LWRS LIGHT WATER REACTOR SUSTAINABILITY

NRC Public Meeting
February 15, 2022

LWRS Program Research on Common Cause Failure Analysis, Safety Evaluation and Design Optimization of Safety-Related Digital I&C Systems

Han Bao

Principal Investigator of Project "Digital I&C Risk Assessment"

U.S. DOE Light Water Reactor Sustainability Program, Risk-Informed Systems Analysis Pathway

han.bao@inl.gov

Idaho National Laboratory

02/15/2022

Light Water Reactor Sustainability (LWRS) Program

LWRS Goal

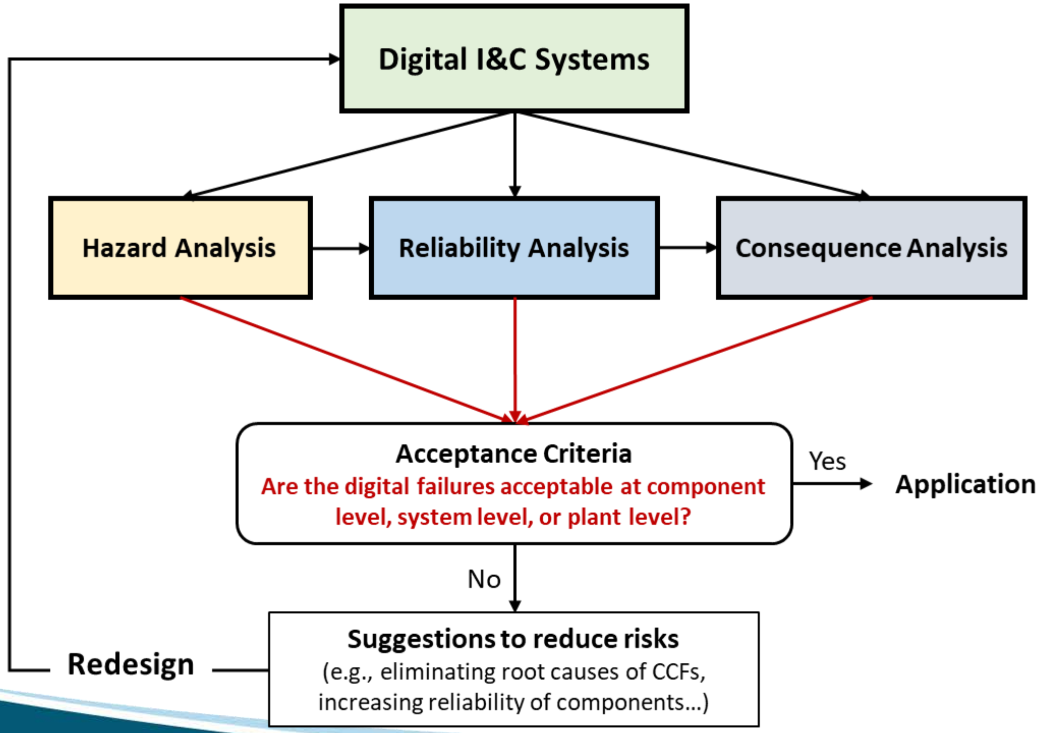
Enhance the safe, efficient, and economical performance of our nation's nuclear fleet and extend the operating lifetimes of this reliable source of electricity

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

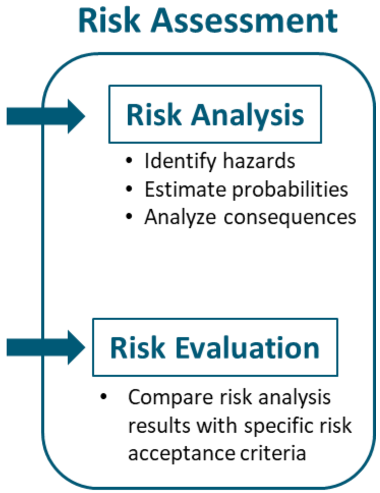
DIVERSIFY REVENUE
REDUCE COSTS
Enhance Economic Competitiveness
MANAGE AGING MATERIALS
ADDRESS TECHNOLOGY OBSOLESCENCE
Ensure Performance of Structures, Systems, Components
21-50005-02

Integrated Risk Assessment for Digital I&C Systems (IRADIC) - Framework

- **Goals of RISA Efforts on Digital I&C (DI&C) Risk Assessment:**
  - Develop an advanced risk assessment framework to support industry's transition from analog to digital technologies for safety-related I&C systems
  - Develop an integrated platform that includes all aspects of a typical risk assessment: hazard analysis, reliability analysis, and consequence analysis
  - Provide a systematic, verifiable and reproducible approach based on technically-sound methodologies



