Protection Guidance for the Layman to Accelerate the Licensing and Deployment of Small Modular Reactors into the Texas Grid (ERCOT)

Version 1.0

WRITTEN BY

Michael Cohen

Tim Roxey

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY®

Protection Guidance for the Layman to Accelerate the Licensing and Deployment of Small Modular Reactors into the Texas Grid (ERCOT)

Version 1.0

Michael Cohen, Raise Up LLC

Tim Roxey, Eclectic Technologies

July 2026

Contents

Abstract

Small Modular Reactors (SMRs) are a faster way to build new nuclear power in Texas than large, traditional reactors. They stay safe and secure through design features that need no operator action and no outside power. Texas has already put money behind them. A 2025 law, House Bill 14, created the Texas Advanced Nuclear Energy Office and a $350 million fund — the largest such state commitment in the nation. The money is released as a project reaches its federal licensing milestones.

SMRs answer three of ERCOT's most pressing reliability needs. They restore grid inertia — the physical stability that Winter Storm Uri showed was missing. They fill the gap in steady, around-the-clock power that the growth of wind and solar has opened. And they can run in “island” mode, powering a local area on their own when the wider grid is down.

One obstacle stands in the way of moving faster: a gap in the rules. The large reactors already running in Texas were licensed against a Design Basis Accident (DBA) — the official list of accidents and disasters, natural and man-made, that a plant must be able to survive. SMRs have no such NRC-issued list yet. To give regulators and the public confidence that SMR designs can prevent or limit credible man-made attacks — not just accidents and natural disasters — this report supplies the missing adversarial DBA. It covers three attack types — cyber, physical, and drones (uncrewed aircraft systems, or UAS) — at three threat levels: Low, Elevated, and High.

Tier 1 Cyber and off-the-shelf drone threats that exist anywhere. A direct physical (kinetic) attack is not a credible near-term risk.

Tier 2 Adds early signs of cyber intruders getting into position, plus a physical attack that is possible but not yet imminent.

Tier 3 A high chance of a near-term terrorist attack, with all three threats at their worst credible level. A separate step — the applicability determination — sets the outer limit. These three levels are the core of the analysis. A deliberate military attack by a nation-state would sit above them, but for a plant at this location that case is judged not to apply, and it is handled in the parent methodology series.

The analysis shows that SMR designs, with their passive-safety features, are already strong enough at the Low and Elevated levels. At the High level they need only small, well-defined changes to close one remaining risk. By providing a ready-to-review DBA before any specific license application, this report supports a faster licensing path for Texas SMRs — for the benefit of all Texans.

A. Introduction and Overview

1. Context and Purpose

Texas has committed to advanced nuclear power on a scale no other state matches. House Bill 14, effective September 1, 2025, created the Texas Advanced Nuclear Energy Office and the Texas Advanced Nuclear Development Fund. The fund starts at $350 million, with legal room to grow to as much as $2 billion, and it ties that money to the federal licensing milestones an advanced-reactor project must reach. The goal is grid reliability as much as economic growth. SMRs supply what the ERCOT system needs most and increasingly lacks:

1. Baseload generation that is fuel-secure.
2. Power when wind and solar are not available.
3. Rotating inertia connected to the grid to stabilize system frequency.
4. A “frequency buoy” that holds Texas’ island grid together — the steady source the SMR island locks onto to keep vital power flowing when outside power is gone (see Section C.1).

A gap in the rules stands between that commitment and its payoff. The large light-water reactors running in Texas — South Texas Project and Comanche Peak — were licensed against a Design Basis Accident (DBA) envelope the NRC built up over decades. No version of that envelope exists yet specific to Small Modular Reactors (SMRs), and the large-reactor version does not simply carry over. This latter because the SMR’s safety case rests on design features large-reactor rules never assumed. Two problems follow.

1. Deployment can stall while the regulator and each applicant build a design basis from scratch
2. And until that basis exists, regulators and the public have no worked-out assurance that SMR designs can prevent or limit credible threats.

