INL/MIS-23-74599-Revision-0

LWRS Program Research on Risk Assessment of Safety-related Digital I&C Systems

September 2023

Han Bao

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-23-74599-Revision-0

LWRS Program Research on Risk Assessment of Safety-related Digital I&C Systems

Han Bao

September 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

LWRS
LIGHT WATER REACTOR SUSTAINABILITY

2023 NRC Fall Risk Forum

Han Bao
Idaho National Laboratory
09/12/2023

LWRS Program Research on Risk Assessment of Safety-related Digital I&C Systems

Light Water Reactor Sustainability (LWRS) Program

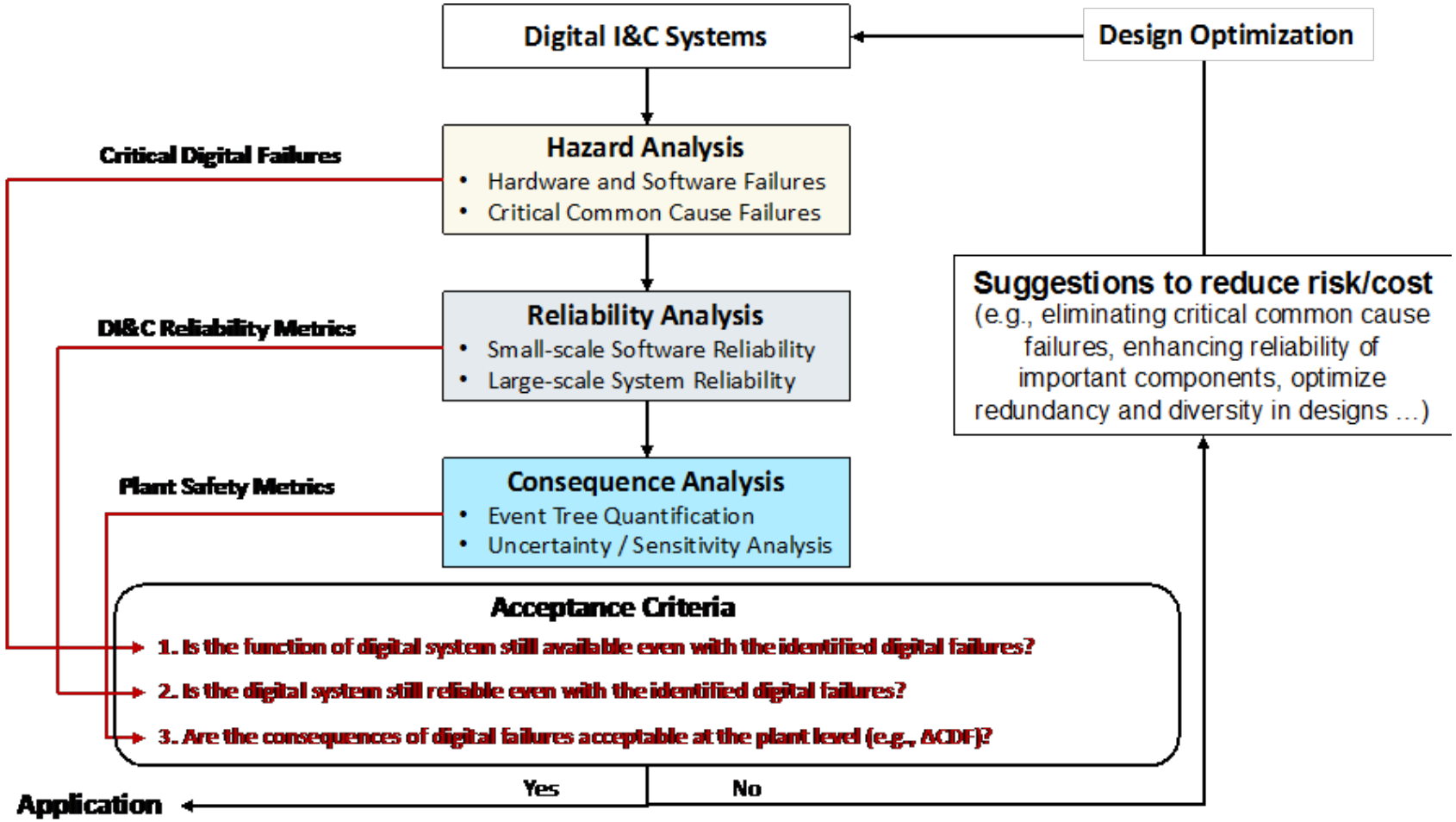
LWRS Goal

Enhance the safe, efficient, and economical performance of our nation's nuclear fleet and extend the operating lifetimes of this reliable source of electricity

