INL/MIS-21-63094-Revision-0

Systems-Theoretic Hazard Analysis of Digital Human-System Interface Relevant to Reactor Trip

April 2023

Edward Chen, Han Bao, Hongbin Zhang, Tate Shorthill

Changing the World's Energy Future

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

INL/MIS-21-63094-Revision-0

Systems-Theoretic Hazard Analysis of Digital Human-System Interface Relevant to Reactor Trip

Edward Chen, Han Bao, Hongbin Zhang, Tate Shorthill

April 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

ANS Virtual Annual Meeting
EMBEDDED TOPICAL
NPIC HMIT 2021

Systems-Theoretic Hazard Analysis of Digital Human-System Interface Relevant to Reactor Trip

Edward Chen[1]
Dr. Han Bao[2] & Dr. Hongbin Zhang[2]
Tate Shorthill[3]
Dr. Nam Dinh[1]

[1]North Carolina State University
[2]Idaho National Laboratory
[3]University of Pittsburgh

Problem Scope

1. Qualification of modern safety control and protection is still difficult, especially with novel digital instrumentation & control (I&C) systems

2. Redundant systems use similar design where both digital hardware and software are less diverse (i.e., less redundant defense-in-depth measure)

3. Existing methods, such as Hazard & Consequence Analysis for Digital Systems (HAZCADS) and Systems-Theoretic Process Analysis (STPA) lack the explicit ability to address common-cause failures (CCFs) across different redundant systems

<u>Objective</u>

A. Help system designers & engineers address digital-based CCFs and qualitatively analyze system vulnerabilities

B. Upgrade existing methods to incorporate the complex safety redundancies in digital plant I&C

ANS

Prior Supporting Work

- Systems Theoretic Process Analysis (STPA)
  - Evaluates and describes undesirable outcomes resultant of inadequate constraints enforcement

  N.G. Leveson et al. “STPA Handbook” MIT Partnership for Systems Approaches to Safety and Security, (2018)

- Hazard & Consequence Analysis for Digital Systems (HAZCADS)
  - Systematically identifies emergent & complex I&C failures – Systematic failure modes

  A.J. Clark et al., “Hazards and Consequences Analysis for Digital Systems.” EPRI, Palo Alto, CA (2018): 3002012755.

- **REdundancy-guided Systems Theoretic Hazard Analysis (RESHA)**
  - Aims to qualitatively identify and analyze effects of digital-based common-cause failures in highly redundant safety systems

