

RISK-INFORMED, PERFORMANCE-BASED DESIGN APPROACHES FOR ENHANCED SAFETY AND RELIABILITY IN NEW NUCLEAR

PAUL AMICO | May 2025

Intro to Jensen Hughes

“Big” JH

*Helping the built environment focus on what matters most without compromising **safety, security or resilience***

- + Global risk engineering, regulation + code consulting, and specialty design firm
- + 1700+ engineers and technical consultants
- + Engineering solutions that drive operational excellence for full facility life cycle:
 - Existing Facilities
 - New Construction
 - Failure Analysis

+

Nuclear Power JH

Maximizing Generation with Risk-Informed, Performance-Based Solutions

Risk-Informed Services

- PRA and Applications (RICT, 50.69, STRIDE/SFCP, SDP, Security)

Programmatic Solutions

- Fire Protection Programs, Safe Shutdown, Security + Emergency Management

Specialty Design Engineering

- Mechanical, Structural, Electrical, and Failure Analysis/Forensics

AI + Advisr Software Suite

- ChatAdvisr™ (Agentic AI), RiskAdvisr™ (Fire Protection), DataAdvisr™ (AI-ML Automation for CAP/PRA), PDMS™ (Cable/Asset Mgmt)

Meeting the Needs of Off-takers

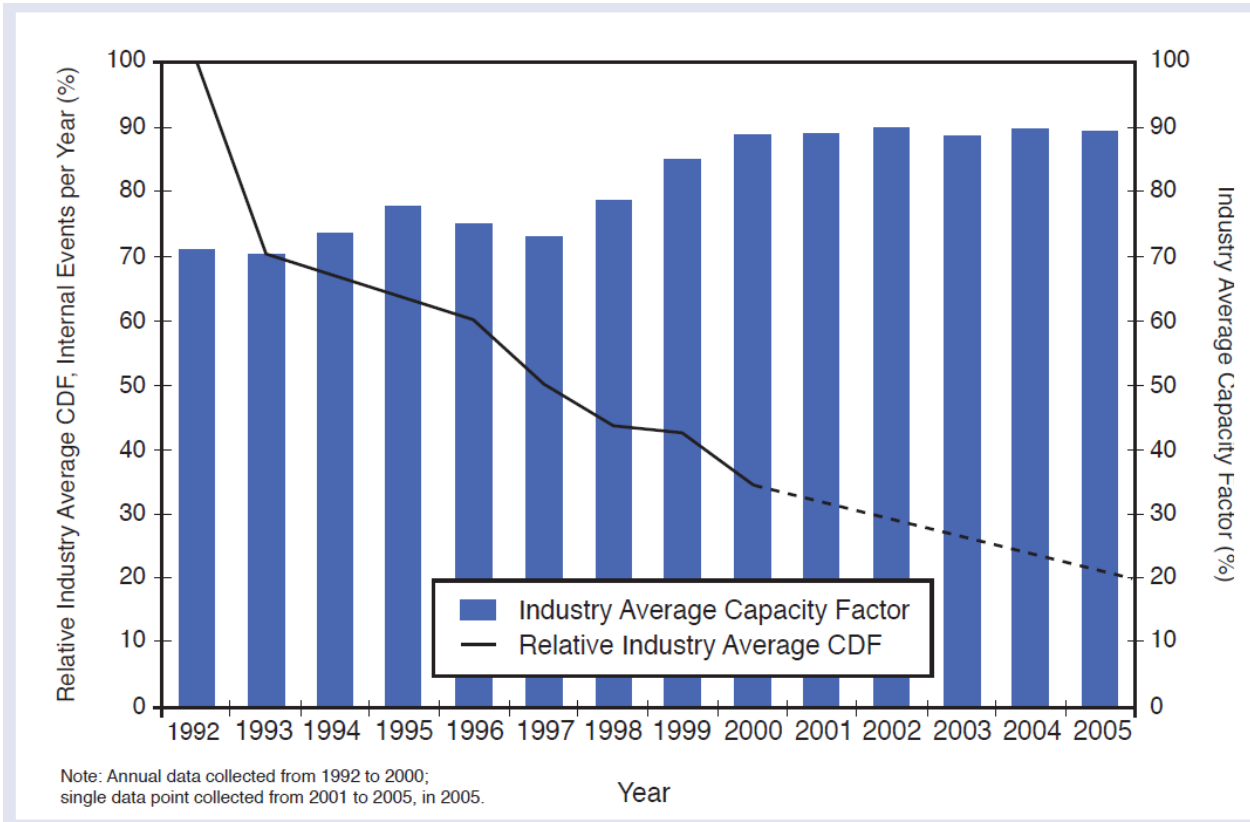
Energy Supply Needs to be RELIABLE

- + Industrial users want and need a reliable supply of energy.
- + Availability or capacity factor issues mean buying replacement power.
- + Replacement power can be quite expensive.
- + Even with no safety implications, asset damage is unacceptable.

