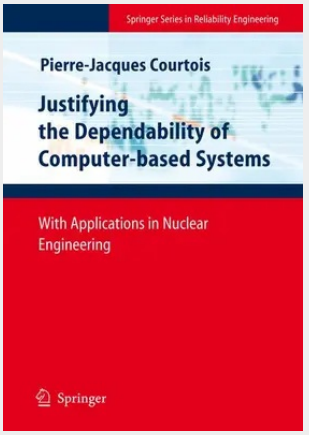
Courtois

Justifying the Dependability of Computer-based Systems

With Applications in Nuclear Engineering



Safety is a paradoxical system property. It remains immaterial, intangible and invisible until a failure, an accident or a catastrophy occurs and, too late, reveals its absence. And yet, a system cannot be relied upon unless its safety can be explained, demonstrated and certified. The practical and difficult questions which motivate this study concern the evidence and the arguments needed to justify the safety of a computer based system, or more generally its dependability. Dependability is a broad concept integrating properties such as safety, reliability, availability, maintainability and other related characteristics of the behaviour of a system in operation. How can we give the users the assurance that the system enjoys the required dependability? How should evidence be presented to certification bodies or regulatory authorities? What best practices should be applied? How should we decide whether there is enough evidence to justify the release of the system? To help answer these daunting questions, a method and a framework are proposed for the justification of the dependability of a computer-based system. The approach specifically aims at dealing with the difficulties raised by the validation of software. Hence, it should be of wide applicability despite being mainly based on the experience of assessing Nuclear Power Plant instrumentation and control systems important to safety. To be viable, a method must rest on a sound theoretical background.

Safety is a paradoxical system property. It remains immaterial, intangible and invisible until a failure, an accident or a catastrophy occurs and, too late, reveals its absence. And yet, a system cannot be relied upon unless its safety can be explained, demonstrated and certified. The practical and difficult questions which motivate this study concern the evidence and the arguments needed to justify the safety of a computer based system, or more generally its dependability. Dependability is a broad concept integrating properties such as safety, reliability, availability, maintainability and other related characteristics of the behaviour of a system in operation. How can we give the users the assurance that the system enjoys the required dependability? How should evidence be presented to certification bodies or regulatory authorities? What best practices should be applied? How should we decide whether there is enough evidence to justify the release of the system? To help answer these daunting questions, a method and a framework are proposed for the justification of the dependability of a computer-based system. The approach specifically aims at dealing with the difficulties raised by the validation of software. Hence, it should be of wide applicability despite being mainly based on the experience of assessing Nuclear Power Plant instrumentation and control systems important to safety. To be viable, a method must rest on a sound theoretical background.

213,99 €
199,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9781849967945
Medium: Buch
ISBN: 978-1-84996-794-5
Verlag: Springer
Erscheinungstermin: 28.10.2010
Sprache(n): Englisch
Auflage: 1. Auflage. Softcover version of original hardcover Auflage 2008
Serie: Springer Series in Reliability Engineering
Produktform: Kartoniert
Gewicht: 522 g
Seiten: 323
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)