digital configurations. The integration of newer methods in the safety assurance of critical systems could provide significant improvements in the review process by providing information earlier in the life cycle and with higher coverage and lower effort, and in less time.

While effective, the current regulatory infrastructure does not meet some of the characteristics—such as efficiency or agility—that would characterize a modern regulatory infrastructure. As part of the longer-term effort, the staff will review and modify the current regulatory structure to be more performance-based and flexible by using new methods in the most effective way and updating the regulatory and guidance structure to acknowledge changes in the technology, the way it is developed, and how it is used. The staff will evaluate the results of implementation of the tactical activities (MP #1, MP #2, MP #3, and MP #4A) and, with continued stakeholder interaction, will develop a performance-based, technology neutral regulatory infrastructure that will anticipate the evolution and future development of digital I&C technology as it is applied to nuclear technologies.

Possible models

As part of this effort, the NRC staff will investigate a number of possible models for providing the desired characteristics in a modernized regulatory infrastructure. The kind of model that could be used, however, is somewhat constrained by the fact that digital I&C regulatory infrastructure must continue to conform to the more general NRC regulatory infrastructure. While the NRC's regulatory infrastructure is recognized by other nuclear regulators as the most comprehensive and is utilized by many of them, the NRC staff also works proactively to learn of improvement opportunities from the other regulators' experiences. The following are some possible models that could be considered in a modernization strategy.

■ *Adopting a reasoning structure for analysis and evaluation*. The NRC's safety focus leads us to consider the assurance-case approach as a framework to organize NRC's licensing infrastructure. In a recent workshop, experts from the United Kingdom's Office of Nuclear Regulation and the U.S. Food & Drug Administration medical devices group reported favorable experiences with their shift to the assurance-case paradigm. The underlying concept, known as the "Toulmin model," was formulated over 60 years ago and has been used across various disciplines, including social sciences, computer science, and software and systems engineering. Starting from the end goal (e.g., "system is safe"), information is organized along logical propositions to demonstrate (or to check) that the end goal is satisfied. This logical organization helps identify the information that is necessary and sufficient to satisfy the safety goal. ISO/IEC Standard 15026-2:2011, *Systems and software engineering—Systems and software assurance–Part 2: Assurance case,* defines the structure of an assurance case, such that it can be consistent and comparable across usages by different people. While maintaining the rigor of a logical proposition structure, ISO/IEC 15026 also provides for the representation of uncertainty and its usage in determining the level to which the safety goal is satisfied. Mapping the existing guidance along an assurance case structure would help identify overlaps, inconsistencies, technical deficiencies, and gaps in the existing guidance.

■ *Improved methods of hazard analysis.* In the context of analyzing or evaluating a digital system, the concern is the degradation of the performance of the safety function associated with the system. In this context, a hazard is the potential for the degradation of the performance of that safety function. Although hazard analysis has been a cornerstone of the NRC's regulations for nuclear power plants and is required per NRC-endorsed consensus standards, the NRC does not have the