This report closes that gap. It provides and tests a Design Basis Accident for the near-term SMR — including the adversarial design basis that deliberate threats require — before any specific construction-and-operating license application is filed. Handing the applicant and the NRC a ready framework to review, instead of one to invent, is what shortens the licensing review.

The report is written for general readers as well as specialists. It draws on two main sources:

1. The Design Basis Accident — Military Action (DBA-MA) series, which builds design-basis methods on the IAEA safety standards and supplies those methods here; and
2. NERC's Large Load Working Group, which ERCOT belonged to, which informs the grid-interaction analysis.

2. Scope and the Applicability Determination

An applicability determination sets the scope of this report up front. The design-basis method used here has three layers: the Design Basis, the Design Basis Accident, and a Military-Action extension of it (DB → DBA → DBA-MA). The determination fixes which layers this report covers and which it does not.

This report develops a three-tier adversarial Design Basis Accident for the reference SMR — cyber, physical, and drone (UAS) threats at the Low, Elevated, and High levels, as the contract's statement of work requires. Its method comes from the DBA-MA series (cited in Appendix A). The statement of work is built around sub-state threats, not nation-states: its highest tier is a near-term terrorist attack at the worst credible level. The DBA-MA series reaches one step higher — to deliberate nation-state military action, marked by intent, persistence, precision, and denial. This report stops at that boundary. It keeps all three adversarial tiers in full and finds that the nation-state military-action layer above the High tier does not apply to this SMR deployment. That decision is recorded here as an explicit applicability determination, so its basis can be audited and the series' inheritance obligation (Appendix A) is preserved.

The determination runs the deployment through the four-filter gate of the Military Action Applicability Framework (DBA-MA-AF §2, Appendix A). Under §2.5 the gate is an "inclusive-or": if any one filter is met, the facility falls inside the military-action design basis. Only if the facility clears all four filters is the answer negative — and each result must be documented and kept for review (DBA-MA-AF §3). The gate is deliberately built to lean toward inclusion. This report clears all four filters, as follows:

Filter 1 — Location relative to defense-critical loads and supply. Cleared. The reference site on the Texas Gulf Coast is not next to an adversary, and its distance from any staging area puts it at the Tier 1 baseline: cyber and commercial-drone threats are present everywhere, but a direct physical attack is not a credible near-term risk. The SMR campus serves community resilience, not a defense-critical load or a continuity-of-government role.

Filter 2 — Position in strategic transport corridors. Cleared. The campus is a power-generation node inside ERCOT. Losing it would not cut a transmission corridor of regional or national importance, and it sits on no military supply chokepoint.

Filter 3 — Substitutability. Cleared, but only on one condition — stated because low substitutability alone would trigger this filter. The resilience mission is what raises this facility's value: an asset whose loss would end the survival power of a hospital-anchored island is, by this report's logic, high-value. Within the required restoration time, that role can be covered only by bridge power — right-sized hospital backup generators or a second anchor source (Section C.4 and Recommendation D.2.d). With that in place, losing the campus does not leave life-safety loads without power, and the filter clears. Without it, the filter reads positive and the military-action layer enters the design basis.

Filter 4 — Adversary targeting logic. Cleared. Seen from a nation-state adversary's point of view rather than the operator's, the campus is not worth attacking at this location: it is neither a defense-critical supply node nor a corridor chokepoint, and the distance that clears Filter 1 applies just as well to the precision strikes and area-denial a state adversary would use.

So the nation-state military-action layer is set aside on the record, tested against each of the four filters as DBA-MA-AF §3 requires — not by a one-off exemption. The consequences that the resilience mission's value raises are already carried by the adversarial design basis this report develops: the range-independent cyber threat across all three tiers, and the persistence and denial-of-access traits handled inside the High-tier analysis.

