CPS Certification (CERT)

To discuss and identify research needs in the certifiable assurance of cyber-physical systems (CPSs), focusing on uncertainties associated with the verification and validation of the complex logic on which these CPSs rely, whether the logic is implemented in software, field-programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), application-specific integrated circuits (ASICs), etc. This growing issue cuts across many application domains affecting society, e.g., medical devices, automobiles, commercial aircraft, and nuclear power plants. Examples of issues experienced:

- The complexity of typical systems in such applications has grown to the level that complete verification coverage takes much longer than the initial development.
- Tool-automated and tool-assisted processes promise to avoid faults caused by human mistakes, but the issue shifts to the assurance of these tools and processes.
- Design-stage verification techniques, e.g. formal methods, simulation, and analysis promise to reduce the effort, but often implementations have fault propagation paths not reflected in the design.
- There is little systematized knowledge to guide integration of verification evidence from the various phases of the lifecycle to evaluate effective coverage for the purpose of safety certification.
- Assuring that safety requirements are complete, correct, and consistent requires high-skill human effort.
- Safety requirements are discovered at every phase of the development lifecycle, e.g. through CPS-internal hazard analysis, FTA, FMEA, etc. However, the volume of information to be processed is very high and the availability of commensurate high-skill human effort, relatively low.
- Assessing the impact of change is a challenge.
- There is inadequate well-accepted guidance or constraints at the conceptual phase of the lifecycle to assure that certain classes of faults or defects will be prevented.

Node: Type

Apply

Validation and Verification Special Interests Group