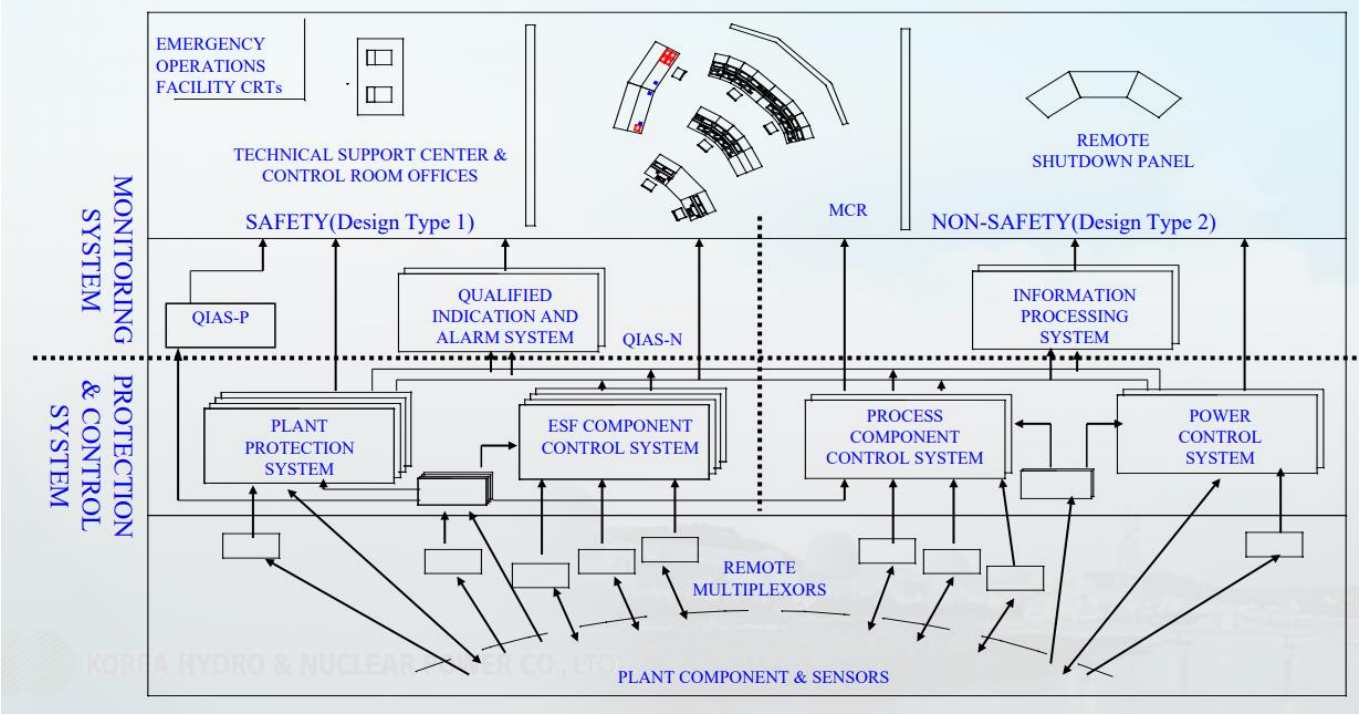
  H. Bao et al. “Hazard analysis for identifying common cause failures of digital safety systems using a redundancy-guided systems-theoretic approach” Annals of Nuclear Energy, 148 (2020), 107686

Scope of Analysis – Advanced Power Reactor 1400

- Safety monitoring system includes multiple redundancies:
  - **(QIAS-P) Qualified Indication and Alarm System – Safety Relevant**
  - (QIAS-N) Qualified Indication and Alarm System – Non-Safety Relevant
  - (IPS) Information Processing System
  - (DIS) Diverse Indication System

- QIAS-P
  - Advanced monitoring, alarm, and early indication system
    - Inadequate core cooling
    - Reactor coolant saturation margin
  - Separated into two redundant independent module level divisions

- Analyze how redundancies in the digital & analog components of the QIAS-P system affect reliability



Lee, M. S. et al. "Development of human factors validation system for the advanced control room of APR1400." Journal of Nuclear Science and Technology, 46, 1, pp. 90-101. (2009).

