T7 Hazard Analysis for Nuclear Automation: Defeating Digital Demons

Digital systems can misbehave even when no component â€œfails.â€ It is the unintended and unexpected behaviorsâ€”the consequences of unknown unknowns in system design and implementationâ€”that can stealthily compromise a safety function. Unintended behaviors are mainly caused by unintended, and unexpected, interactions. The potential for hazardous interactions is increasing with trends toward more networking and sharing of resources across systems of different criticality and across redundant divisions. Traditional hazard analysis practices, developed for hardware-dominated systems, are not able to identify hazards caused by unexpected interactionsâ€”the unknown unknowns. However, newer hazard analysis methods show promise. In this session, experts will discuss whether the state-of-the-art in these methods can enable the safety assurance and evaluation of a critical digital system, such as a reactor protection system, including interactions with the operator and other elements in the system environment. Some questions for discussion include the following:

- Can newer hazard assessment methods reveal the unknown unknowns completely enough for all the eggs to be placed safely in one basket (e.g., eliminate the need for design diversity)?
- How do we know the method can do that?
- What does it take for the hazard analysis to be that good?
- Is there enough evidence to answer these questions?
- If not, is there expert consensus?

Find out in this panel discussion. Demons beware!

SESSION CHAIR(S):

- Stephanie Coffin, Deputy Office Director, RES/NRC e-mail: Stephanie.Coffin@nrc.gov
- Sushil Birla, Senior Technical Advisor for Digital I&C, Division of Engineering, RES/NRC

SPEAKER(S):

- Introductory Remarks

  Stephanie Coffin, Deputy Office Director, RES/NRC

- Hazard analysis for Nuclear Automation Defeating Digital Demon

  Sushil Birla, Senior Technical Advisor for Digital I&C, Division of Engineering, RES/NRC

- Matt Gibson, Technical Executive, Electrical Power Research Institute
- Paul Butchart, Instrumentation and Control Engineer 4, NuScale
- John Thomas, Director, Partnership for Systems Approaches to Safety, Massachusetts Institute of Technology
- Alan Wassyng, Professor, McMaster University
- Mark Vernacchia, GM Technical Fellow, General Motors Company
- Shem Malmquist, Captain, Visiting Instructor, fellow Royal Aeronautical Society, Florida Institute of Technology

SESSION COORDINATOR(S):

- Paul Rebstock, Senior Instrumentation and Control Engineer, Instrumentation Controls and Electrical Engineering Branch, Division of Engineering, RES/NRC e-mail: Paul.Restock@nrc.gov