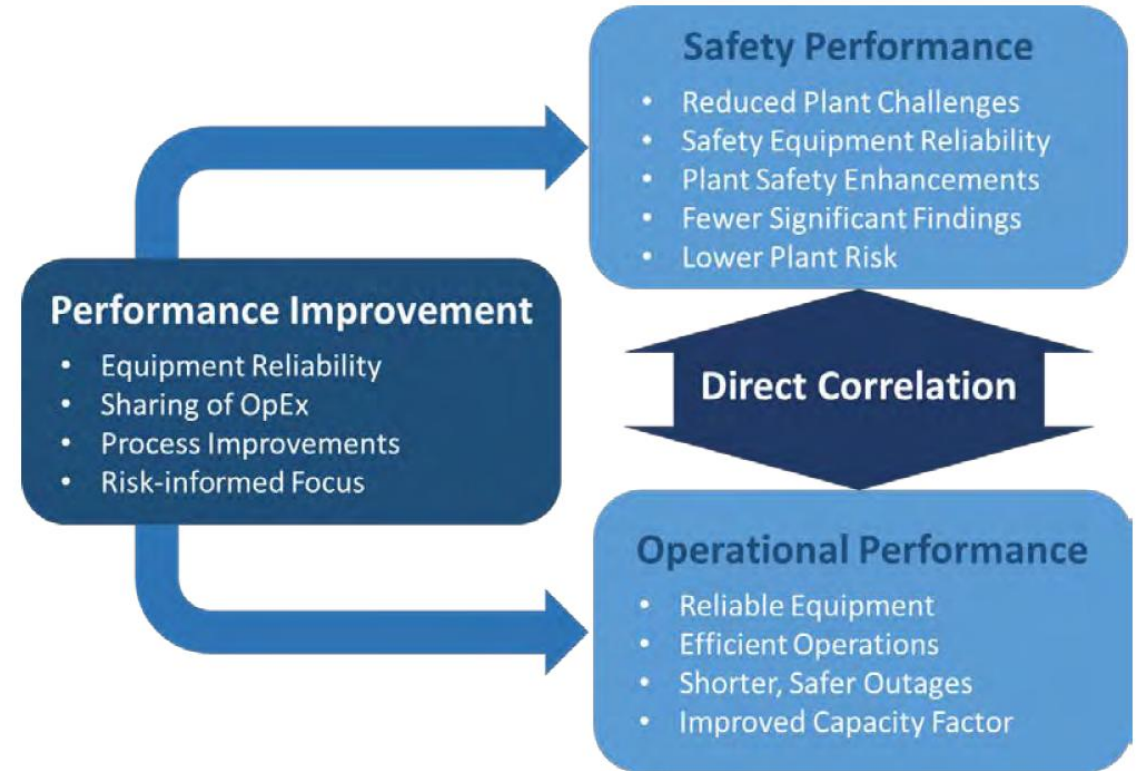
So, there is a balance that needs to be achieved that optimizes both safety goals and production goals, and the best way to do that is with a risk-informed, performance-based approach.

The Principle Behind Risk-informed Design

Safety and Economics are Mutually Reinforcing



From EPRI 1016308 Safety and Operational Benefits of Risk-Informed Initiatives



From NEI 20-04 The Nexus Between Safety and Operational Performance in the U.S. Nuclear Industry