Basics of Hazard Analysis & RESHA

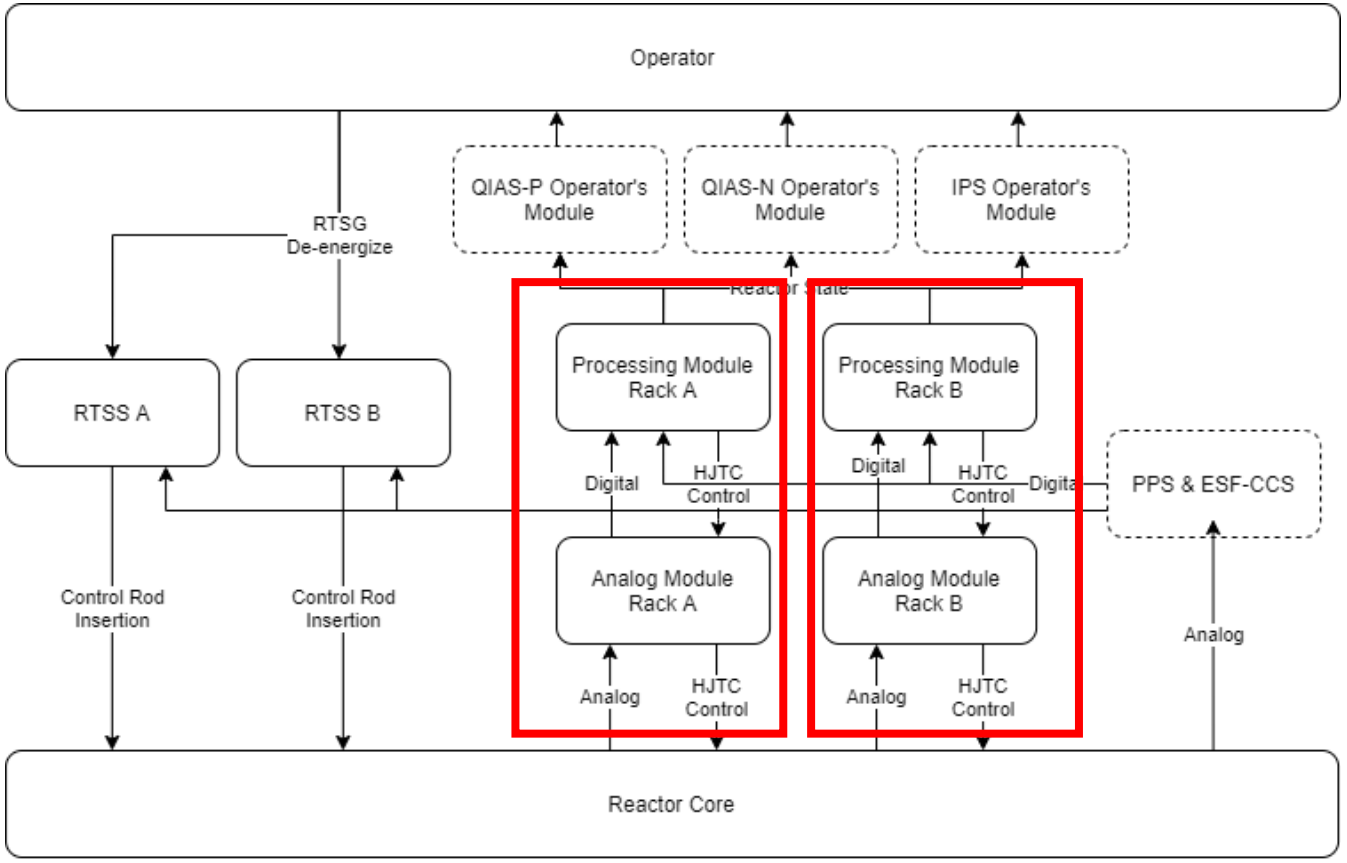
1. Identify control flow diagram and scope of analysis
2. Create hardware fault tree (FT) based on control diagram
3. Apply STPA to control diagram to identify software basic events
   a) Identify Losses & Hazards
   b) Identify unsafe control actions & unsafe information flow interactions between digital components
4. Integrate STPA identified software basic into hardware FT
5. Identify common-cause failures among redundant systems from integrated FT
6. Determine minimal cut sets to discover potential single points of failure and triggers

ANS

Control Flow Diagram

- QIAS-P
  - Advanced monitoring, alarm, and early indication system
    - Inadequate core cooling
    - Reactor coolant saturation margin
  - Instrumentation & alarm reading alert the operator for **manual** reactor trip

