Software Reuse and Safety

William B. Frakes[1] and John Favaro[2]

[1] Department of Computer Science, Virginia Tech,
7054 Haycock Rd., Falls Church VA 22043
frakes@cs.vt.edu
[2] Intecs SpA, Via Giannessi 5,
56100 Pisa, Italy
john.favaro@intecs.it

Abstract. This tutorial addresses issues and current practices regarding the important topic of the interaction of software reuse and safety. This topic has become very relevant to modern embedded systems in domains from aerospace to automotive, as new architectures are introduced that encourage the development and use of reusable components. The two sections of the tutorial provide first an introduction to the theoretical concepts relevant to safety-related software development, and then an introduction and discussion of concrete examples in today's industry. Current examples of standards regulating reusable software components in safety-critical domains are presented. An example from the automotive industry is presented in more detail.

1 Software Safety and Reuse

Topics covered include: safety definitions, a discussion of software safety myths, presentation of real world software safety disasters, a categorization of types of reuse, an introduction to the most prominent reuse and safety issues, a presentation of the key concept of safety integrity levels, and a discussion of the relationship between dependability and safety.

2 Current Industrial Practice in Software Reuse and Safety

Topics include: an overview of reuse standards and practice in selected safety critical sectors (aerospace, railway, space); a discussion of current safety-related reuse concepts in industry (e.g. problems related to achieving certification, and the implementation of so-called 'proven in use' concepts); and an in-depth presentation of reuse-oriented issues in the automotive industry today, including a discussion of the new AUTOSAR architecture and ISO 26262 safety standard.

K. Schmid (Ed.): ICSR 2011, LNCS 6727, p. 246, 2011.