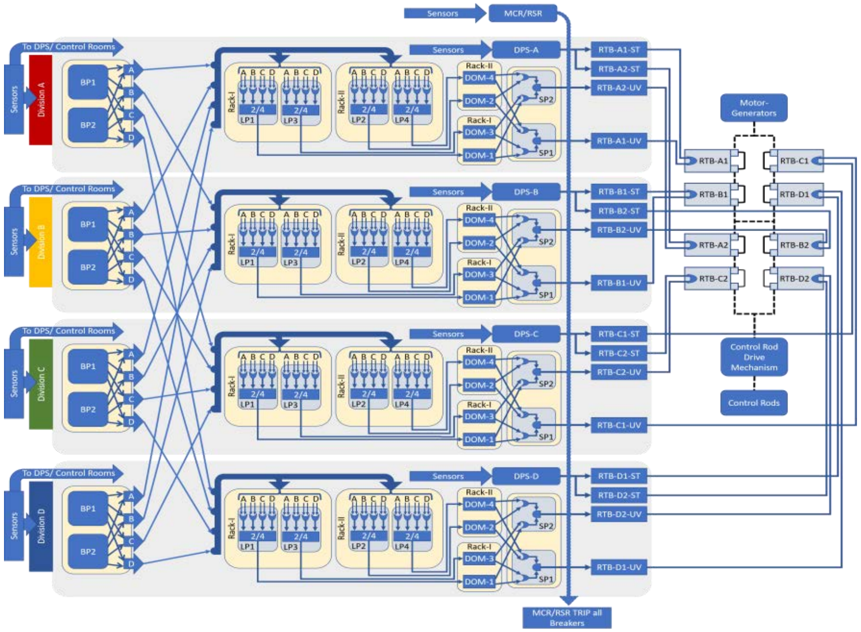
Digital I&C Systems
Hazard Analysis
Reliability Analysis
Consequence Analysis
Acceptance Criteria
Are the digital failures acceptable at component level, system level, or plant level?
Yes
Application
No
Suggestions to reduce risks
(e.g., eliminating root causes of CCFs, increasing reliability of components…)
Redesign



IRADIC Framework (continued)

- **IRADIC** is envisioned and developed as **an integrated risk-informed tool** to support the nuclear industry in addressing regulatory requirements in DI&C system implementation.

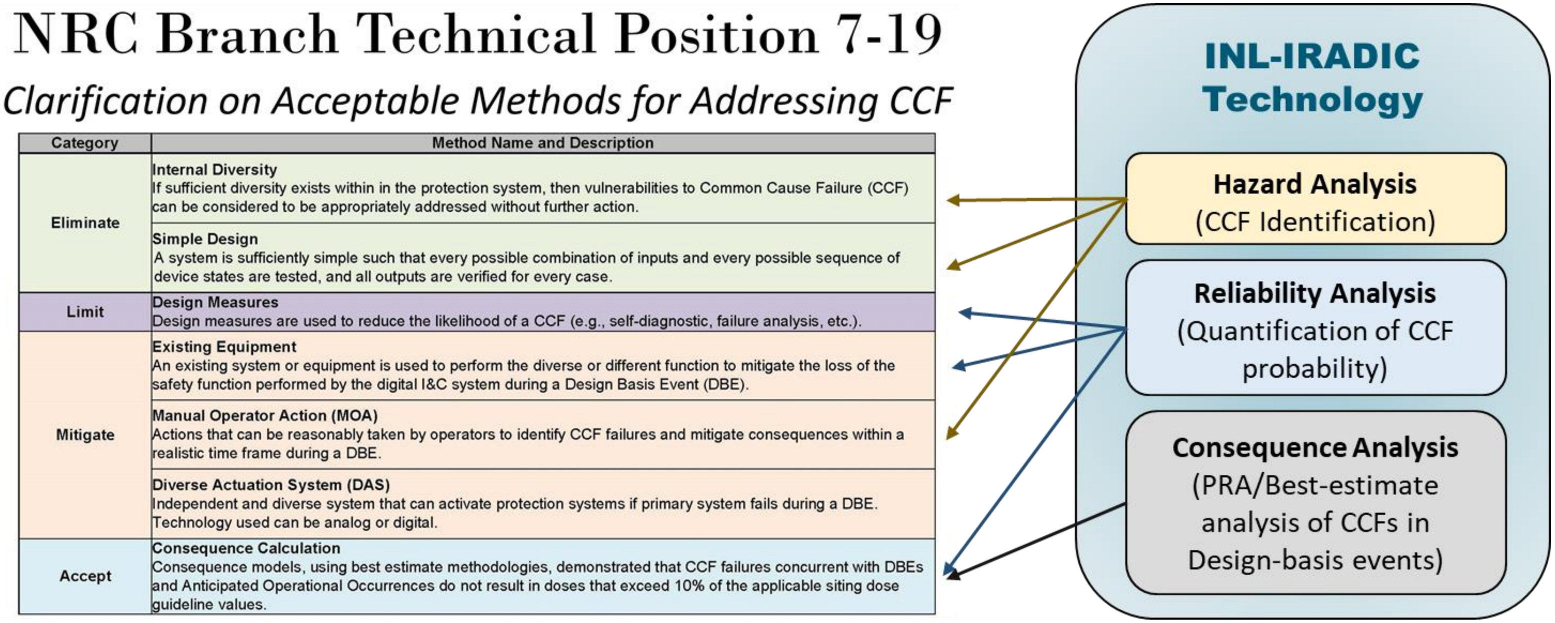
  - **Quantitative Risk Analysis**
    - Software and Hardware Failure Probabilities → DI&C System Failure Probability → ∆CDF / ∆LERF
  - **Risk-Informed Design**
    - Management strategy of CCFs
      - All elimination vs. selective elimination
    - Level of redundancy
      - 4 divisions vs. 2 divisions
      - 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

