Preface

For a number of years, I have been thinking about conceptual issues associated with system safety and in particular software safety which have arisen from international standards, in particular IEC 61508, on the functional safety of electrical, electronic and programmable-electronic (so-called E/E/PE) systems.

There are a significant number of conceptual issues which in principle arose with the first edition of IEC 61508 in 1997, which to my mind have not been solved. Indeed, some of them are nowhere near solved. One is figuring out system verification and validation, including the use of mathematical methods to assure objective properties of the system, its software, and the accompanying documentation. Another is figuring out a notion of system integrity which fits with the varied uses of this term. A third is the use of statistical methods to gain assurance, to high confidence (but not certainty), that a system behaves functionally the way it was designed.

Some major themes, such as cybersecurity, and also the effective integration into customary practice of the toolsets associated with so-called formal methods, mathematical methods for assurance of certain objective properties of designs, algorithms and software, have increased in importance over the two decades since. And some themes, such as system resilience, are still in their engineering infancy, but gaining in importance as the ability of malfeasant actors to disturb the normal functioning of digital-electronics-based systems is becoming ever more apparent.

One may write about these matters because they are interesting. One may also write with a view to changing engineers' views and attitudes, indeed to changing the views of those engineers who sit on the reviewing panels for the standards, the National Committees and the international Maintenance Teams.

And things do change. Views are proposed, may achieve consensus and are adopted.

And others languish, no matter how technically well-justified. Searching for a word to describe a series of argued technical viewpoints which may well evolve with the evolution of views in National Committee and Maintenance Team views, I thought "manifesto" was appropriate. So this is a manifesto – a series of technical views on matters I consider to be at the core of critical-system assurance as it appears in IEC standards.

Peter Bernard Ladkin
Bielefeld, December 2017.