This decision fits this SMR site as it stands today, and it can change. It is revisited if the site becomes adversary-adjacent, if its strategic value is reclassified, if the bridge-power condition behind Filter 3 lapses, or if the threat environment shifts; the full DBA-MA military-action analysis stays available in the parent instrument for that purpose (Appendix A). The plant's physical-protection duties are unaffected: detecting and stopping drones is treated here as a standing 10 CFR Part 73 life-safety and security matter, whoever is flying.

3. Document Organization

This section has given the context, scope, and applicability determination for the SMR deployment.

Section B names the gaps the report addresses: the missing SMR adversarial design basis; how the federal licensing pathways (10 CFR Parts 50, 52, and 53, plus the proposed Part 57) map to the SMR, and the gap each one leaves; the coordination gap between the NRC and the Texas grid authorities; and the gap in authority to defeat hostile drones.

Section C develops the four analytical topics: the grid-reliability case for SMRs in ERCOT, the accident characteristics an SMR must show for licensing, the three-tier adversarial design basis, and how well SMR passive safety holds up across that threat range.

Section D makes the case for faster licensing of SMRs in Texas.

B. Gap Assessment

This report addresses two kinds of gaps. The first is substantive: there is no specified Design Basis Accident for the SMR that accounts for deliberate attacks. The second is regulatory and institutional: the openings that the federal licensing pathways, the grid-coordination rules, and the airspace laws leave for SMRs on the Texas grid. The report does not list problems for their own sake — each gap below is one that a fully developed SMR design basis, supplied before licensing, is meant to close.

1. The Absent SMR Adversarial Design Basis

The large light-water reactors in Texas were licensed against a Design Basis Accident envelope built over decades of NRC practice. The near-term SMR has no equivalent in SMR-specific form, and — more to the point — no adversarial design basis exists for the SMR class at all. The accident-side safety case is well developed for certified designs: passive safety handles decay heat and loss of cooling, and the smaller radioactive source term supports a smaller emergency planning zone. But that case says nothing about a deliberate attacker. The smaller source term is credited only for accidents; it does not bound an attacker who can break the barriers the accident case assumes stay intact. Section C closes this gap by developing the cyber, physical, and drone design basis across three threat levels that accident analysis does not cover.

2. Federal Licensing Pathways and Their Residual Gaps

An SMR builder in Texas has three federal licensing pathways available, with a fourth proposed for microreactors and other designs with a similar risk profile. Each is a mature or maturing tool that does a defined job, and each leaves one gap for an SMR facing a deliberate threat. The table below credits what each pathway does and names the gap it leaves.

Pathway	Status and SMR fit	What it does	Gap it leaves for SMRs
10 CFR Part 50 — Domestic Licensing of Production and Utilization Facilities	Two steps: a construction permit, then an operating license. The original home of the Design Basis Accident idea. Available, but not the near-term SMR path.	Defines the design-basis envelope, the General Design Criteria, the safety analysis report, and the event-reporting setup that DBA analysis is built on.	Built around equipment failure, natural hazard, and operator error. There is no adversarial design basis; sabotage is handled separately under Part 73 as a security-and-barrier matter. It is also the slowest path, which works against the goal of speed.
10 CFR Part 52 — Licenses, Certifications, and Approvals for Nuclear Power Plants	Combined license plus design certification. The near-term SMR path: the NuScale design is certified as Appendix G (effective February 2023), and the reference deployment is licensed here.	Bundles construction and operation in one license. Many applications can reference one certified design. Each needs a safety analysis report, a probabilistic risk assessment, and a physical-security plan.	Inherits the Part 50 accident envelope. The smaller emergency planning zone is credited from the accident source term, not an adversarial one. No adversarial design basis is required in the application, and the SMR threat tiers are not separately assessed.