Addressing CCF Considerations

- **IRADIC** is expected to provide technical bases and risk-informed insights for **addressing CCF considerations** for safety-significant DI&C systems.



NRC Branch Technical Position 7-19

Clarification on Acceptable Methods for Addressing CCF

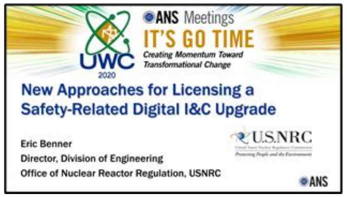
Category	Method Name and Description
Eliminate	**Internal Diversity** If sufficient diversity exists within in the protection system, then vulnerabilities to Common Cause Failure (CCF) can be considered to be appropriately addressed without further action.
	Simple Design A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case.
Limit	**Design Measures** Design measures are used to reduce the likelihood of a CCF (e.g., self-diagnostic, failure analysis, etc.).
Mitigate	**Existing Equipment** An existing system or equipment is used to perform the diverse or different function to mitigate the loss of the safety function performed by the digital I&C system during a Design Basis Event (DBE).
	Manual Operator Action (MOA) Actions that can be reasonably taken by operators to identify CCF failures and mitigate consequences within a realistic time frame during a DBE.
	Diverse Actuation System (DAS) Independent and diverse system that can activate protection systems if primary system fails during a DBE. Technology used can be analog or digital.
Accept	**Consequence Calculation** Consequence models, using best estimate methodologies, demonstrated that CCF failures concurrent with DBEs and Anticipated Operational Occurrences do not result in doses that exceed 10% of the applicable siting dose guideline values.

INL-IRADIC Technology

Hazard Analysis
(CCF Identification)

Reliability Analysis
(Quantification of CCF probability)

Consequence Analysis
(PRA/Best-estimate analysis of CCFs in Design-basis events)



ANS Meetings
IT'S GO TIME
Creating Momentum Toward Transformational Change
UWC 2020

