Some "hot issues" in Software-Safety Standardisation

Professor Peter Bernard Ladkin

University of Bielefeld CITEC and Causalis Ltd

Peter Bernard Ladkin is a recognised specialist in system safety. He is Professor of Computer Networks and Distributed Systems at the University of Bielefeld in Germany and lead the group of the same name, but known after its German initials as the RVS Group, in the Faculty of Technology at the University of Bielefeld in Germany.

Peter's interests are: specification, verification, and failure analysis of complex heterogeneous systems, and distributed systems in general. He recently concentrated on problems in rail and aviation contexts, and is the originator of the Why-Because Analysis (WBA) method of causal analysis of incidents, which has been adopted as company standard by Siemens Transportation Systems Rail Automation and Mass Transit Divisions.

Peter has worked in the analysis and optimisation of parallel programs; constraint satisfaction methods and temporal reasoning; and logical, philosophical and ethical issues in computing.

Peter's research specialises in methods for ensuring the reliability, and for analysing the failure, of complex heterogeneous systems, and distributed systems in general. He has specialised mainly in systems used in public transportation, primarily air and rail. Apart from that, he has worked on constraint satisfaction problems and temporal reasoning, and performed combinatorial analysis of message-passing in concurrent systems. He contributes regularly to the ACM's on-line Forum on Risks to the Public in Computing and Related Systems (the Risks Forum). He is especially keen to apply formal and informal logic in systems engineering, where he feels logical techniques could do a lot of good, and is interested in social and ethical issues and consequences of ubiquitous computing.

Peter Ladkin and his group's current collaborations are primarily with system engineers at the Institute of Railway Systems Engineering and Traffic Safety (IfEV) at the Technical University of Brunswick (Braunschweig); Siemens Transportation Systems Rail Automation Division, Research and Development Integrity, in Brunswick; the Chair of Railway Signalling and Traffic Safety Systems at the Technical University of Dresden; and the company Causalis Limited which he founded.

'The IET System Safety conference is one of the three main forums in Europe for researcher and industry exchange on system safety, in which Britain has a leading engineering community and tradition. I am delighted in the strong support for this essential work through the IET, and delighted to contribute.'

Synopsis

Looking to the next version of IEC 61508 and related standards, three issues stand out. First, to include modern state-of-the-practice assurance methods, such as those which can rule out run-time failures.

Second, to formulate a reasonable approach to reuse of preexisting SW (so-called "proven in use" arguments), which turns out to pose a true dilemma. Third, the incorporporation of human-factors issues. An IEC project has started on that. This talk considers the first two issues.