Reassessing Nuclear Risk Assessment Using Marked Point Processes and Discrete-Event Simulation: Challenges and Opportunities

Ernie Kee[1] Wen-Chi Cheng[2]

[1]University of Illinois Urbana-Champaign, Urbana, Illinois, USA
[2]Idaho National Laboratory, Idaho Falls, Idaho, USA

PSAM 18
July 19–24, 2026, Pittsburgh, Pennsylvania

Presented by Wen-Chi Cheng

Outline

Why Revisit Classical PRA?

Classical PRA has served well...

Formalized in the Reactor Safety Study (WASH-1400); the primary framework for quantifying nuclear plant risk across design, operation, and regulation.

...but rests on assumptions increasingly hard to reconcile with practice

- Steady-state availability metrics and effectively infinite time horizons
- Independent, memoryless initiating event processes
- System behavior represented through static fault-tree logic
- Risk expressed as long-run frequencies from combinatorial approximations

These assumptions obscure time-dependent behavior and configuration-specific vulnerabilities in modern plants and advanced reactors.

The Regulatory Context Is Shifting

- Risk-informed, performance-based frameworks — including those envisioned under 10 CFR Part 53 — emphasize:
  - Demonstrable system performance *over time*
  - Explicit treatment of uncertainty
  - Transparent linkage between design choices and safety outcomes
- Judicial developments (*Loper Bright Enterprises v. Raimondo*) reinforce transparency and traceability requirements
- Classical PRA's long-run frequency metrics (CDF, LERF) are not well matched to these expectations

Question: can risk be reformulated as a time-domain stochastic process problem suited to licensing?

Risk as a Time-Domain Stochastic Process

System state trajectory: time-indexed vector describing the plant — component status, maintenance/test/repair state of each train, plant configuration, environmental and hazard conditions.

Internal events (reconfigure the plant)

- Component failures, repair completion
- Surveillance tests; scheduled & corrective maintenance
- Failure-mode removal via root cause analysis

Challenge events (arrive at the plant)

- Internal initiating events
- External hazard arrivals — stochastic events with arrival-time process and magnitude/type marks

Accident occurrence = a counting process

Accidents are counted when a challenge arrival coincides with a plant configuration unable to respond — an initiator meeting a vulnerable protection-system state.

Coupled Time Scales Within a Finite Horizon

- **Hours to months**: internal configuration changes — testing, maintenance, repair, failure-mode removal
- **Characteristic recurrence scales**: external hazard and initiating-event arrivals
- **Seconds to hours**: accident progression and containment response, once initiated
- All embedded within the finite operating horizon of years that defines the licensing-relevant evaluation period

Separating internal configuration dynamics from the external arrival process — while coupling them in one stochastic formulation — is what enables configuration-specific, time-localized risk quantification: ETTA distributions, exposure durations, conditional risk under evolving conditions.

Relation to Prior Work

- **Dynamic PRA / DES methods**: typically retain event-tree logic and scenario-based simulation rather than an underlying stochastic process formulation
- **Holmberg (1997)**: demonstrated MPPs for nuclear safety — living PRA, risk follow-up, operational optimization — but did not address accident progression, normal process termination, or maintenance-driven removal of failure modes
- **This work**: frames the transition to MPP/DES as a licensing-relevant finite-horizon modeling problem
  - Finite-horizon accident quantification
  - Explicit maintenance efficacy and corrective action
  - Dynamic dependencies and failure-mode removal
  - Interpretation of time-dependent metrics for oversight

Challenge 1: Computation and Data

Computational demands

- Classical PRA: rare-event frequencies approximated analytically via minimal cut sets
- DES: repeated simulation of trajectories to estimate ETTA distributions and exposure durations
- Rare events require large run counts or variance-reduction techniques; parallelization and convergence diagnostics become central

Data requirements and parameterization

- Time-dependent failure behavior, repair duration distributions, maintenance scheduling and effectiveness
- Imperfect maintenance: partial restoration and "better-than-new" outcomes
- Integration of operational sources such as CMMS records; new estimation methodologies may be needed

Challenge 2: Dependencies and Common Cause Failure

- Classical PRA treats failures as largely independent, with dependencies folded into simplified CCF constructs
- Static CCF models implicitly assume simultaneous latent failure mechanisms persisting across redundant components until challenged

But operational practice says otherwise

Failures are mostly identified during testing, inspection, or maintenance — not during accidents — triggering root cause analysis and corrective action that remove failure mechanisms before subsequent demands.

