Rethinking Safety-Related Controls for the DOE Test Reactor Pilot Program

By Ryan Marcum | Nuclear I&C Consultant July 7, 2025

The DOE's newly announced Advanced Reactor Pilot Program to authorize test reactors outside the national laboratories represents a major shift in the regulatory pathway available to advanced reactor developers. At least three reactors are expected to reach criticality by July of 2026; a timeline that, on the surface, seems optimistic but achievable for teams with progressing designs and sufficient funding.

According to a Request for Applications (RFA) issued by the DOE, submitters must demonstrate a mature reactor design, a qualified fuel and waste disposition plan, full execution readiness, and sufficient financial and supply chain resources. However, a critical supply chain reality raises a difficult but necessary question, *"Is procuring and integrating a modern, safety-related I&C systems in time to meet this 12-month window feasible?"* For anyone from the currently operating nuclear fleet with experience doing so, the answer is no.

At present, the lead time for NQA-1 pedigreed safety-related control systems—especially those requiring qualified 1E components and V&V'ed software with the full accompanying suite of documented proof—often ranges from 12 to 18 months… or more. And that assumes that you fully specified the system and issued the PO yesterday. These timelines reflect unavoidable design changes and the complexity of qualification, dedication, validation and integration processes necessary for compliance under the typical NRC licensing framework. The currently operating fleet begrudgingly, accommodates margin for these delays into the schedule. For a test reactor seeking rapid deployment under DOE authority, they are a non-starter.

The good news is that such highly qualified systems are not required for these unique circumstances.

DOE Authorization and the Nature of Safety Controls

The pilot program explicitly operates under DOE's independent authority granted by the Atomic Energy Act similar to how the NRC licenses research reactors under Class 104(c) provisions. To clarify, reactors selected for this program will not be licensed by the NRC (yet). Instead, safety authorization will be governed by DOE Order "O" 420.1C and supported by a documented safety analysis in the format of DOE-STD-3009.

These directives do not prescribe safety-related controls in the manner typical of NRC frameworks. Instead, they emphasize appropriate functional safety - ensuring reactor hazards are analyzed, bounded, and controlled proportionately to the actual risks posed. The focus is on performance-based requirements and the reliable fulfillment of essential safety functions, rather than component pedigree or specific design lineage.

This distinction can save several crucial months from a safety controls vendor's delivery schedule. DOE Order 420.1C explicitly permits the use of a graded approach, enabling developers to align the rigor of safety systems directly with the severity and likelihood of potential system failures. Similarly, DOE-STD-3009 emphasizes hazard-based analysis, resulting in safety system classifications only when necessary to prevent or mitigate consequences exceeding defined evaluation guidelines.

For organizations already applying a risk-informed, performance-based approach to reactor systems, this perspective may not be new. However, being at the forefront, your team will likely need to guide your safety controls vendor along this less-familiar path.

Practical Implications for Reactor Developers

This opens the door to a fundamentally different approach to I&C system design. Rather than beginning with an assumption that safety-related controls must be designed, procured, and qualified using a one-application-fits-all mindset, applicants can instead start from a hazard-based analysis and justify the minimal-yet-sufficient use of safety-classified I&C.

The following suggestions respect DOE's safety expectations without importing the weight of commercial-reactor orthodoxy. The result is a test platform that gets out of the way of reaching criticality on time and supports proving your technology.

1. Strip Commercial-Grade Lingo Out of Your Specification
   The moment a procurement package mentions IEEE Stds. 603 or 7-4.3.2, it tacitly declares that your test reactor intends to look, feel, and cost like a grid-connected plant. That single cue invites vendors to assume Class 1E hardware and full software lifecycles. By omitting legacy power-reactor references altogether, you preserve the freedom that DOE's hazard-based framework is meant to provide and keep quotations aligned with a test-scale budget.
2. Control the Connotation. No "V&V," No "Safety-Related" Labels
   In commercial circles those terms (and others along the same vein) trigger expansive quality programs and exhaustive paperwork. Under DOE and NRC-approved test reactor programs, they are neither mandatory nor particularly helpful. Discussing your control project in specific test reactor language communicates to reviewers and vendors only what is necessary for your reactor, which helps them calibrate their expectations.
3. Limit Documentation to What DOE Must Approve
   There is elegance in restraint balanced with sufficiency. A concisely delineated set of deliverable documentation demonstrates that the system meets exactly what is necessary. Everything else adds value only after the reactor has proven itself. Deferring these "housekeeping" or commercial-oriented items guards time without compromising regulatory approval.