New Approaches for Licensing a Safety-Related Digital I&C Upgrade

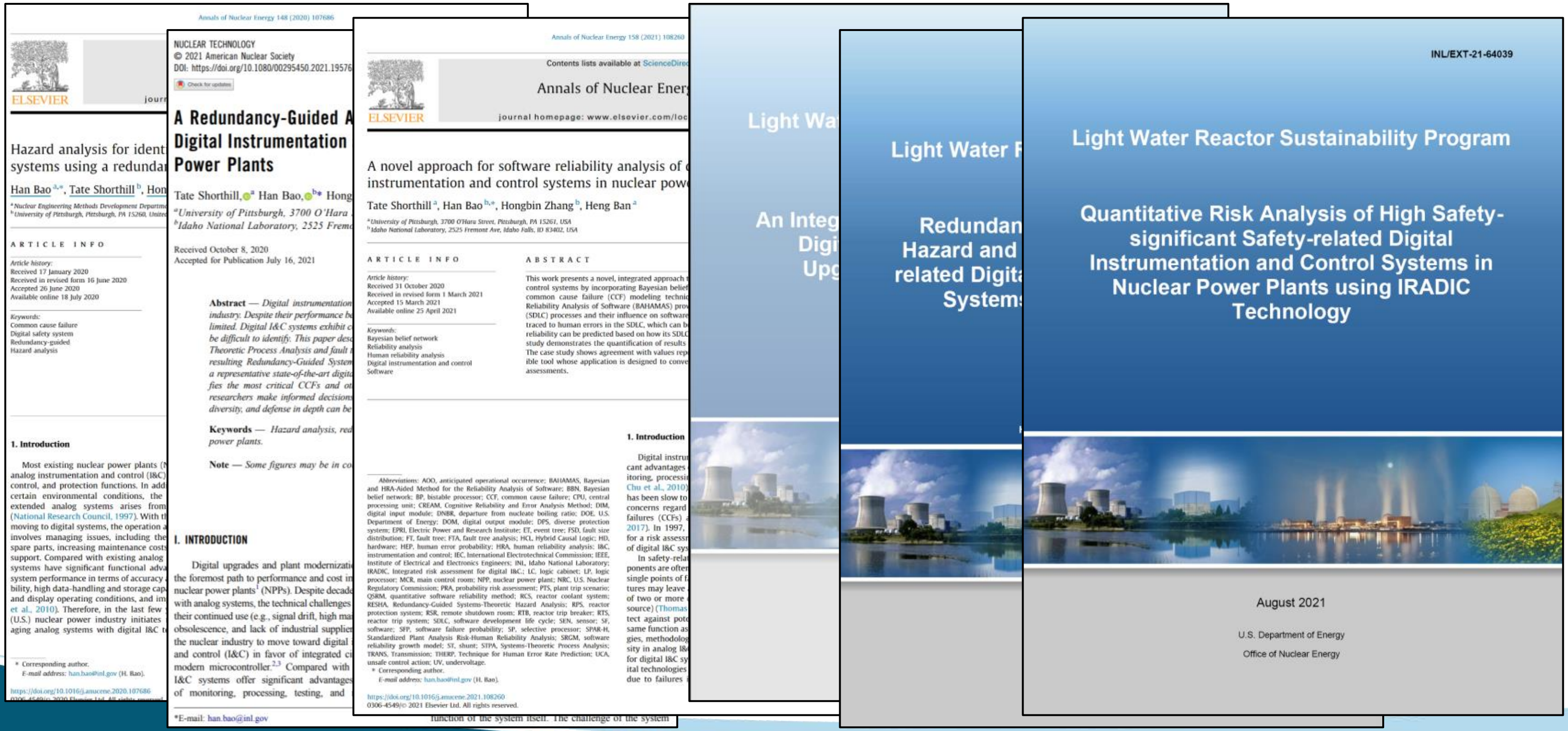
Eric Benner
Director, Division of Engineering
Office of Nuclear Reactor Regulation, USNRC

U.S.NRC
ANS

LWRS LIGHT WATER REACTOR SUSTAINABILITY

IRADIC: Current Status

- Collaborating with universities (e.g., NCSU) to develop **risk assessment framework for AI-guided control system designs** (e.g., identification of new CCF modes).
- Building capability to address **cyber vulnerabilities** (e.g., cyber-attacks leading to CCFs) in digital systems and networks.
- **Publications:** 3 journal articles, 3 milestone reports, 6 conference papers.



Annals of Nuclear Energy 148 (2020) 107686

Hazard analysis for ident… systems using a redundan…

Han Bao, Tate Shorthill, Hon…

NUCLEAR TECHNOLOGY
© 2021 American Nuclear Society
DOI: https://doi.org/10.1080/00295450.2021.19576…

A Redundancy-Guided A… Digital Instrumentation… Power Plants

Tate Shorthill, Han Bao, Hong…

Annals of Nuclear Energy 158 (2021) 108260

Annals of Nuclear Ener…

A novel approach for software reliability analysis of … instrumentation and control systems in nuclear pow…