Pathway	Status and SMR fit	What it does	Gap it leaves for SMRs
10 CFR Part 53 — Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants	Final rule effective April 29, 2026. An optional third path that does not replace Parts 50 or 52. Open to the reference SMR, and the most open to a performance-based safety case.	Risk-informed and performance-based. Uses a narrower DBA analysis under Subpart C, driven by probabilistic risk assessment, with alternative siting under Section 53.530.	Its risk basis rests on event frequencies and accident source terms, so it does not bound a deliberate, adaptive attacker. It also dropped the traditional aircraft-impact assessment — exactly the precise-strike and drone hazard class. And its option for higher-population siting raises the stakes without assessing them on adversarial grounds.
Proposed 10 CFR Part 57 — Licensing Requirements for Microreactors and Other Reactors with Comparable Risk Profiles	Proposed rule (published May 1, 2026; comments closed June 15, 2026). Not the reference-SMR path. Eligibility is set by consequence and fuel-mass limits — a risk-profile test, not a power rating — so it covers microreactors and other low-source-term designs. A commercial light-water module like the reference SMR falls outside that band.	Draws on Parts 50, 52, and 53 to allow manufacturing licenses, fleet approval, and remote or autonomous operation. No emergency planning zone is defined for eligible plants.	Relaxes the source term the furthest, which makes it the clearest example that an accident-side relaxation does not bound the adversarial side. Its autonomous-operation provisions also raise an AI-governance question, which this report answers through the design-basis posture in Section C.3.

Which pathway a given SMR uses depends on its own risk profile — the source term, the possible consequences, and the fuel mass that follow from the design, the same quantities the Section C analysis develops. The reference deployment, a commercial light-water power module, enters through Part 52. A genuinely low-consequence design could enter through the proposed Part 57. Part 53 is open to advanced reactors broadly. One gap, though, is common to every pathway. It is the through-line: the emergency-planning-zone and source-term basis for the SMR licensing case is an accident-side construct, and none of the pathways requires the adversarial design basis that would bound a deliberate threat. That is the gap Section C is built to fill — and supplying it before the license application is filed is what shortens the NRC review.

3. Institutional Coordination: the NRC and the Texas Grid Authorities

A Texas SMR sits on a jurisdictional seam that today's coordination rules do not fully close. FERC Order 706-B is the model for the handoff between NRC physical-security rules and the grid-reliability authority (NERC): it treats nuclear plants as bulk-power assets and lines up NERC reliability standards with the NRC cybersecurity rule. But ERCOT is an in-state grid run under the Texas Public Utility Commission, and FERC's reach over ERCOT is far more limited than over the interstate grids. For a Texas SMR, the grid authority is the Public Utility Commission and ERCOT, not FERC and NERC — and no NRC / Public-Utility-Commission framework like Order 706-B exists. An SMR run purely as the anchor of an island microgrid, with no tie to the bulk grid, would fall outside FERC's reach entirely.

A multi-module SMR campus sharpens the point. A six-module, 50-MWe campus that trips its passive safety systems in a single event drops about 300 MWe at once — inside an island ERCOT grid that lacks the frequency backstop the interstate ties provide. Whether ERCOT's contingency planning handles a simultaneous multi-module drop — rather than the single-large-unit trip the old rules were built around — is an open reliability question the deployment raises, and one the Texas grid authority needs to engage. There is a direct precedent on the load side of the same grid: NERC's May 2026 Level 3 Alert already tells planners to treat the sudden loss of large computing load (such as AI data centers) as a credible event. That is the mirror image of the concern here — a sudden loss of load rather than of generation — but it shows the planning rules must now account for exactly the kind of large, sudden, non-traditional event a multi-module SMR campus creates on the generation side.

4. Counter-Uncrewed-System Defeat Authority

The drone (UAS) threat in Section C.3 is one a commercial nuclear operator can detect and report but cannot legally defeat. Today's law gives the authority to track, jam, or destroy an intruding aircraft only to designated federal agencies such as Homeland Security and Defense — not to commercial nuclear operators. This is a legal gap, and it rests on physical-protection grounds, not on any one adversary: a drone over a nuclear plant's protected area is a 10 CFR Part 73 life-safety and security concern no matter who is flying it — a hostile state, a terrorist, a criminal, an activist, or a careless hobbyist. The threat does not depend on intent, and neither does the gap. What is needed is authority for nuclear operators to use active counter-drone tools under defined threat conditions — going beyond the state, local, territorial, and tribal authorities in the Safer Skies Act — modeled on the federal authority that already exists for other critical assets. Section D names this as the report's main legislative recommendation.