Establishing the Performance Goals

Quantitative Performance Goals

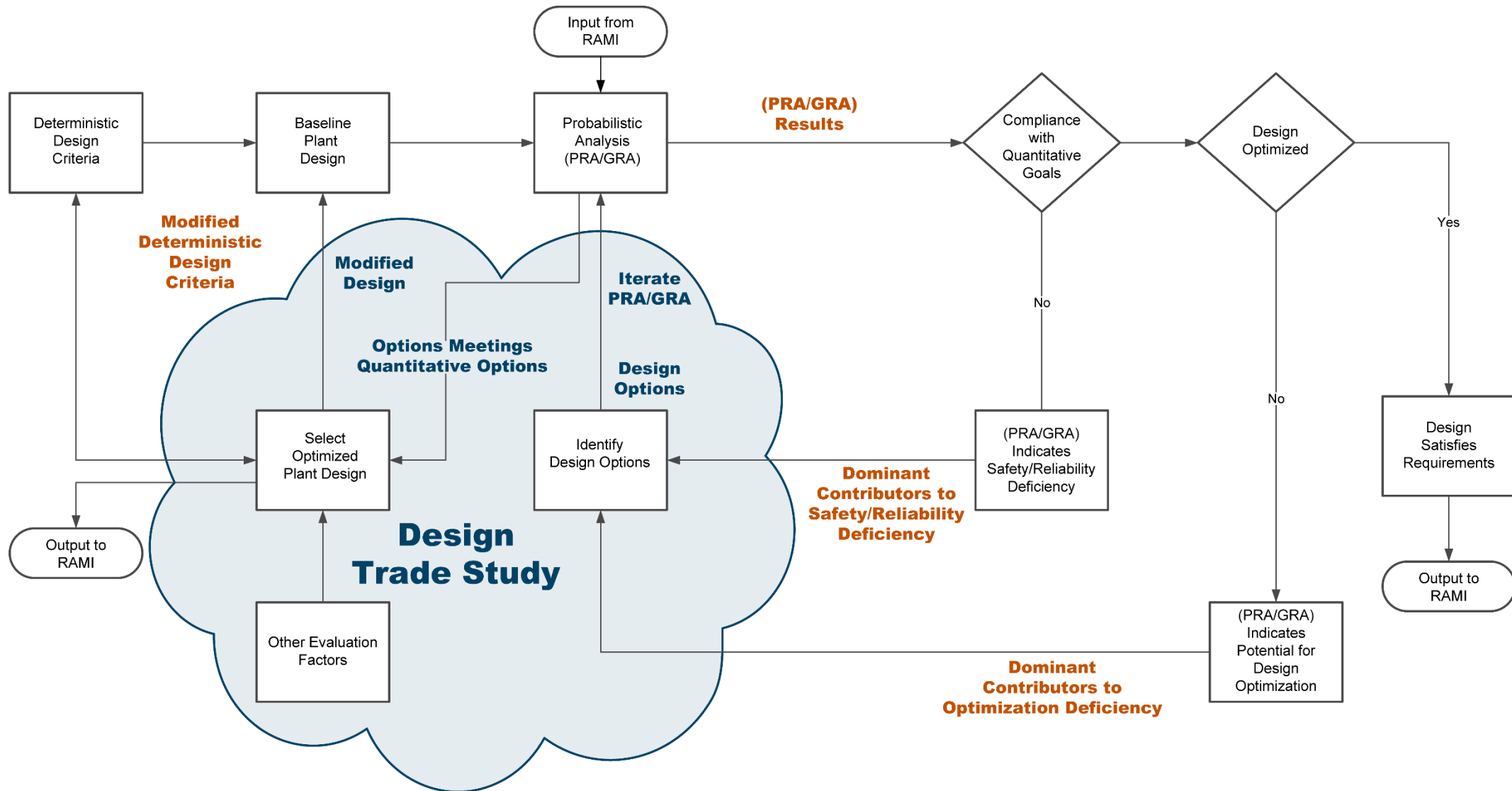
- + **Optimum performance of a nuclear power plant requires a balance between safety and productivity.**
- + **The starting point is to establish quantitative goals for both at the plant level:**
 - Core damage and large (or large early) release are typical safety performance goals
 - Availability factor and capacity factor are typical productivity performance goals
- + **To provide a match between the plant level goals and the design process, probabilistic risk assessment (PRA) and generation risk assessment (GRA) are used to allocate these goals at lower levels (e.g., function, system, component). The level of the goal will depend on the status of the design process.**
- + **Not all goals are quantitative. Qualitative safety and production goals have their place. Although they are qualitative, they are still considered probabilistic (i.e., risk-informed) goals.**