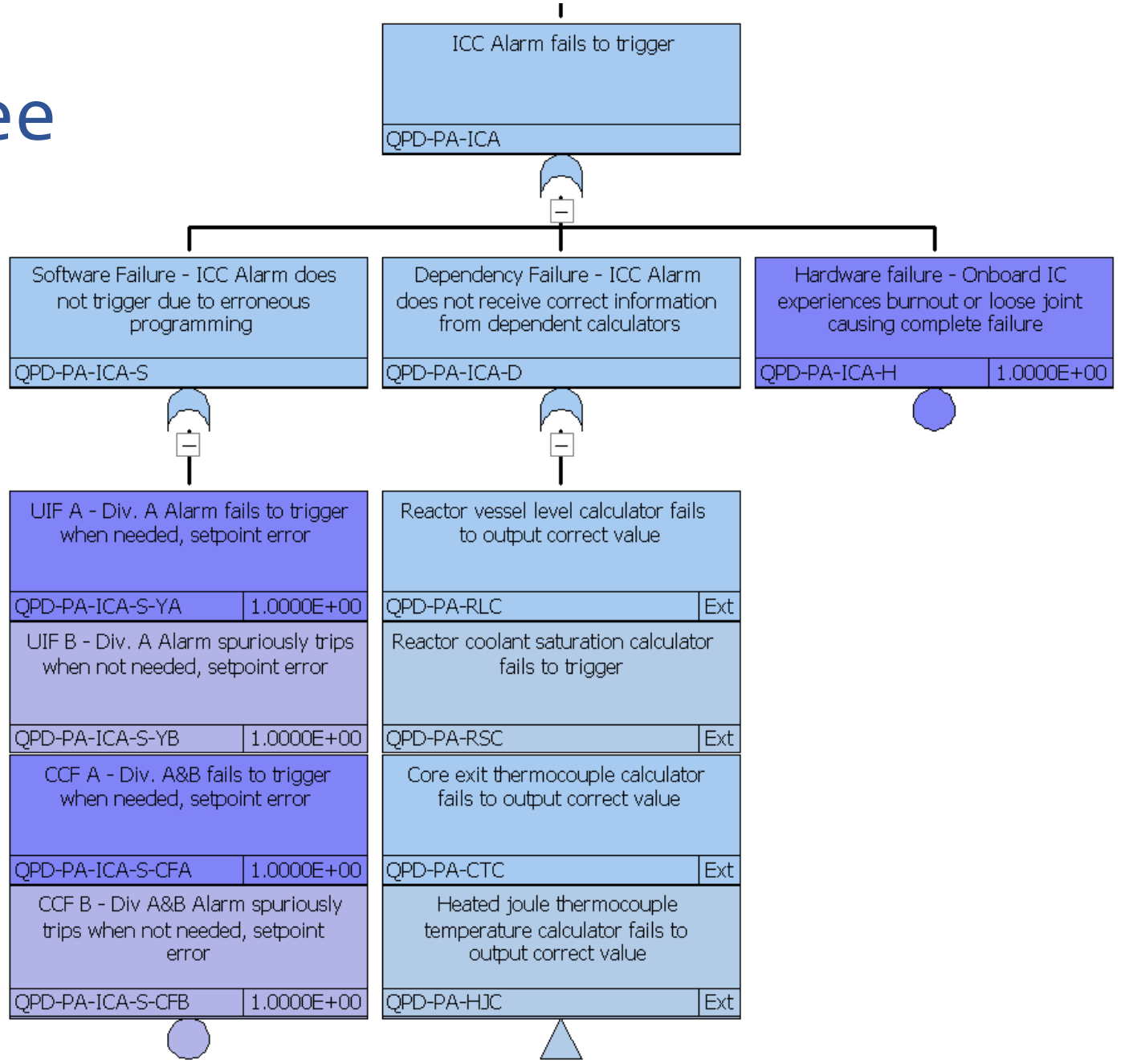
- Separated into two redundant & independent module level divisions
  - Each division has an analog and a digital module receiving sensor information throughout the plant
  - Documentation suggests no hardware diversity between two divisions