Plant Modernization	Enable plant efficiency improvements through a strategy for long-term modernization
Flexible Plant Operation & Generation	Enable diversification and increase revenue of light water reactors by extracting electrical and thermal energy to produce non-electrical products
Risk Informed System Analysis	**Develop risk assessment methods and tools to optimize the safety, reliability, and economics of plants**
Materials Research	Understand and predict long-term behavior of materials in nuclear power plants
Physical Security	Develop technologies and the technical bases to optimize physical security postures

Goals of LWRS-RISA Efforts on DI&C Risk Assessment

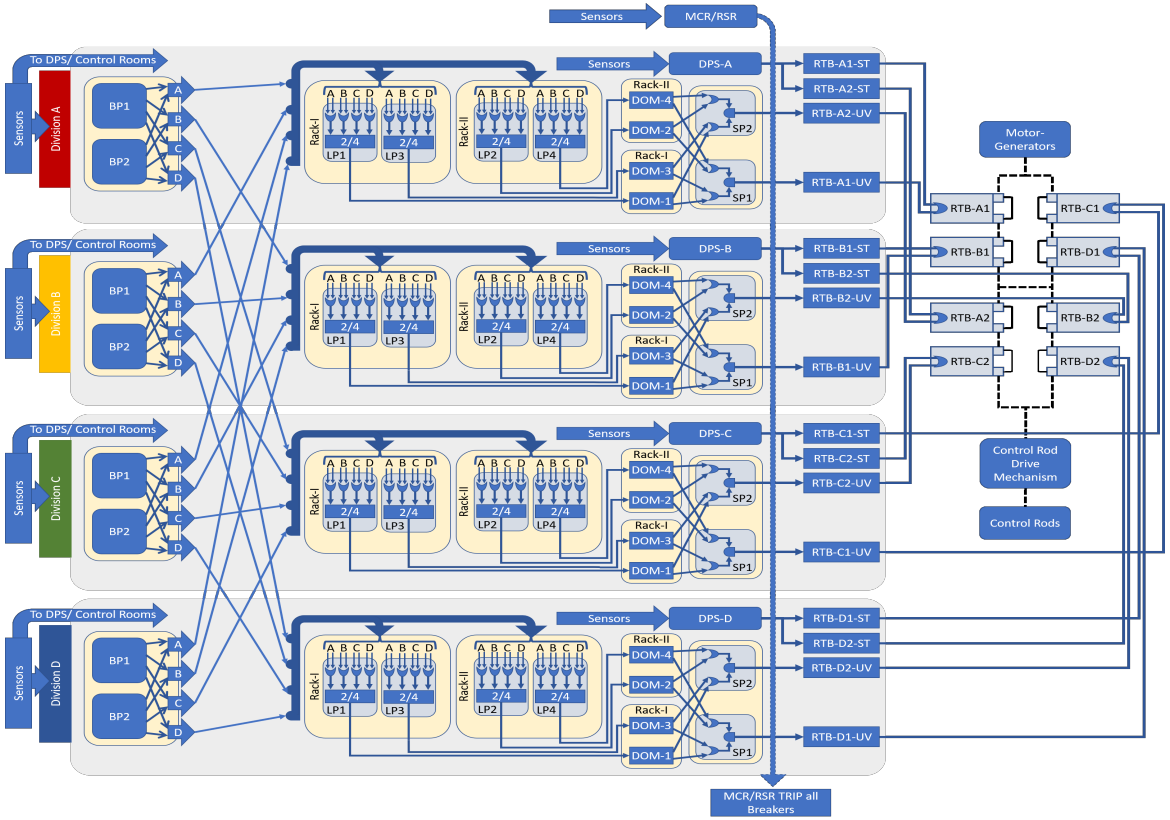
- **Offer a capability of design architecture evaluation** of various DI&C systems to support system design decisions on **diversity and redundancy applications**;
- Develop approaches to **address CCFs and estimate corresponding failure probabilities** for DI&C technologies;
- **Support existing risk-informed DI&C design guides** by providing quantitative risk-informed evidence.