Establishing the Performance Goals

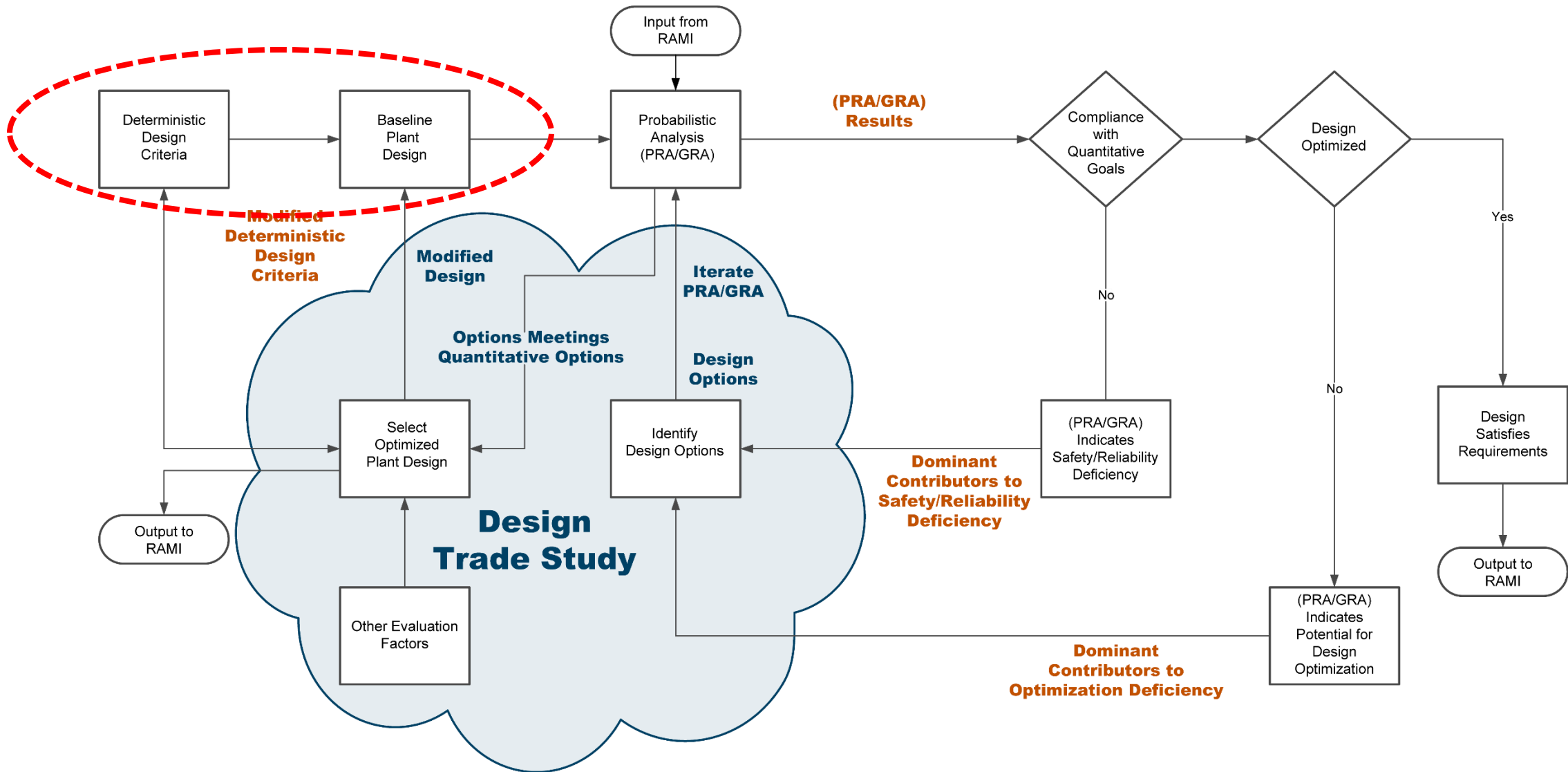
Qualitative Performance Goals

- + **Qualitative performance goals are related to specific functional or operational features that have proven an acceptable level of performance in the past. They must be:**
 - Clearly stated in an unambiguous manner;
 - Related to physical, functional, and administrative features of the design; and
 - Must be measurable and verifiable by inspection, testing, and/or analysis
- + **Most qualitative goals imply certain likelihoods of occurrence. Examples include:**
 - Single failure criterion;
 - Functional diversity requirements;
 - Alternate operating modes;
 - Physical separation;
 - Equipment redundancy; and
 - Functional backup.

