A Method for Quantifying the Dependability Attributes of Software-Based Safety Critical Instrumentation & Control Systems in Nuclear Power Plants

PI: Dr. Carol Smidts- Ohio State University **Collaborators**: Tedd Quinn- Technology Resources

Program: NEET: Advanced Sensors and Instrumentation

ABSTRACT:

The lack of systematic science-based methods for quantifying the dependability attributes in software-based instrumentation and control systems in safety critical applications has shown itself to be a significant inhibitor to the expanded use of modern digital technology in the nuclear industry. This lack of objective basis is rendered significant by the fact that analog technology is aging and becoming obsolete, the new generation of nuclear power plant engineers is now more familiar with digital technology than it is with analog technology, and that the benefits that digital technology offers cannot be tapped into. These benefits include enhanced features, greater diagnostics, prognostics and on-line monitoring capabilities and added flexibility. The NE R&D's NEET-2 program is geared specifically towards addressing factors that inhibit the expanded use of modern digital technology by the nuclear power industry, including demonstrated science-based safety case, and reduction of regulatory uncertainty.

This proposal addresses this need through the development of a method of software dependability quantification as well as its associated science basis. Dependability includes multiple attributes: reliability, availability, safety, integrity, confidentiality and maintainability. The general approach followed will be to identify measures for the different attributes of dependability through expert opinion elicitation; to develop causal models to link measures to threats to the application; to develop models asserting the dependencies between attributes; to define dependability gates which will control the process of development from a dependability perspective and as such reduce the risk (including the licensing risk); to identify dependability attributes most important for a specific application of interest; these models will allow us to asses dependability at different stages of the lifecycle; to verify the practicality, applicability and validity of these measures and models, experiment will be carried out on variants of a function of a safety critical nuclear application which has been licensed. This research will lead to the development of hybrid causal maps, an advanced representation of knowledge, as well as to a more robust elicitation of causal maps which further enhance the science of elicitation.

In the proposed effort, the university PI (U-PI) is partnering with an industry PI (I-PI) and industry collaborators with access to platforms, tools, development information and knowledge on actual systems as well as expertise in the licensing of digital applications for nuclear power plants. The U-PI will develop a quantification method based on expert elicitation, which will capture existing dependability and measurement knowledge, and transform it to a quantification framework. Feasibility of the method will be tested in collaboration with the industry partner. A suitable component of reactor protection system, whose documents and software is accessible within the industry partners non- disclosure-agreement will be selected for the experiment.