High Assurance Autonomous Control Systems

Data sharing and preservation

Data management plans should describe whether and how data generated in the course of the proposed research will be shared and preserved and, at a minimum, describe how data sharing and preservation will enable validation of results, or how results could be validated if data are not shared or preserved.

This research will generate formal specifications (temporal logic), discrete automata models, continuous controller implementations, simulation data from SmAHTR models, and hardware-in-the-loop validation results. Digital research data necessary to validate findings include: synthesized controller code, FRET requirement specifications, Simulink reactor models, and experimental performance metrics.

All code will be documented following standard software engineering practices with inline comments and README files. Controller specifications will use FRET and temporal logic formats compatible with reactive synthesis tools. Simulation data will be stored in CSV format with accompanying metadata describing experimental conditions.

All research artifacts will be published in a public GitHub repository under an open-source license immediately upon publication of research findings. The repository will remain publicly accessible indefinitely through GitHub's standard preservation policies. No proprietary software is required for data access.

Open access to controller synthesis methodologies and validated implementations will accelerate adoption of formal methods in nuclear control systems and enable reproducibility of safety-critical autonomous control research.

Data used in publications

Data management plans should provide a plan for making all research data displayed in publications resulting from the proposed research open, machine-readable, and digitally accessible to the public at the time of publication. This includes data that are displayed in charts, figures, images, etc. In addition, the underlying digital research data used to generate the displayed data should be made as accessible as possible to the public in accordance with the Principles published in the DOE Policy for Digital Research Data Management. The published article should indicate how these data can be accessed.

All data displayed in charts, figures, and images in publications will be made publicly available in machine-readable formats (CSV, JSON) in the project's GitHub repository at the time of publication. Underlying digital research data used to generate all visualizations and results will be included with comprehensive metadata. LaTeX source files for papers will also be published to enable full reproducibility. Each publication will include a data availability statement with direct links to the corresponding datasets and source files in the repository.

Data management resources

Data management plans should consult and reference available information about data management resources to be used in the course of the proposed research. In particular, DMPs that explicitly or implicitly commit data management resources at a facility beyond what is conventionally made available to approved users should be accompanied by written approval from that facility. In determining the resources available for data management at DOE Scientific User Facilities, researchers should consult the published description of data management resources and practices at that facility and reference it in the DMP.

This research will utilize standard computational and data management resources provided by the University of Pittsburgh Cyber Energy Center, including local computing infrastructure for simulation and data storage. Hardware-in-the-loop testing will use Emerson Ovation control equipment already available at the Center for approved research use. All data management activities fall within conventional resource allocations for approved users and do not require additional commitments beyond standard laboratory access. No DOE Scientific User Facilities will be utilized for data management.

Confidentiality, security and rights

Data management plans must protect confidentiality, personal privacy, Personally Identifiable Information and U.S. national, homeland, and economic security; recognize propriety interests, business confidential information, and intellectual property rights; avoid significant negative impact on innovation and U.S. competitiveness; and otherwise be consistent with all applicable laws, regulations, agreement terms and conditions, and DOE orders and policies.

This research involves no collection or processing of Personally Identifiable Information. All published data will be reviewed to ensure compliance with export control regulations and nuclear security requirements before public release. Any proprietary information from industry partners (e.g., Emerson control system specifications) will be excluded from public repositories or shared only with appropriate written permission. Controller implementations will be published at a methodological level that advances scientific knowledge while avoiding disclosure of sensitive facility-specific details that could impact national or homeland security. All data management practices will comply with applicable DOE orders, export control laws, and university intellectual property policies.

Planned Research Outputs

Model representation - "Controller Proof Artifacts"

All artifacts created in the process of generating a hybrid autonomous controller will be disseminated, including all intermediate representations. These include formal specifications in FRETtish, hybrid automata in the form of .dot files, and finally built controllers in the form of Simulink models.

Planned research output details

Title	Type	Anticipated release date	Initial access level	Intended repository(ies)	Anticipated file size	License	Metadata standard(s)	May contain sensitive data?	May contain PII?
Controller Proof Artifacts	Model representation	2027-08-30	Open	None specified		None specified	None specified	No	No