Modern society is increasingly dependent on complex software systems for operating its critical infrastructures, including transportation, communication, finance, energy distribution, and healthcare. As a result, the consequences of failures are becoming increasingly severe. We believe that the growing recognition of risks and consequences of failures will lead to increasing use of rigorous specification and verification techniques for such systems.

The Advances in Software Specification and Verification minitrack focuses on research and applications that will drive widespread use of rigorous specification and verification technologies, particularly for complex, large-scale systems. Topics include new specification and verification techniques, methods for scale-up to large systems, techniques for complexity reduction in specification and verification, integration of specification and verification methods, development of engineering practices and tools, and case studies.

We accepted three papers for this year’s minitrack that provide an excellent overview of current research in system specification and verification. The papers cover a number of emerging research areas, including use of box structures for system specification in the context of Strategic Information Systems Planning, integration of viewpoints, use-cases, and sequence-based methods for specification, and use of wrapping-based architectures and anomaly detection algorithms to achieve system-level analysis and verification. At least three external reviewers and both minitrack chairs refereed each of the submitted papers. The accepted papers are summarized below.

The Strategic Information Systems Planning (SISP) process seeks to align business strategy with computer-based information systems to achieve business objectives. Yet many SISP efforts are not successful due to the difficulty of implementing recommendations. A significant contributing factor is the specification gap that exists between the definition of recommended systems and their detailed implementations. In the case study paper by Alan Hevner, Donald Berndt, and James Studnicki, box structure technology is employed as a solution to this problem, and a SISP method based on box structure specification is defined. Partial results of a case study are presented to illustrate use of box structures to bridge the specification gap. The bridging is enabled by the scale-free nature of box structures, which permits their uniform application at all levels of detail. The authors demonstrate advantages of the box structure approach, including ease of use, natural representations, and rigorous descriptions.

The value of rigorous specification methods, such as the box structure sequence-based specification technique, is often limited by the ability of a specification team to fully understand system requirements. Viewpoints and use-cases address this need by supporting requirements elicitation. In a complex system, however, it is difficult to reconcile these views and translate their unique semantics into unified and coherent specifications to support system development. The paper by Gwendolyn Walton describes a process for combining the strengths of viewpoints, use-cases, and sequenced-based specification to produce complete and correct specifications of system behavior that can be traced to requirements. Combining the strengths of each of these methods yields improved specifications and reduces errors and misunderstandings.

It is well understood that complex systems are difficult to analyze and verify. Verification at the component level has progressed to the point where verification analysis of all the components of a complex system can be produced. What remains is system-level verification. The paper by Christopher Landauer and Kirstie Bellman defines an approach to system development that can contribute to system-level verification. The authors introduce a knowledge-based system integration infrastructure based on wrappings, and discuss algorithms (originally developed for verification of knowledge-based systems) for detecting anomalies in systems. They show how systems organized using wrappings are particularly amenable to correctness verification, both offline and online. The authors assert that wrapping-based architectures help make system-level specifications more transparent and analyzable, and system-level verification and testing more reliable.