Modern society is increasingly dependent on software systems of remarkable scope and complexity. Yet methods for assuring dependability and quality of these systems have not kept pace with their rapid deployment and evolution. The result has been persistent errors, failures, vulnerabilities, and compromises. Research is required in assurance technologies that can scale beyond present labor-intensive practices that are increasingly overwhelmed by the task at hand. Many organizations in academia, industry, and defense are interested in this subject, but often with a focus on specific subject-matter areas. The goal of this Minitrack is to bring together researchers from all areas of system assurance to promote sharing and cross-pollination of promising methods and technologies. We will promote a unified assurance discipline characterized by science foundations and substantial automation that can effectively address the scope and scale of the problem. This year the ARDSS Minitrack presents six papers that introduce tools and techniques for development of secure software.

The first paper, “Foundations for Software Assurance” by Carol Woody, Nancy Mead, and Dan Shoemaker introduces key principles for software assurance, and discusses a new curriculum that has been developed for a master’s degree program in software assurance. The curriculum addresses current disconnects among research, education, and practical development of assured software. The paper maps elements of the curriculum to the key principles to demonstrate coverage.

In the second paper, “Business Process Mining and Reconstruction for Financial Audits,” authors Michael Werner, Nick Gehrke, and Markus Nüttgens discuss the mismatch between voluminous automated financial transactions in organizations and the largely manual methods employed to audit them. They show how business process mining and reconstruction can be employed to overcome this discrepancy and provide a basis for automated procedures for financial audits.

The third paper, “Determining Software Product Release Readiness by the Change-Error Correlation Function: On the Importance of the Change-Error Time Lag,” by Roman Wild and Philipp Brune discusses a new model for error prediction in software projects based on linear response theory and the change-error cross-correlation function. This work shows the importance of considering the number of changes as well as the number of errors in making release decisions for a software product.

In the fourth paper, “Analyzing Workflows in Business Processes for Obstructions Due to Authorization Policies,” authors Nick Spear, Sreekanth Malladi, and Sandeep Lakkaraju discuss the problem of aligning security policies with business objectives. They present a new approach to analyzing workflows to avoid obstructions (deadlocks) due to authorization policies. An algorithm is given for determining if a workflow is obstruction-free for given authorization policies. This work incorporates loops, conditions, and parallelism in the analysis, and is illustrated with workflow analysis in financial and healthcare areas.

The fifth paper, “Hardware-assisted Application Integrity Monitor,” by Jiang Wang, Kun Sun, and Angelos Stavrou, discusses the difficulty of hardware-assisted detection of tampering in dynamically allocated applications. They propose a hardware-assisted framework based on semantic information in source code and input from developers. This framework provides a correct view of application state for extraction and inspection, and can also monitor dynamically spawned applications.

In the sixth paper, “Improving Security Assurance of Embedded Systems Through Systemic Dissolution of Architected Resources,” authors Michael Wilder and Robert Rinker discuss improving security assurance of embedded systems through systematic dissolution of architected resources that reduces the attack surface. This approach involves automatic transformation of binaries into circuitizable finite state machines with datapath (FSMD) descriptions.