Value Proposition

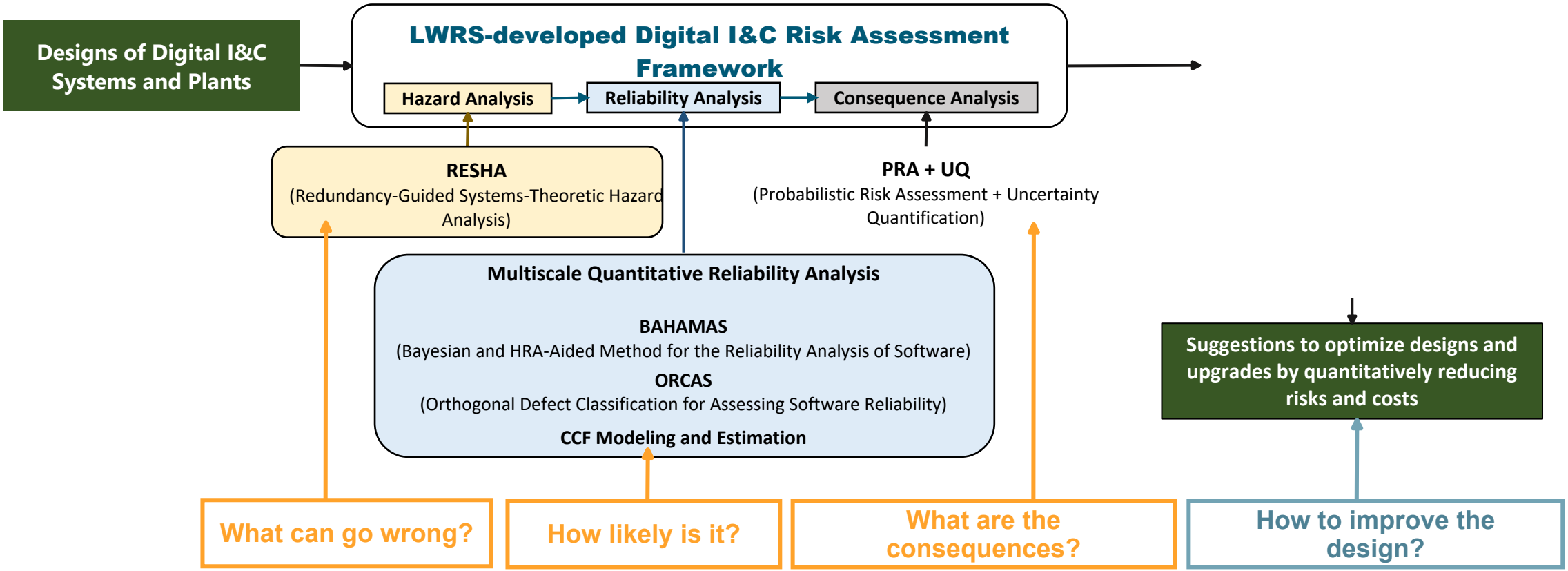
- **The framework** is envisioned and developed as **an integrated risk-informed tool** to support vendors and utilities with optimization of design solutions from economical perspectives GIVEN the constrain of meeting risk-informed safety requirements.

- **Quantitative Risk Analysis**
  - Software reliability metrics → DI&C system reliability → Plant safety analysis
- **Risk-informed Design**
  - Management strategy of CCFs
    - All elimination vs. selective elimination
  - Level of redundancy
    - 4 divisions vs. 2 divisions
    - 4 vs. 2 local logic processors per division
  - Level of diversity
    - Design: Analog? Digital? A combination of both?
    - Software: Design requirements, programming language, etc.
    - Hardware Equipment: Manufacturers, designs, architectures, etc.



