

Tutorial on IEEE\AIAA Recommended Practice on Software Reliability Applied to Mobile Devices

**Norman Schneidewind
Mike Hinchey**

Objectives

This tutorial serves to elaborate key software reliability process practices that are included in the IEEE\AIAA Recommended Practice on Software Reliability. The objectives are achieved by first discussing the issues in achieving high reliability in software and how the recommended practice supports achieving that result, followed by examples of applying the recommended practice to the reliability of mobile devices. Given the prevalence of mobile devices in contemporary society and the workplace, it is important to address not only their reliability, but their maintainability and availability, as well.

Due to the prevalence of software-based systems, the focus is on learning how to produce high reliability software. However, since hardware faults and failures can cause the highest quality software to fail to meet user expectations, considerable coverage of hardware reliability is provided. Practice problems with solutions are included to provide the engineer with real-world applications of the principles that are discussed.

Software-based systems have become the dominant player in the computer systems world. Since it is imperative that computer systems operate reliably, considering the criticality of software, the IEEE and AIAA commissioned the development of a new standard called, the Recommended Practice on Software Reliability, IEEE P1633 [IEE08]. While the focus of the IEEE P1633 Standard is software reliability, software and hardware do not operate independent of one another, therefore, both software and hardware are addressed in this tutorial in an integrated fashion.

What you can expect to take away from this tutorial is oriented to the key reliability issues described below. Audience participation is encouraged to bring to the tutorial the experience, knowledge, and opinions of the participants.

Issues

Issue 1. Why Have a Recommended Practice for Software?

It is important for an organization to have a disciplined process if it is to produce highly reliable software. This process uses a life cycle approach to software reliability that takes into account the risk to reliability due to software errors caused by requirements changes.

Issue 2. Both Hardware and Software Reliability are Important

Before analyzing reliability for your products, you must fully understand what constitutes lack of reliability. Computer systems, whether hardware or software, are subject to failure.

Issue 3: Do not Neglect Software Reliability Engineering Risk Analysis

Often, there is excessive focus on the test phase and reliability models and predictions. While important, this is not the whole story. Software Reliability Engineering (SRE) is an established discipline that can help organizations improve the reliability of their products and processes through a *life cycle approach*. The process takes into account the risk to reliability due to requirements changes.

Issue 4. Can Software Reliability Models be Applied to Mobile Devices?

Reliability models are central to making predictions of the reliability of various types of software, but are they applicable to mobile devices? Reliability has become very important as new critical applications emerge for mobile phones (e.g., robot control, traffic control, and telemedicine). In such scenarios, a phone failure affecting the application could result in a significant loss or hazard (e.g., a robot performing uncontrolled actions).

Issue 5. What are the Characteristics of Mobile Device Failure Data?

Symbian OS-based smart phone failure data were collected from 25 phones (in Italy and USA) over a period of 14 months. Key findings indicate that: (i) the majority of kernel exceptions are due to memory access violation errors (56%) and heap management problems (18%). This tutorial will show how to apply SRE to improve the reliability of mobile devices – the same process that can be applied to other software intensive systems.

Biography

Dr. Norman F. Schneidewind (ieeelife@yahoo.com, 831-375-5450) is Professor Emeritus of Information Sciences in the Department of Information Sciences and the Software Engineering Group at the Naval Postgraduate School. He is now doing research and publishing in software reliability and metrics with his consulting company Computer Research. Dr. Schneidewind is a Fellow of the IEEE, elected in 1992 for "contributions to software measurement models in reliability and metrics, and for leadership in advancing the field of software maintenance". In 2001, he received the IEEE "Reliability Engineer of the Year" award from the IEEE Reliability Society. In 1993 and 1999, he received awards for Outstanding Research Achievement by the Naval Postgraduate School. Dr. Schneidewind was selected for an IEEE USA Congressional Fellowship for 2005 and worked with the Committee on Homeland Security and Government Affairs, United States Senate, focusing on homeland security and cyber security (see photo below).

IEEE-USA's four Government Fellows began their Fellowships in January 2005: Randall Brouwer (with Representative Dana Rohrabacher); Gordon Day (with Senator Jay Rockefeller); Norman Schneidewind (on the Senate Homeland Security Committee); and Nick Zayed (with the State Department Office of Science and Technology Cooperation).

Shown at the Jefferson Memorial in Washington, D.C., are left to right: IEEE-USA Government Fellows: Norman Schneidewind, Nick Zayed, Randall Brouwer, and Gordon Day