C. Topic Discussion

This section develops the four topics the statement of work requires. It moves from the grid-reliability case for SMRs in ERCOT (topic 1), through the ordinary (non-adversarial) accident characteristics an SMR must show for licensing (topic 2), into the adversarial design basis as a three-tier threat model (topic 3), and closes with how well existing passive-safety SMR designs hold up across that range (topic 4). As set in the Introduction, the three adversarial tiers are the core here; the nation-state military-action step above the highest tier is handled in the parent series (Appendix A), not in this report.

1. Grid Reliability and the Islanded-Mode Case

Texas has made a deliberate, funded commitment to advanced nuclear power. House Bill 14, effective September 1, 2025, created the Texas Advanced Nuclear Energy Office and the Texas Advanced Nuclear Development Fund, starting at $350 million — described by the State as the largest such commitment in the nation — with legal room to reach $2 billion. The fund pays out through reimbursement programs tied to the federal licensing milestones a project reaches: development and supply-chain support at the early-permit and application stage, and construction support once a project is under NRC review. In other words, the State has tied public money directly to the federal licensing path — the same path this report speeds up. So the licensingreadiness work here is not an abstract exercise; it bears directly on how fast money already set aside becomes power on the grid.

The grid case for that new power rests on three features of the ERCOT system that SMRs are well suited to provide.

Inertia deficit. ERCOT is its own synchronous grid, joined to its neighbors only by direct-current (HVDC) ties that carry scheduled power but not physical inertia. So ERCOT cannot borrow inertia from the Eastern or Western grids during a disturbance; that support has to come from inside ERCOT. As spinning fossil generators retire and wind and solar take their place — which lock to the grid's frequency but add no spinning mass — the system holds less inertia per unit of capacity, and its frequency swings more with sudden changes. Winter Storm Uri in February 2021 exposed the danger: a large, weather-driven loss of generation pushed frequency to the edge of collapse, stopped only by widespread blackouts. An SMR fleet supplies exactly what that event showed ERCOT was short of — spinning generation that steadies frequency against sudden shocks (see also NERC PRC-029-1).

Baseload gap. Wind and solar are now a large and growing share of ERCOT capacity, but both depend on the weather and cannot be called on at will. As steady fossil plants (large gas and coal) retire, the system needs firm, fuel-secure power that is there when renewables are not. SMRs supply that steady power with on-site fuel measured in years — not the limited hours of fuel supply that worsened the generation losses during Winter Storm Uri.

Islanded-mode operability. A near-term SMR campus can be set up as the anchor of a local or regional island grid. That role directly supports critical-infrastructure resilience, making the campus a mainstay for hospitals, nursing homes, emergency services, and other priority users that cannot ride out a long outage. Multiple modules help: a campus that can drop and restore power one module at a time can follow a shrinking or growing critical load smoothly, rather than in one big step.

One forward-looking grid trend matters to the threat discussion that follows. ERCOT is absorbing fast growth in large data-center load — single campuses of hundreds of megawatts to low gigawatts — against an interconnection queue ERCOT put at about 226 GW in late 2025, more than seventy percent of it data centers. Much of that queue is speculative and only a fraction will connect (only about 2 GW cleared to energize in the same period), but the near-term share is already large, and its key trait for reliability is that the workloads behind it can move out of ERCOT on short notice. A sudden, large compute migration drops load on a scale like a large generator trip — but it pushes frequency up rather than down. This is not hypothetical: since 2022 NERC has recorded several events, including in Texas, where more than 1,000 MW of computing load dropped off the grid within seconds, faster than operators could react. In May 2026 NERC raised this to a Level 3 Essential Action Alert, which now tells planners to treat a sudden loss of computing load as a credible event. The reliability point cuts both ways: losing generation pushes frequency down, losing load pushes it up, and the two together form a combined stress ERCOT's automatic protections were not built to manage as one coordinated event. It is noted here because it is one of the consequence paths the adversarial design basis must weigh.