Integrated Fault Tree

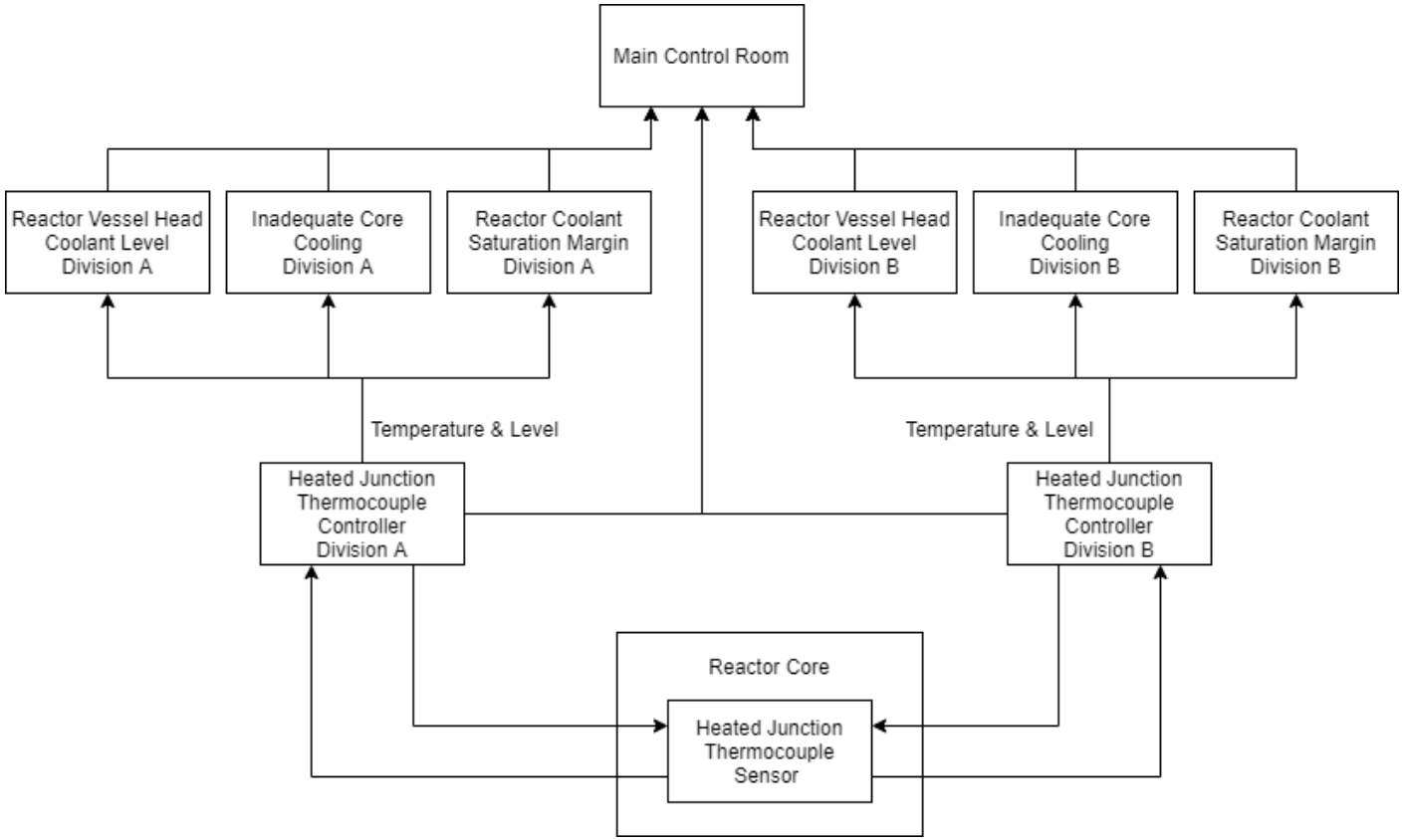
- Three Branches to Top Event
  - Software failures
  - Dependency / interface failures
  - Hardware failures
- Possible software failure modes
  - Alarm fails to trigger when needed
  - Alarm trips spuriously when not needed
  - Division A&B alarm fails to trigger when needed (CCF)
  - Division A&B alarm trips spuriously when not needed (CCF)
- Possible dependency issues
  - 1/4 dependent readings not received by ICC* Alarm module, alarm fails to trip

*Inadequate Core Cooling



Identified Potential Single Point of Failure Example

- Software failure of the division-level Heated Junction Thermocouple Controller
  - Programmed HJTC power level incorrect, no reference level provided to heated junction
  - Power control algorithm inadequate causing higher/lower reference levels to heated junction
- Software CCF
  - CCF of the reactor vessel head calculator and alarm
  - CCF of the inadequate core cooling calculator and alarm
  - CCF of the reactor coolant saturation margin calculator and alarm
  - Operator monitoring in MCR



Concluding Remarks

Major contributions of this work:

1. Further demonstration of software and hardware hazard identification using RESHA
2. Demonstration of CCF identification for human-machine interface systems for informed design

Primary results of this work:

1. Identification of different division and module basic events and CCFs:
   a) i.e., # of division-level software CCFs: 28 (Assuming no design diversity among redundant QIAS-P divisions)
2. Creation of integrated fault tree with both software and hardware failures across redundant divisions

ANS