- MPP/DES models the lifecycle of failure modes: introduction, detection, correction, removal, possible reintroduction
- Dependencies arise and dissipate over time rather than persisting as latent conditions

Challenge 3: Interpretability and Regulatory Alignment

- CDF and LERF are simple, widely understood scalars; trajectory-based models produce distributions of outcomes and time-dependent measures
- CDF/LERF are not inaccurate — but as time-averaged frequencies predicated on stationarity and an infinite horizon, they cannot express:
  - the distribution of Expected Time To Accident (ETTA)
  - finite-horizon exposure and risk clustering within an operating cycle
  - instantaneous, configuration-specific risk during a particular maintenance or test state
- A single scalar acceptance threshold is ill-posed for a time-indexed, distribution-valued risk measure
- New acceptance criteria needed — e.g., limits on finite-horizon accident probability, or on duration and depth of elevated-risk configurations

What the Framework Buys You

Time-dependent risk

- ETTA distributions, exposure durations
- Configuration-specific risk under evolving conditions
- Maintenance scheduling and environmental stressors in one structure

Dynamic dependencies

- Failure modes introduced, detected, corrected, removed
- Redundancy effectiveness depends on design diversity *and* the processes that find and fix failure modes

Explicit maintenance & corrective action

- Interventions modeled in time, not as average availability
- Root cause analysis removes failure modes before demands

Performance-based alignment

- Observable behavior over the operating horizon
- Direct, defensible basis for safety margins

Containment as a Dynamic Barrier to Risk

- ECCS hearings (1973) highlighted uncertainty in protection-system performance — and containment's role as the final barrier to public risk
- The distinguishing contribution is *not* dynamic in-accident modeling (existing dynamic PRA does this), but embedding the pre-accident process in the same stochastic structure:
  - Plant configuration at accident onset is an endogenous outcome of maintenance, repair, testing, and failure-mode removal — not a boundary condition
  - Pre-accident operation, accident occurrence, and containment response carried within a single filtration
- Core damage as an absorbing state reached at a stopping time; the relevant quantity is first-passage probability over the finite horizon — something a steady-state frequency cannot express

Prevention–Mitigation Tradeoffs, Unified

- Both accident occurrence *and* post-accident consequence exposure quantified over finite horizons
- Supports a regulatory strategy that:
  - relies on established industry practices for core-damage prevention
  - evaluates containment under the assumption that core damage has occurred
- Provides robustness against residual uncertainty in protection-system performance while maintaining consistency with defense-in-depth principles
- Licensing evaluations may benefit from treating inspection, testing, and maintenance programs as integral components of system reliability rather than secondary considerations

A Necessary Caveat: Unanticipated Failure Scenarios

- All predictive risk formulations condition on information available at analysis time — implicitly assuming all relevant failure scenarios are known
- Unanticipated protection-failure scenarios introduce an unavoidable optimistic bias in computed risk metrics (Kee & Wortman, 2023)
- This limitation applies to classical PRA *and* to MPP/DES — greater fidelity does not eliminate it
- Reinforces defense in depth, safety margins, and corrective action programs as essential complements to quantitative risk assessment

Conclusions

- Classical PRA organizes knowledge of failure pathways well, but steady-state assumptions, static logic, and simplified dependency treatments limit fidelity to operational reality
- MPP/DES represents system evolution explicitly in time: accident occurrence emerges from the interaction of initiating-event arrivals and protection availability
- Maintenance efficacy, root cause analysis, and failure-mode removal are determinants of future exposure — not secondary details
- Real challenges remain: computation, data, abstraction, regulatory implementation
- The shift from long-run frequencies to time-indexed behavior aligns naturally with risk-informed, performance-based regulation

Future work

Efficient rare-event simulation • parameter estimation from operational data • regulatory metrics that fully leverage time-domain risk representations

Acknowledgments

- Professor Paul Nelson (Texas A&M University, deceased) and Professor Martin Wortman (Texas A&M University), whose work informed the stochastic analysis concepts presented here
- Jim Liming, David Johnson, and Don Wakefield (formerly of ABS Consulting) for discussions and contributions to risk analysis
- Colleagues at South Texas Nuclear Operating Company (STPNOC), particularly Alice Sun
- Vera Moiseytseva, Ph.D., for her work as an STPNOC intern and ongoing collaboration

Thank you — Questions?

WenChi.Cheng@inl.gov • erniekee@illinois.edu