Identifying Hazards from Engineering Digital I&C Systems: State of the Art

July 27, 2023
Halden (HTO) Workshop:
Modern Hazard Analysis for Safety Assurance

Presenter: Sushil Birla
Office of Nuclear Regulatory Research
Division of Engineering
The views expressed herein are those of the author and do not represent an official position of the U.S. NRC.
Objective

Assess through discussion:

1. Can the state-of-the-art techniques identify all significant hazards in the design of a cyber-physical system as simple as a nuclear reactor protection system?

2. If not:
   1. Limitations?
   2. Promising directions to overcome these limitations?
Insignificant: Support consistent judgment

Safety claim satisfied unconditionally
Residual uncertainty has insignificant effect.
No one can find:
• Any uncontrolled hazard.
• Any unmitigated defeater.

The safety claim is not satisfied with the given evidence.
The evidence gaps are identified.

The safety claim does not hold.
• Fallacies in logic.
• Deficiencies in evidence.
## State-of-the-art: Meaning

### State-of-the-art
- Capability demonstrated in leading-edge implementations.
  - Not yet scaled up.

### State-of-the-practice
- Best-in-class; best practices, e.g.:
- as seen in leading-edge industry consensus standards

### Current practice
- Prolific in many organizations
Reference Framework

Verification Validation (V&V)

\[ V_p \rightarrow V_c \rightarrow V_r \rightarrow V_a \rightarrow V_{dd} \rightarrow V_i \rightarrow V_t \]

System Development

Plans \rightarrow Concept \rightarrow Requirements \rightarrow Architecture \rightarrow Detailed design \rightarrow Implementation \rightarrow Testing

Safety Engineering

Adapted from IEEE Std 1012
Acronyms

- HA$_p$ – Hazard analysis of plans
- HA$_r$ – Hazard analysis of requirements
- HA$_a$ – Hazard analysis of architecture
- HA$_{dd}$ – Hazard analysis of detailed design
- HA$_i$ – Hazard analysis of implementation
- HA$_t$ – Hazard analysis of testing (including test specifications and oracles)
- IEEE – Institute of Electrical and Electronics Engineers
- NPP – Nuclear Power Plant
- NRC – U.S. Nuclear Regulatory Commission
- V&V – Verification and Validation
- V$_p$ – V&V of plans
- V$_r$ – V&V of requirements
- V$_a$ – V&V of architecture
- V$_{dd}$ – V&V of detailed design
- V$_i$ – V&V of implementation
- V$_t$ – V&V of testing (including test specifications and oracles)