safety system's lifecycle, performing hazard and risk analysis, specifying the requirements of safety-related components and systems, developing and implementing the systems, and the process ends with the system's operation and maintenance.

The work "Functional Safety" examines all relevant topics in detail. The reader gains an overview on the historical development of safety systems and of the standards related to programmable engineering. This includes the discussion of different application areas as well as national and international standards. The book presents basic concepts such as risk and reliability analysis, faults, root cause analysis and failures as well as all necessary safety-related parameters, their definition and evaluation. This includes both qualitative and quantitative factors.

Hardware and software requirements of a safety-related system are given appropriate consideration as well as the potential approaches and measures for achieving the required quality and safety. The comprehensive section on software is a true highlight as it is often difficult to obtain a thorough overview of this subject. Practical examples of how these concepts are applied round off this section.

IEC 61508, as a basic standard, and IEC 61511, as a sector standard for the process industry, are the currently most important standards on functional safety. Both are comprehensive and complex. The reader gains a clear overview, useful explanations and helpful procedures for applying the standards. Safety management and the required documentation are covered, as are measures for avoiding and controlling faults in a system's hardware and software.

The last section provides terminology and definitions for all relevant concepts and depicts quantitative or statistical parameters.

In my every-day project work and numerous discussions during conferences on safety-relevant systems, I am often asked where appropriate literature can be found about this topic. In my opinion, the author has provided a thorough introduction to the subject matter while simultaneously offering the experienced user a valuable reference work.

I have known the author for many years as an expert who has participated in safety-relevant projects and standardization work. I would underscore his dedication as a contributor to the "TÜV Rheinland Functional Safety Programs", where he provided valuable proposals in interest groups and as an expert for functional safety.

October 2006

Dipl.-Ing. Heinz Gall
TÜV Rheinland Industrie Service GmbH
Business Segment Manager: Automation, Software and Information Technology