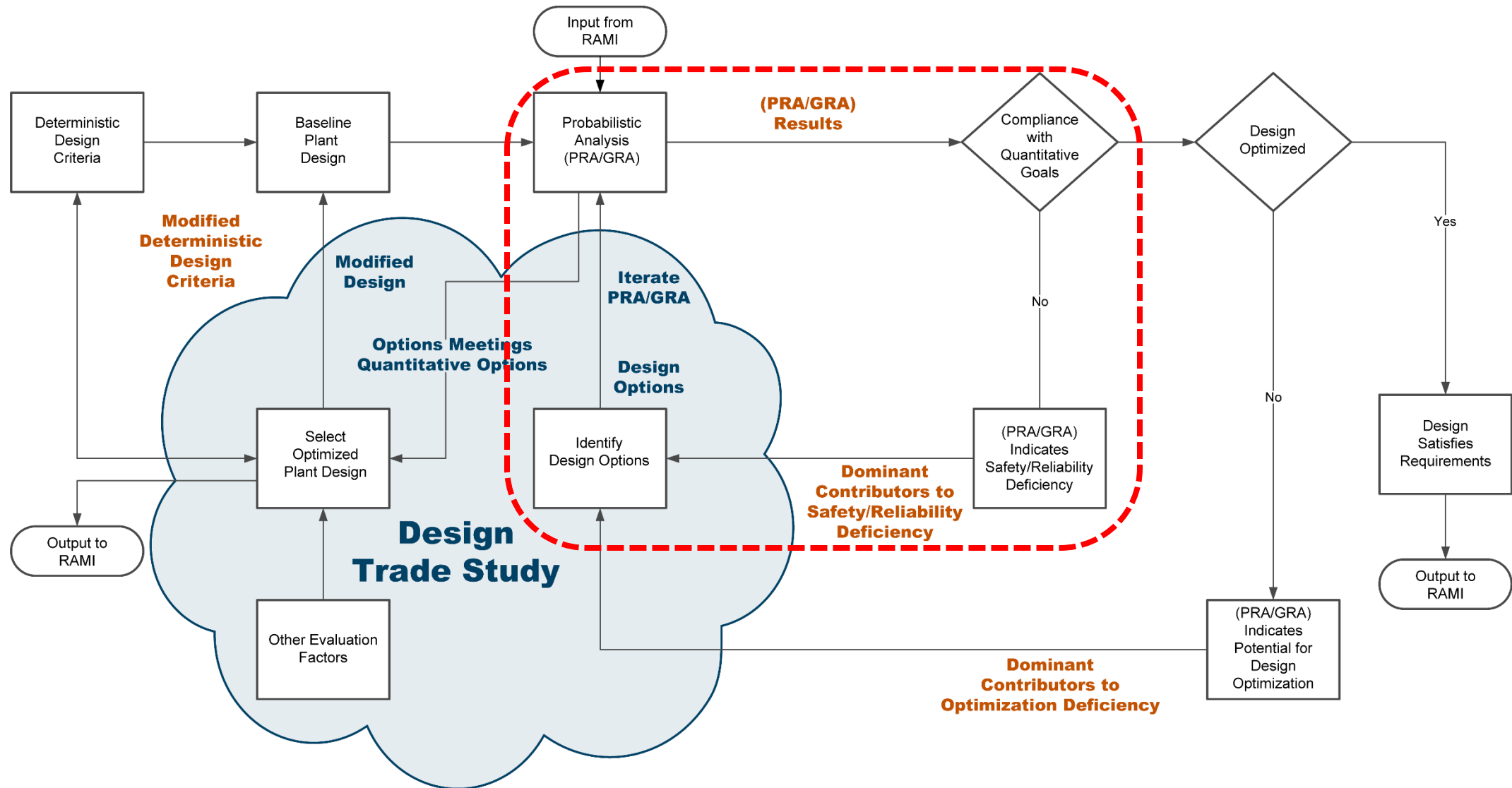
Process Flow for Risk-informed Design



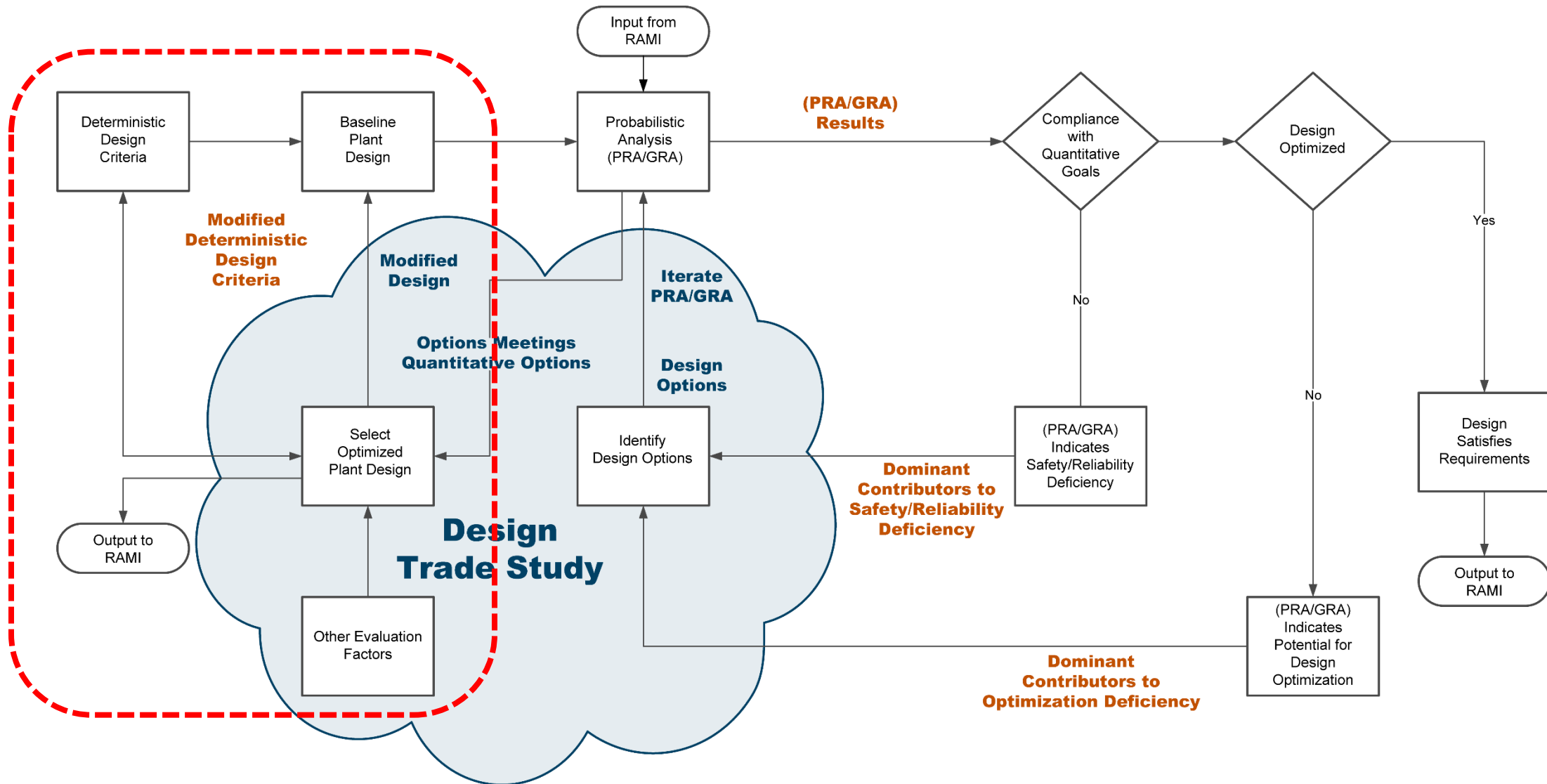
Process Flow for Risk-informed Design



Process Flow for Risk-informed Design



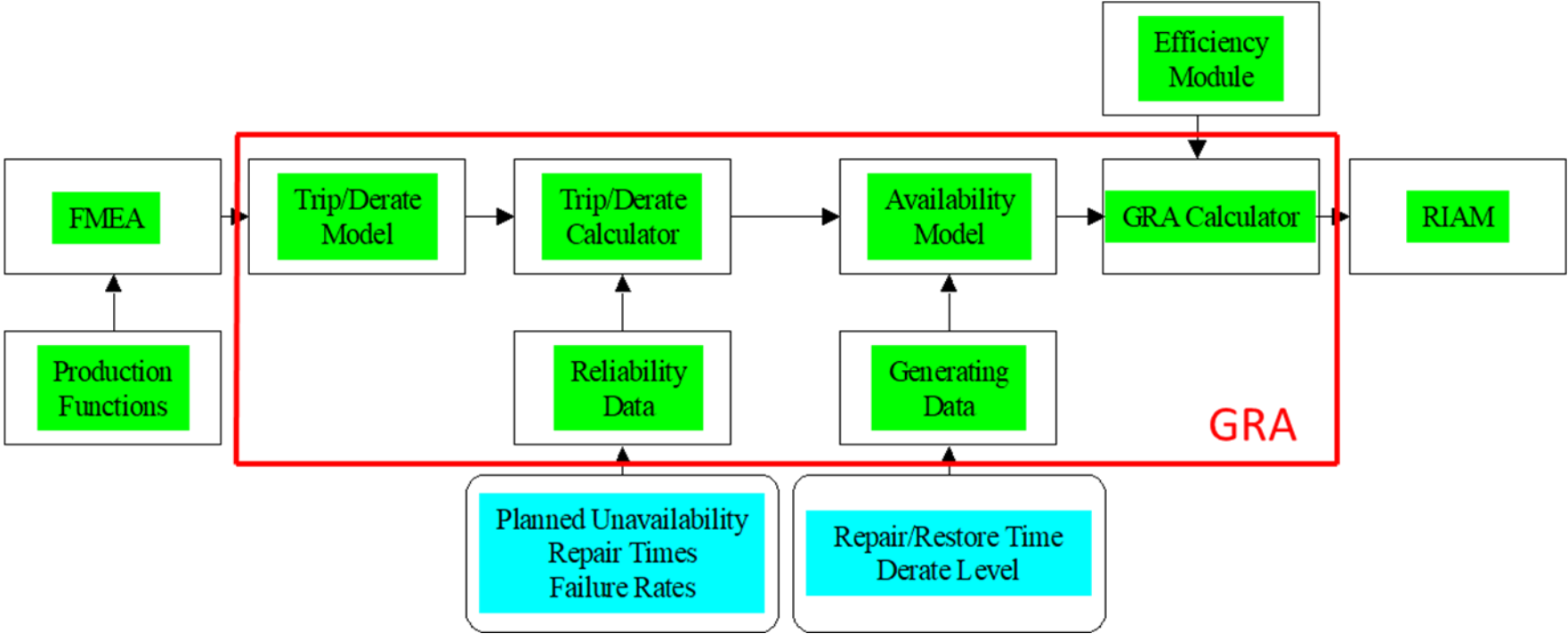
Process Flow for Risk-informed Design



What Is Generation Risk Assessment?

- + GRA is the process of estimating the risk of generation loss during plant operation
 - Combines modeling of probability, magnitude, and duration of plant trip or derate due to postulated equipment failures
- + GRA models potential generation and economic impact (MWh/yr) -- similar to modeling of safety impact in probabilistic risk assessment (PRA)
- + More robust than simplistic qualitative approaches (e.g. single point vulnerability)
 - Addresses redundancies / interdependences of plant systems and components
 - Provides quantitative estimates to support decision-making.
- + Provides importance rankings of critical components in terms of production risk to support effective and efficient resource allocation

Typical GRA Flow Diagram



RAMI serves as an integral element of nuclear plant safety and economic performance

- + A cornerstone of nuclear plant design and operation is an effective reliability, availability, maintainability, and inspectability (RAMI) program
- + RAMI is an integrated planning, design, analysis and operational program to ensure that plant structures, systems, and components (SSCs) are capable of achieving plant safety and operational objectives in a cost-effective manner
- + RAMI is focused primarily at the system and equipment levels to set and monitor performance goals throughout the plant life cycle
- + The interface with the PRA and GRA is to make sure that more aggressive goals are set for equipment (or sets of redundant equipment) whose inability to perform its function would result in increased safety risk (e.g., environmental release) or reduced operational capability (e.g., capacity factor)

What is RAMI?

Three step process integrated into plant design, commissioning, and operation

Step 1: Qualitative Reliability Evaluation

- + Analytical Technique: Failure Modes and Effects Analysis (FMEA)
- + Answers Question: “What are the possible component failure mechanisms and their effects?”
- + Outcomes: Specification of SSC functional importance and prescribed inspections, monitoring, and preventive maintenance activities