A Four-Division Digital Reactor Trip System

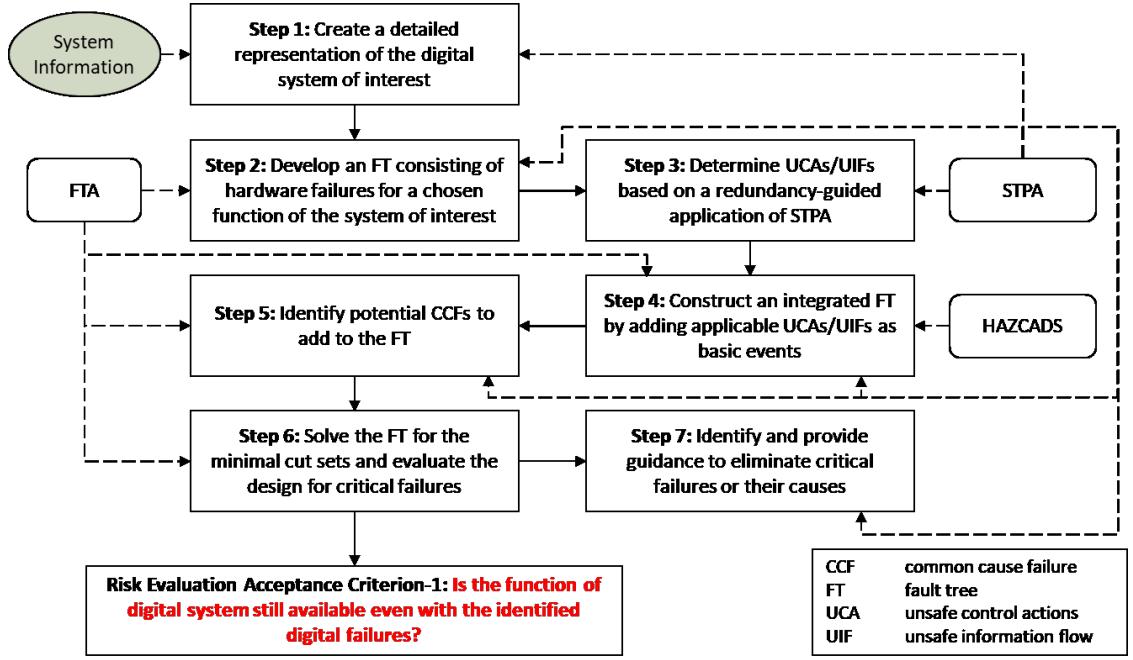
LWRS-developed DI&C Risk Assessment Framework

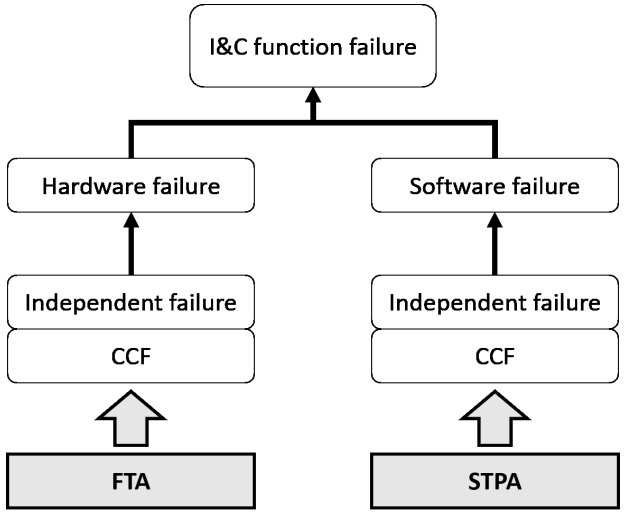


Redundancy-guided System-theoretic Hazard Analysis (RESHA)

Hazard analysis in the LWRS-developed framework:

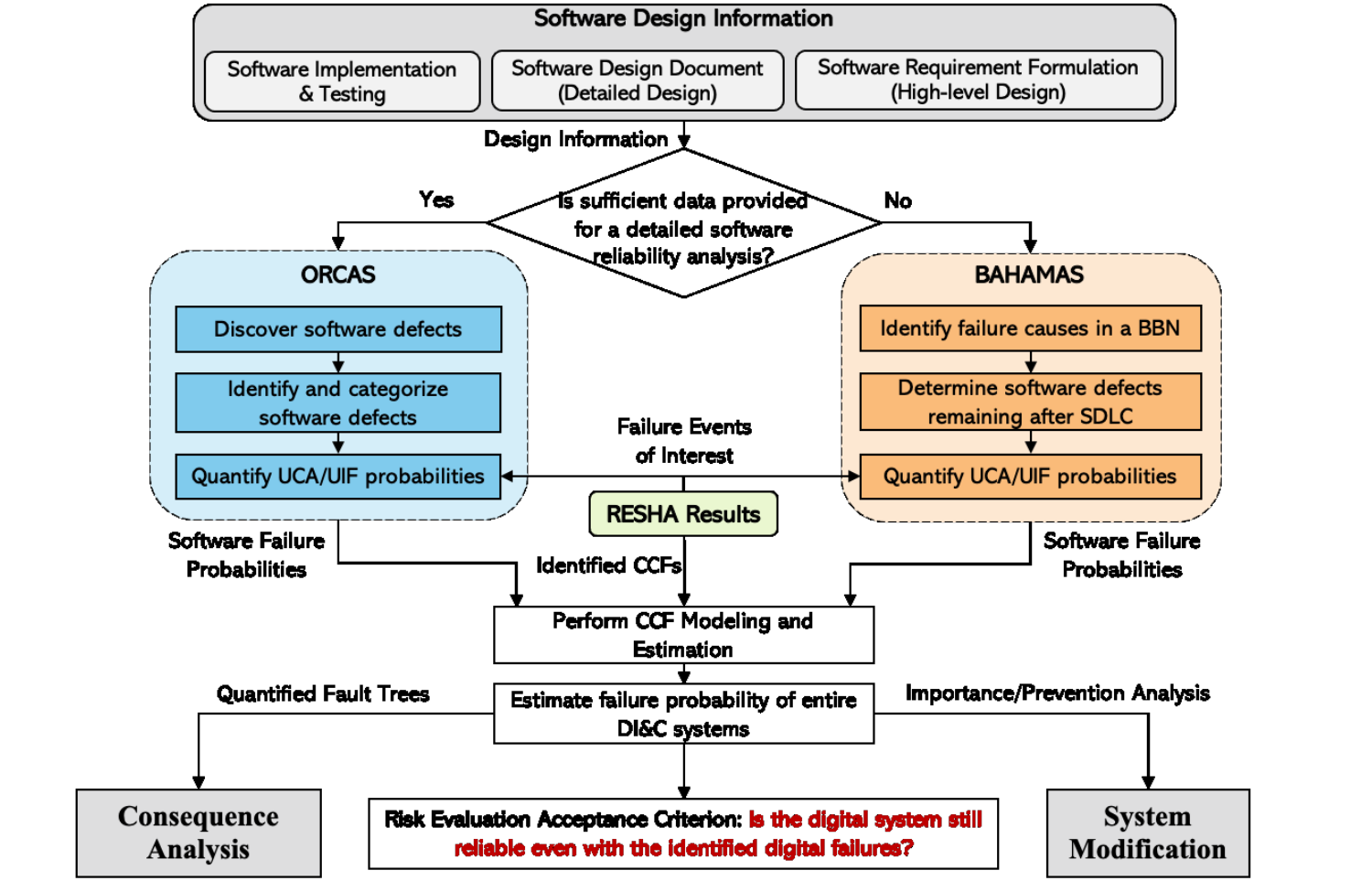
- Incorporates the concept of combining FTA and STPA from HAZCADS.
- Reframes STPA in a redundancy-guided way to identify various CCFs in highly redundant DI&C systems.
- Identifies and traces failures in both the actuation and information feedback pathway of DI&C systems due to unintended latent design or implementation defects or intended cyber attacks.





Workflow of the Redundant-guided System-theoretic Hazard Analysis (RESHA)

Multiscale Quantitative Reliability Analysis



BAHAMAS	Bayesian and human-reliability-analysis-aided method for the reliability analysis of software	CCF	common cause failure	RESHA	redundancy-guided systems-theoretic method for hazard analysis
		ORCAS	orthogonal-defect classification for assessing software reliability	SDLC	software development life cycle

