Preface

Cyber-physical systems representing networked computational systems controlling physical entities build on the concepts of embedded and autonomous systems that can be enhanced by methods of artificial intelligence. They are spatially and temporally determined and need to be aware of that during their operation, for the signals from their environment to be adequately captured and assessed. They need to expose properties, native to autonomous systems: self-management, self-configuration, self-optimization, self-protection and self-healing. An important emphasis while using these systems lies with the concepts of their timeliness, functional correctness, safety of their operation as well as security of their transferred and stored data, which need to be assured according to appropriate standards on all levels of their operation. Hence, they need to be designed holistically by using the systems approach and engineering with respect to these standards.

The dependability of cyber-physical systems is usually assured by redundancy and over-scaled components. This results in more complex designs and higher costs, but often without guaranteeing safety or security. To achieve better overall quality, much effort was invested in the search for standardized components, methods and tools apt to improve the designed system's predictability and dependability. The design and development procedures of contemporary cyber-physical systems are well established, relatively cheap and widely used. Hardware components come with specifications, which undoubtedly state their capabilities and performance indicators. Complexity increases, however, when there is a need for their integration into larger set-ups and system-level performance must be assured. Software makes things even more complicated, as the WORE (Write-Once-Run-Everywhere) principle is hard to achieve, and different software engineering techniques can lead to programs with very different quality-of-service while running on the same hardware platform. To achieve a managed level of quality (of service), systems engineering methods should enable hardware–software co-design as well as efficient system's design and subsequent prototype verification and validation before putting them to use.

Throughout this book, a holistic quality of service-oriented approach to design and development of cyber-physical systems, with emphasis on their (timely) predictable and dependable behaviour, is presented and discussed. By following the standards for embedded system's safety and using appropriate hardware and software components inherently safe system's architectures can be devised and certified. At the same time their complexity is reduced to a reasonable level. The methodology and guidelines for designing and developing cyber-physical systems will result in their increased ability to be certified for safety and security as well as their improved interoperability.

Celje Roman Gumzej
January 2015

Springer

http://www.springer.com/978-3-319-28903-8

Engineering Safe and Secure Cyber-Physical Systems
The Specification PEARL Approach
Gumzej, R.
2016, XIII, 128 p. 28 illus., Hardcover
ISBN: 978-3-319-28903-8