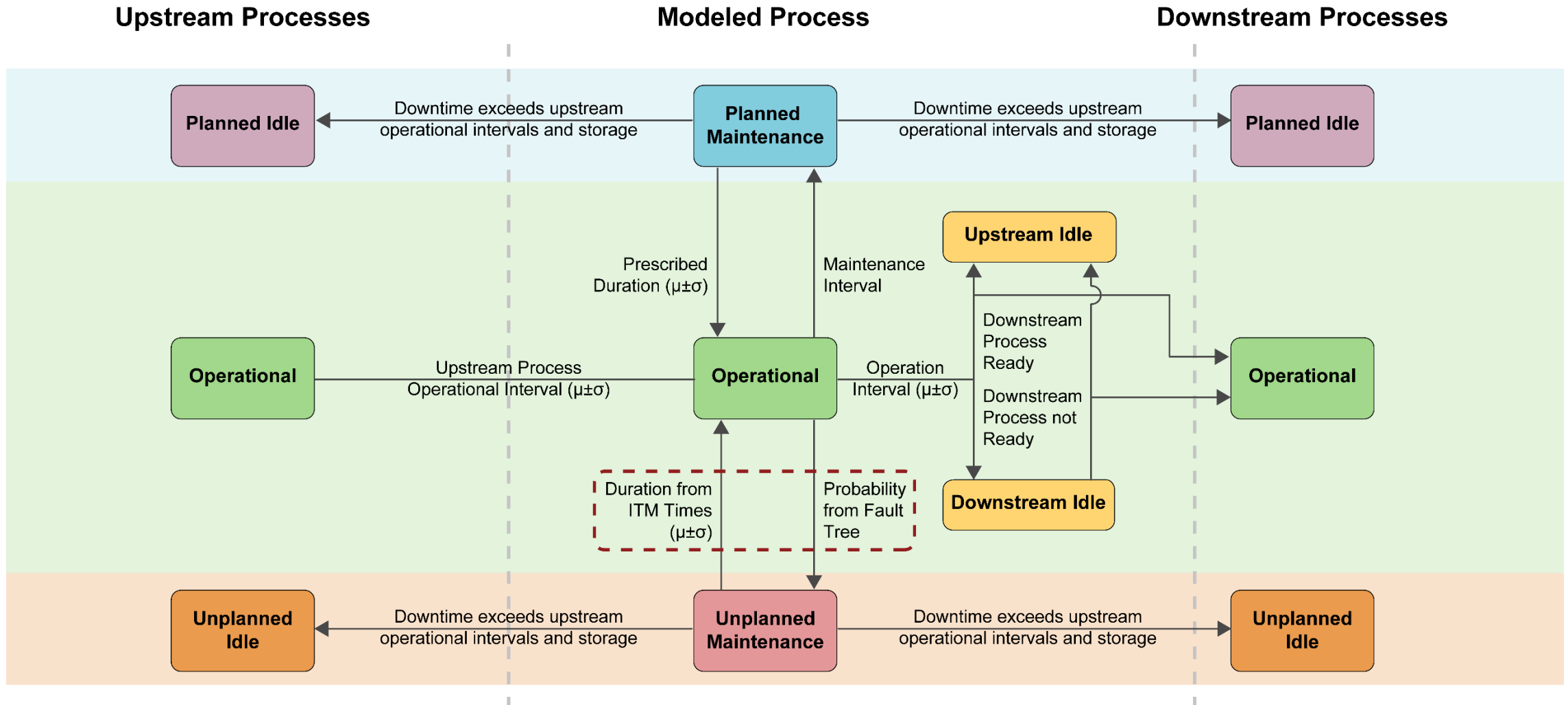
Step 2: Quantitative Reliability Evaluation

- + Analytical Technique: Event Tree / Fault Tree Analysis
- + Answers Question: “How does failure of a component affect the system and plant?”
- + Outcome: Estimates of key metrics for safety (frequency of core damage event or radioactive release via PRA model) and production (frequency of plant trip or load reduction via GRA model)

Step 3: Production Analysis

- + Analytical Technique: Production State Model (simulation model)
- + Answers Question : “What is the expected performance over the facility’s operational lifetime?”
- + Outcome: Estimates of plant performance over projected operating life

