An Integrated Risk Assessment Strategy for DI&C Systems (IRADIC)

**Goals of RISA Efforts on DI&C Risk Assessment:**
- Provide a best-estimate, risk-informed capability to estimate quantitatively and accurately the safety margin obtained from plant digitalization, especially for the high safety-significant safety-related (HSSSR) DI&C systems
- Develop an advanced risk assessment strategy to support transition from analog to DI&C technologies
- Assure the long-term safety and reliability of vital safety-related DI&C systems
- Reduce uncertainty in costs and support integration of DI&C systems in the plant
Value Proposition for IRADIC Technology

- **IRADIC aims to provide a modularized platform** for I&C designers, software developers, plant engineers, and risk analysts to efficiently predict and prevent risk by:
  - **Identifying crucial failure modes** (including common cause failures [CCFs]) and system vulnerabilities
  - **Quantifying the reliability** of digital I&C systems with the identified digital failures
  - **Evaluating the impact of consequences** of digital failures on the plant responses.

**Designs of Digital I&C Systems and Plants**

**IRADIC Technology**

- **Hazard Analysis**
- **Reliability Analysis**
- **Consequence Analysis**

**RESHA**
(Redundancy-Guided Systemic Hazard Analysis)

**PRA/MP-BEPU**
(Multi-Physics Best-Estimate Plus Uncertainty)

**BAHAMAS**
(Bayesian and HRA-Aided Method for the Reliability Analysis of Software)

**ORCAS**
(Orthogonal Defect Classification for Assessing Software Reliability)

**Suggestions to optimize designs and upgrades by quantitatively reducing risks and costs**
How IRADIC Could Support Industry for Risk-Informing HSSSR DI&C Designs or Upgrades?

- IRADIC is expected to become an integrated risk-informed tool for vendors and utilities to meet the regulatory requirements and optimize the diversity and defense-in-depth (D3) applications in the DI&C designs and upgrades.

- IRADIC details the risk analyses of high safety-related and safety-significant (HSSSR) DI&C systems (A1) with an emphasis on potential CCFs.

Conceptual Framework for a Proposed Graded Approach for Assessing CCF and Defense-in-Depth (From Nuclear Regulatory Commission (NRC) public meeting for Modernization Plan #1D BTP 7-19 Update)

<table>
<thead>
<tr>
<th>Safety-Related</th>
<th>Non-Safety Related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety-Significant</td>
<td>A1</td>
</tr>
<tr>
<td>Significant contributor to plant safety</td>
<td>Analysis Needed: D3 Assessment</td>
</tr>
<tr>
<td>Non-Safety-Significant</td>
<td>A2</td>
</tr>
<tr>
<td>Not a significant contributor to plant safety</td>
<td>Analysis Needed: Qualitative Assessment</td>
</tr>
</tbody>
</table>

NRC Branch Technical Position 7-19

Risk-Informed Graded Approach

Allows leveraging of any available risk information and insights
How IRADIC Could Support the Licensing Process of HSSSR Digital I&C Upgrades?

- **IRADIC** is expected to provide:
  - Technical basis and risk-informed insights to assist NRC and industry in formalizing licensing processes relevant to **addressing CCF issues** in HSSSR DI&C systems.

## NRC Branch Technical Position 7-19

**Clarification on Acceptable Methods for Addressing CCF**

<table>
<thead>
<tr>
<th>Category</th>
<th>Method Name and Description</th>
</tr>
</thead>
</table>
| **Eliminate** | Internal Diversity  
If sufficient diversity exists within 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)
IRADIC Development Timeline and Status

**IRADIC Technology**

**Hazard Analysis**
- RESHA

**Reliability Analysis**
- BAHAMAS + ORCAS

**Consequence Analysis**
- PRA/LOTUS

**FY-19**: Methodology development
- BAHAMAS

**FY-19**: Methodology development of BAHAMAS

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

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

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

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

**FY-22**: Methodology development of software CCF modeling

**FY-22**: Methodology improvement and uncertainty quantification, further demonstration of ORCAS on HSI

**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 different accident scenarios

**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

**LOTUS**: The LOCA Toolkit for U.S. LWRs
JOURNAL PUBLICATION


CONFERENCE PAPER / PRESENTATION


TECHNICAL REPORT

Sustaining National Nuclear Assets

http://lwrs.inl.gov