Tate Shorthill, Han Bao, Hongbin Zhang, Heng Ban

Light Wa…

An Integ… Digi… Upg…

Light Water R…

Redundan… Hazard and… related Digit… System…

INL/EXT-21-64039

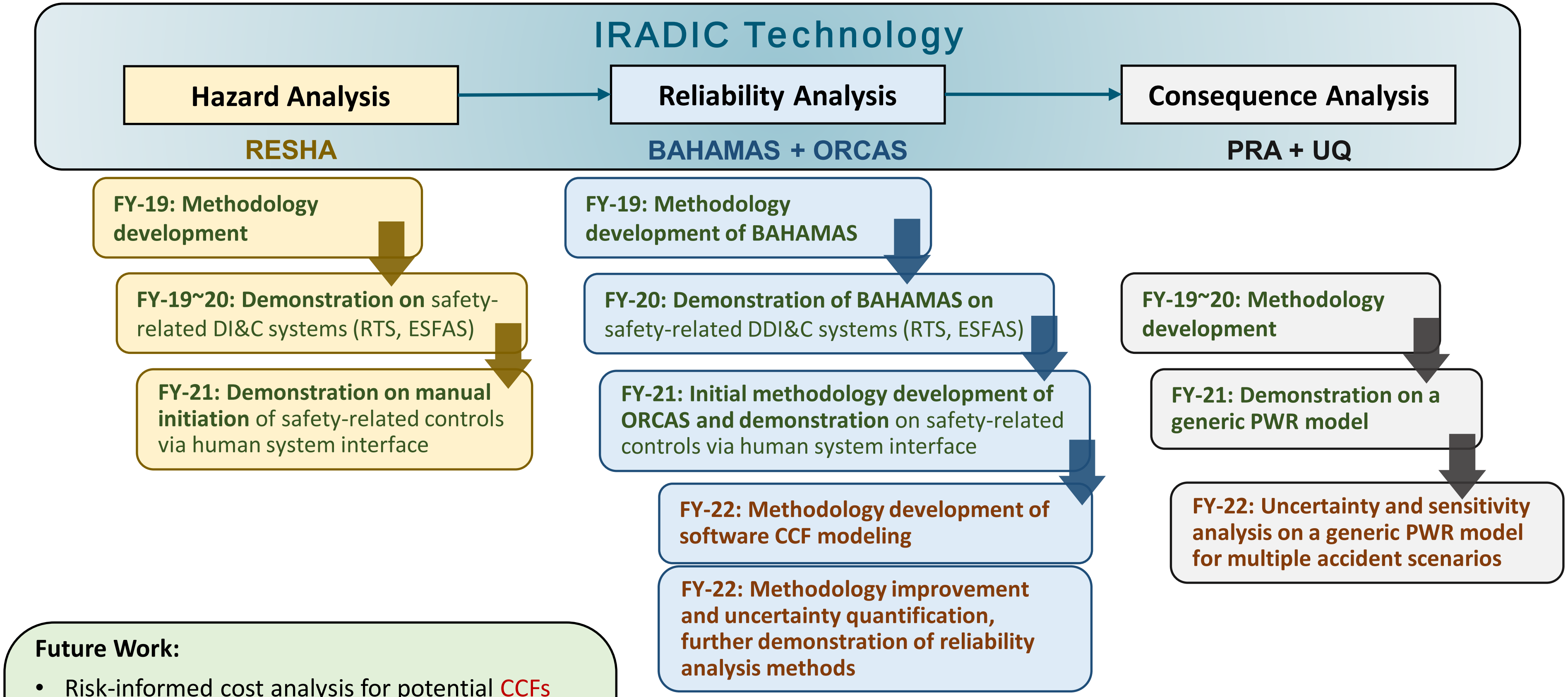
Light Water Reactor Sustainability Program

Quantitative Risk Analysis of High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants using IRADIC Technology

August 2021

U.S. Department of Energy
Office of Nuclear Energy

IRADIC Development Timeline



IRADIC Technology

Hazard Analysis → Reliability Analysis → Consequence Analysis

RESHA

FY-19: Methodology development

FY-19~20: Demonstration on safety-related DI&C systems (RTS, ESFAS)

FY-21: Demonstration on manual initiation of safety-related controls via human system interface

BAHAMAS + ORCAS

FY-19: Methodology development of BAHAMAS

FY-20: Demonstration of BAHAMAS on safety-related DDI&C systems (RTS, ESFAS)

FY-21: Initial methodology development of ORCAS and demonstration on safety-related controls via human system interface

FY-22: Methodology development of software CCF modeling

FY-22: Methodology improvement and uncertainty quantification, further demonstration of reliability analysis methods

PRA + UQ

FY-19~20: Methodology development

FY-21: Demonstration on a generic PWR model

FY-22: Uncertainty and sensitivity analysis on a generic PWR model for multiple accident scenarios