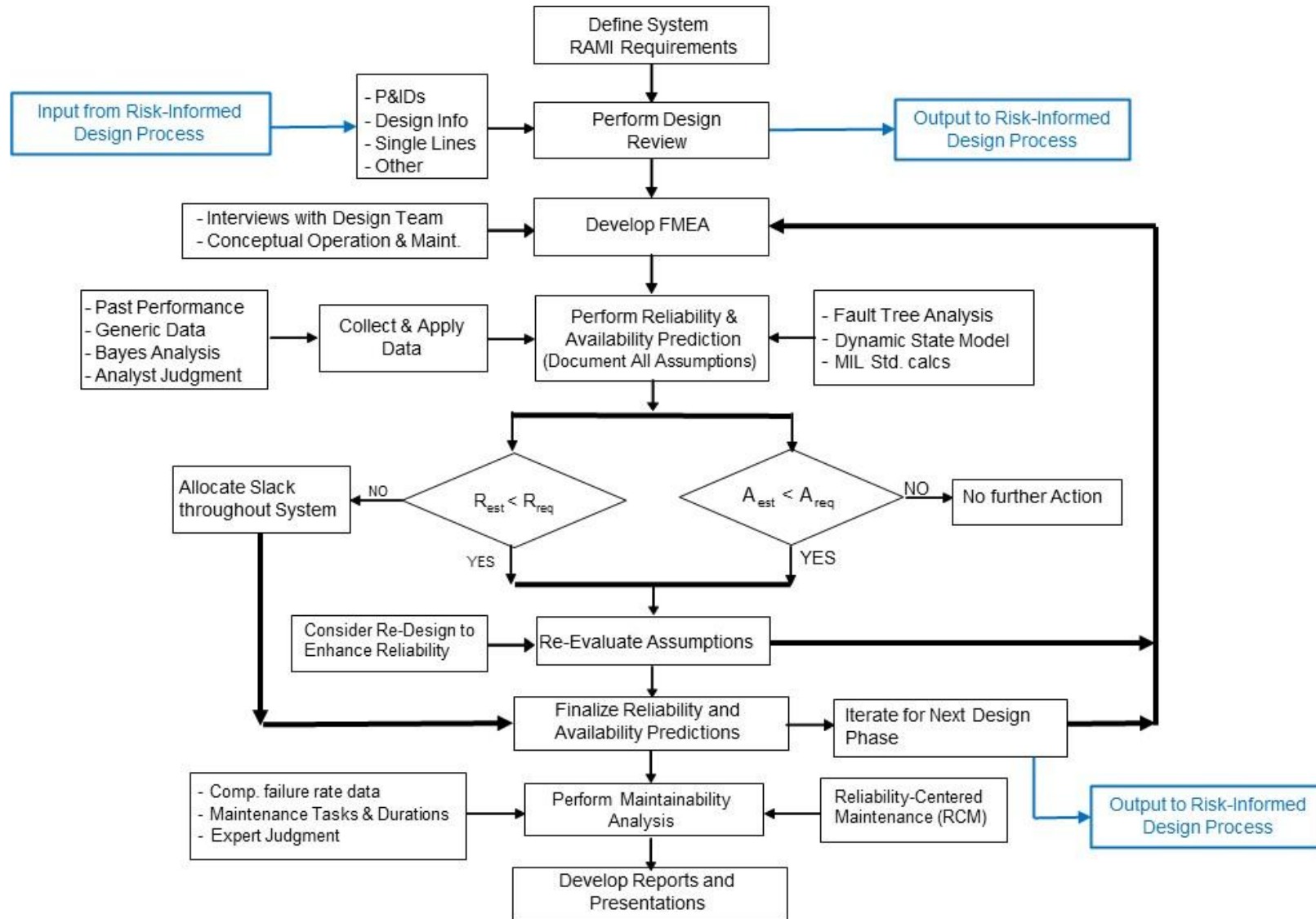
State Model Approach



RAMI provides essential information to support decision-making

- + **Classification of the functional importance (criticality) of plant SSCs with respect to safety, production, and economics**
- + **Identification and prioritization of actions that can be taken to improve plant performance. Specific applications where the RAMI program provides feedback include:**
 - Identification of areas where design changes would provide substantial safety, production, or economic benefits
 - Specification of maintenance activities (preventive, predictive, or condition based) required to ensure SSC performance capabilities are achieved
 - Identification and evaluation of alternatives to enhance plant economics (e.g., minimize costs)
- + **Integrated monitoring of plant SSCs to assess performance and trends against desired outcomes**
- + **Provide comprehensive framework to evaluate potential modifications to plant maintenance and asset management strategies throughout the facility life cycle**

RAMI Process Flow



Typical Design Issues Addressed by the Process

Plant Modeling and Evaluation Activities, Including Importance and Sensitivity Studies, Help Determine Which Design Aspects Are Key to Meeting the Goals

- + Physical separation of systems
- + Functional capacity of equipment
- + Basis and content of operations and maintenance procedures
- + Testability of equipment or systems during operation
- + Corrective and preventative maintenance, including during operation (maintainability)
- + Test and inspection intervals
- + Allowable outage times for failed equipment
- + Actions to mitigate equipment failures
- + Operational aids
- + Operation and maintenance training

Overall Approach

The Basis for the Design Assessments and Decisions Are the Plant Models

- + The keys to the successful application of the models are:
 - A structure that provides useful output for the major design packages **as the design evolves**;
 - A close integration of the modeling activities into the design process to keep pace with the design at each decision point;
 - The use of automated computer tools to allow for easy iteration as the design changes; and
 - The creation of addressable parameters that will be used in the design decision process
- + The models must reflect only what is known at the given point in the design process, and so will start out being simple and will gain detail as the design process continues.
- + The decisions at each point in the design process will focus on those aspects of the design that are most difficult to change as the design evolves.
- + The PSA model scope should include all modes and all hazards

The Models Need to Cover Both Safety and Production

- + The PSA model scope will be typical as currently done for operating plants
 - All modes
 - All hazards
- + The GRA model scope needs to address the ways in which capacity factor can be lost.
 - Planned outages
 - Primarily refueling outages
 - How can the plant design make these outages more efficient, e.g., fuel handling, major equipment overhaul
 - Unplanned outages – the “OK” sequences in a PRA
 - All normally operating systems need to be modeled; e.g., primary cooling, secondary cooling, water cleanup systems, chemistry control; anything whose failure can result in a shutdown.
 - Administrative shutdowns – the interface between safety and production (“a safe plant is an efficient and reliable plant”)

Model Progression Through the Process

Evolves Through the Phases of the Design – Roughly as Follows

- + Conceptual Design Phase
- + Preliminary Design Phase
- + Final Design Phase
- + Construction Phase
- + Pre-Operations Phase
- + There isn't really a “bright-line” separating the phases.
- + Different parts of the plant could be in different phases at any given point in time.
- + The risk-informed decisions are not made all at one point in a phase – they happen during the phase as adequate information comes out of the modeling activities.

Model Progression Through the Process

During Each Phase, The Risk Team Needs to Define....

- + What information is available and should be provided by the Design Team?
- + Based on that information, what should be modeled?
 - Level of detail
 - Don't get ahead of the design
 - Stick to what is known
 - Assume only what fits the known envelope
- + How should human factors and actions be considered?
- + What are the types of decisions can be supported given the state of the design?

Don't torture the risk model until it screams for mercy and gives you what you want!

Questions?



Thank You

Paul Amico

pamico@jensenhughes.com

Skype: paul.amico

WhatsApp: +1.443.745.2360



*Executive Consultant
Energy + Utilities
pamico@jensenhughes.com*