Major Accomplishments in FY-23

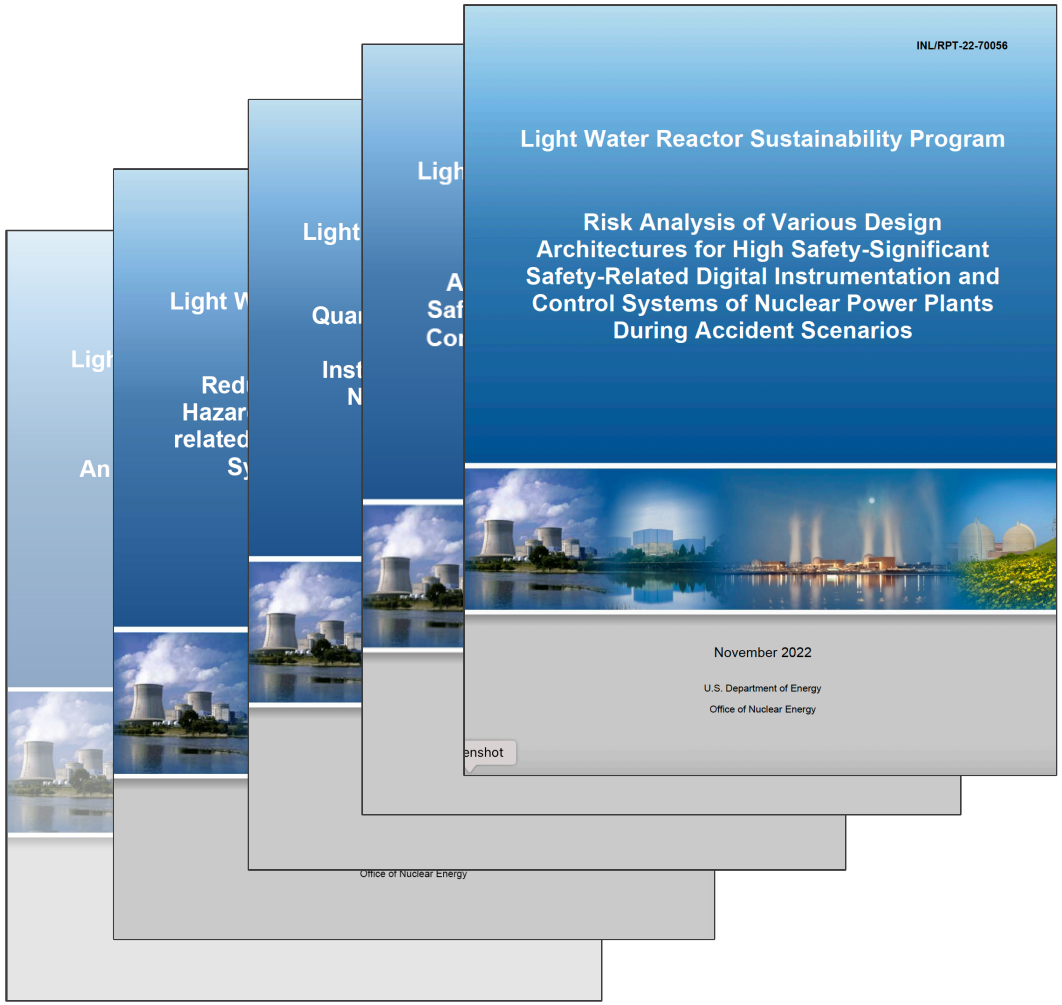
- Completed an industry peer review with reviewers from the *NRC, GEH, EPRI, and RPI*.
  - Feedbacks are positive pointing that framework addresses industry needs and closes gaps in the current state of practice.
  - Constructive suggestions are offered for methodology advancement and maturation, and integration with other toolsets (i.e., EPRI's framework) to gain the most benefits for the industry.
  - Delivered a peer review report in March 2023.

- Completed the reliability analysis of a safety-related DI&C system in collaboration with *PWROG*.
  - Feedback provided by the industrial collaborators for methodology refinement in FY-24.
  - Delivered a technical report in February 2023.

- Improved the current methods for identifying, quantifying, and evaluating potential software CCFs in highly redundant and diverse safety-related DI&C systems in collaboration with university partners.
  - Will deliver a technical report in September 2023.

Publications

- Published 6 journal articles, 7 milestone technical reports, 15 conference papers.



Research Activities in FY-24

- Improve and further develop the current framework and methods for risk assessment of multi-function DI&C systems in collaboration with the industry *(e.g., GE Hitachi)*.
- Refine the current methods to (1) keep supporting the need of DI&C reliability analysis from the industry *(e.g., PWROG);* (2) align better with international standards and existing risk-informed approaches and guides *(e.g., EPRI)*.
- Develop capabilities on risk-informed evidence generation and evaluation to support DI&C safety assurance and design optimization with the industry and other research institutions *(e.g., Halden and KAERI)*.
- Develop novel approaches to inform risk management and design optimization of advanced (semi-) autonomous DI&C systems designed for existing LWR fleets. *(with NCSU and KAERI)*

Collaborations

- **Industry:**
  - PWROG: DI&C reliability analysis and CCF evaluation
  - GE Hitachi: Risk assessment of multi-function DI&C platforms
  - Halden: DI&C hazard analysis and safety assurance

- **Universities (for new methodology exploration):**
  - University of Pittsburgh: Modeling and estimation of software CCF in safety-related DI&C systems.
  - North Carolina State University:
    - Development of a risk assessment framework for AI-aided control system designs
    - Software CCF modeling using model-based approaches.
  - Ohio State University: Software CCF modeling using dynamic methodologies.

Sustaining National Nuclear Assets

lwrs.inl.gov