Future Work:

- Risk-informed cost analysis for potential CCFs
- Demonstration on optimization of D3 application
- Extension of IRADIC on risk assessment of new CCFs in AI-guided control systems
- Productization of IRADIC as a user-friendly software tool

RESHA: Redundancy-Guided Systemic Hazard Analysis

BAHAMAS: Bayesian and HRA-Aided Method for the Reliability Analysis of Software

ORCAS: Orthogonal Defect Classification for Assessing Software Reliability

Contacts

Han Bao

Principal Investigator

LWRS Program RISA Project "Digital I&C Risk Assessment"

Idaho National Laboratory

han.bao@inl.gov

Svetlana (Lana) Lawrence

LWRS Program RISA Pathway Lead

Idaho National Laboratory

svetlana.lawrence@inl.gov

Publications

JOURNAL PUBLICATION

- H. Bao, T. Shorthill, H. Zhang. “Hazard Analysis for Identifying Common Cause Failures of Digital Safety Systems using a Redundancy-Guided Systems-Theoretic Approach,” *Annals of Nuclear Energy*, 148, pp. 107686 (2020). DOI: 10.1016/j.anucene.2020.107686.
- T. Shorthill, H. Bao, H. Zhang, H. Ban. “A Novel Approach for Software Reliability Analysis of Digital Instrumentation and Control Systems in Nuclear Power Plants,” *Annals of Nuclear Energy*, 158, pp. 108260, (2021). DOI: 10.1016/j.anucene.2021.108260.
- T. Shorthill, H. Bao, H. Zhang, H. Ban. “A Redundancy-Guided Approach for the Hazard Analysis of Digital Instrumentation and Control Systems in Advanced Nuclear Power Plants,” *Nuclear Technology* (2021). DOI: 10.1080/00295450.2021.1957659.

TECHNICAL REPORT

- H. Bao, T. Shorthill, E. Chen, H. Zhang, “Quantitative Risk Analysis of High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants using IRADIC Technology,” INL/EXT-21-64039, Idaho National Laboratory, 2021. https://lwrs.inl.gov/RiskInformed%20Safety%20Margin%20Characterization/Quantitative_Risk_Analysis_High_Safety.pdf.
- H. Bao, T. Shorthill, H. Zhang, “Redundancy-guided System-theoretic Hazard and Reliability Analysis of Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants,” INL/EXT-20-59550, Idaho National Laboratory, 2020. https://www.osti.gov/biblio/1668835.
- H. Bao, H. Zhang, K. Thomas. “An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants,” Technical milestone report, INL/EXT-19-55219, Idaho National Laboratory, 2019. https://doi.org/10.2172/1616252.

CONFERENCE PAPER / PRESENTATION

- H. Bao, H. Zhang, T. Shorthill, E. Chen. “Common Cause Failure Evaluation of High Safety-significant Safety-related Digital Instrumentation and Control Systems using IRADIC Technology”, *16th Probabilistic Safety Assessment & Management conference* (*PSAM 16)*, Honolulu, HI, June 26 – July 1, 2022.
- T. Shorthill, H. Bao, H. Zhang and H. Ban. “A Bayesian and HRA-Aided Method for the Novel Reliability Analysis of Software”, *The 2021 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2021)*, Columbus, OH, November 07-12, 2021.
- E. Chen, H. Bao, H. Zhang, T. Shorthill. “Systems-theoretic Hazard Analysis of Human-machine Interface for Digital Reactor Trip System”, *12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021)*, Providence, RI, June 13-16, 2021.
- H. Zhang, H. Bao, T. Shorthill, E. Quinn. “Integrated Risk Assessment of Digital I&C Safety Systems for Nuclear Power Plants”, *12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021)*, Providence, RI, June 13-16, 2021.
- H. Bao, T. Shorthill, H. Zhang. “Hazard Analysis of Digital Engineered Safety Features Actuation System in Advanced Nuclear Power Plants using a Redundancy-guided Approach”, *28th International Conference on Nuclear Engineering (ICONE28)*, Anaheim, CA, August 2-6, 2020.
- T. Shorthill, H. Bao, H. Zhang and H. Ban. "Demonstration of Integrated Hazard Analysis for Reactor Trip Systems”, *ANS Winter Meeting*, Washington D.C., November 17-20, 2019.

LWRS

LIGHT WATER
REACTOR
SUSTAINABILITY

Sustaining National Nuclear Assets

http://lwrs.inl.gov