4. Draft with Tomorrow in Mind—within Reason
   The I&C architecture, like the pilot reactor design, is a stepping-stone to a future commercial version. Craft your core documents so they can be adapted, but not necessarily precisely reproduced. Recognize that the design itself will evolve; an efficient baseline now is far more valuable than a "perfect" file destined for revision later.
5. Leverage Operator Actions for Non-Urgent Events
   Where the physics provides ample response time, crediting trained operators instead of auto-trip logic allows protective functions to remain in a lower QA tier under DOE Order 420.1C.
6. Opt for an SER-Approved Platform
   A platform that already carries an NRC Safety Evaluation Report approval stamp is admittedly over-qualified for a test unit, yet that pedigree buys immediate regulatory credibility. More importantly, it eliminates the calendar drain of additional qualification testing which isn't required for a test reactor application. Time saved here dwarfs the incremental up-front cost.
7. Match Component Lifetimes to the Project's Actual Horizon
   If your experiment will conclude in a few years, specifying components with shorter but available lead times is smart risk management. For instance, mineral-insulated detector cabling rated for ten years is overkill and can cost an additional 6 months when the core mission spans three.
8. Consolidate Protective Functions Where Justifiable
   Combining multiple safety systems into a single, well-justified one reduces hardware and project documentation. The simplicity complicates regulatory review but streamlines procurement and field installation.
9. When in Doubt, Keep Digital Out
   Analog safety trips are old-fashioned, but they carry no software life-cycle burden and virtually no regulatory risk. In a pilot setting, that conservatism is paradoxically the most schedule-agile option.

This path clearly aligns with the stated goals of the pilot program: to establish the *technological viability* of advanced reactor designs, not to qualify them for power production or immediate commercial readiness. It also avoids the lead time and cost burdens associated with unnecessary qualification processes that can delay deployment.

Avoiding the Commercial Mindset Trap

Most advanced reactor developers harbor long-term commercial ambitions and thus may feel pressured to overengineer their initial I&C systems under the assumption that this approach will simplify future NRC licensing. While understandable, this rationale is counterproductive within the context of the DOE test reactor pilot program.

A test reactor, at this stage, is not a commercial power reactor. It does not require a Reactor Protection System (RPS) with full NQA-1 safety-related pedigree. Rather, it requires a credible, clearly documented safety case supported by reliable operational systems and sufficient safety margins appropriate for its specific hazards.

You might be thinking, “But we plan to commercialize. Eventually, we envision this reactor, or its successor, being commercially licensed. Shouldn't we build to those standards now and gain a head start?”

You certainly could. However, doing so may severely jeopardize your ability to meet the program’s deadline. A meticulously engineered reactor that never achieves criticality due to timeline overruns contributes nothing to your future commercialization goals.

A more strategic approach is to clearly differentiate what your reactor requires today from what will be needed later. Initially, design your system explicitly to meet the criteria for achieving criticality under DOE authorization. Use this early opportunity to generate empirical data, demonstrate robust performance, and document a successful operational history. With this evidence in hand, your transition toward future commercial NRC licensing becomes both smoother and more compelling.

Conclusion

The timeline of the DOE test reactor pilot program all but precludes the use of traditional safety-related I&C systems as typically conceived in the commercial nuclear space. The constraint should be viewed as a design parameter, not a restriction.

The authority under which this program operates encourages developers to take full advantage of the graded approach and hazard-based design philosophy. Reactors can, and should, be designed with minimal safety-related controls where justified and should avoid adopting commercial standards that are neither required nor viable per the current schedule.

By focusing on unique safety analyses and risk rather than testing pedigree, applicants can meet the program’s timeline, secure authorization, and position themselves for future commercial pathways with real world data in hand.

Ryan Marcum is a nuclear instrumentation and control consultant with a focus on non-commercial test reactors, licensing strategy, and lean system design. He has supported safety and control system development for research, test, and demonstration reactors licensed under DOE and NRC authority.
marcum@icoperative.com | LinkedIn