2. Design Basis Accident Characteristics for SMR Licensing

The Design Basis Accident (DBA) is the foundation of nuclear safety analysis: the set of assumed events a plant must be designed and shown to withstand, and against which the safety systems are defined. For the large Texas reactors — South Texas Project and Comanche Peak — that envelope was built over decades under 10 CFR Part 50 and its General Design Criteria. For the near-term SMR it has not been issued in SMR-specific form, and the large-reactor envelope does not carry over cleanly, because the SMR's safety case rests on design features the large-reactor rules do not have. This section states the SMR accident characteristics that follow from those features, framed for NRC use as the baseline the adversarial analysis then builds on.

Three design features define the ordinary (non-adversarial) SMR envelope.

1. **The integral primary system:** by housing the core, pressurizer, and steam generators inside a single reactor vessel, the design removes most large primary piping — and with it the large-break loss-of-coolant accident that dominates the large-reactor design basis.
2. **Passive safety:** if all active cooling and outside power are lost, the design reaches and holds a safe shutdown on its own — carrying away decay heat by natural circulation and conduction, with no pumps, no AC power, and no operator action — for a licensed coping time on the order of seventy-two hours.
3. **The reduced source term:** the smaller core and integral layout produce a smaller assumed radioactive release, which is the technical basis for the smaller emergency planning zone (EPZ) certified for near-term designs.

This reference point is real, not hypothetical. The NRC certified the NuScale standard design as Appendix G to 10 CFR Part 52, effective February 2023 — a 50-MWe module, with up to twelve modules sharing one safety pool, for a maximum 600-MWe plant. The reference deployment here is a six-module, roughly 300-MWe campus from that certified design class, licensed through the Part 52 combined-license path that references the certified design. So the characteristics above are demonstrated properties of a design the NRC has already reviewed and certified. The point of this section is that those same properties — established for the accident case — are the starting point, not the finish line, of the adversarial analysis that follows, because an accident-side safety case does not by itself bound a deliberate attacker.

3. Adversarial Design Basis: The Three-Tier Threat Model

The characteristics above answer the questions the accident case was built for: equipment failure, natural hazard, and operator error. They do not answer the question a deliberate attacker poses. An attacker adapts, can target specific systems, and can act with persistence and with intent to deny access for repair, response, and recovery — none of which the accident case assumes. The smaller source term that justifies a smaller EPZ is credited for accidents; it does not bound an attacker who can break the barriers the accident case assumes stay intact. The adversarial design basis here fills that gap across three man-made threats — cyber, physical, and drone (UAS) — at three rising threat levels.

The three tiers, as defined for this analysis, are:

Tier 1 — Low Threat. Cyber threats are present everywhere. The drone threat from off-the-shelf platforms is present. A direct physical attack is not a credible near-term risk at this tier.

Tier 2 — Elevated Threat. There are detectable signs of cyber attackers getting into position, and a physical attack that is possible but not imminent. The threats are more precise, and their ability to deny access is more credible than at Tier 1.

Tier 3 — High Threat. A near-term terrorist attack is highly likely. All three threats — cyber, physical, and drone — apply at their worst credible level.

These tiers are built around sub-nation-state adversaries: the top tier is a near-term domestic or international terrorist attack — the threat class the 10 CFR Part 73 physical-protection rules are already built around. As set in the applicability determination, the reference SMR on the Texas Gulf Coast sits at Tier 1: cyber and commercial-drone threats are present regardless of location, while a direct physical attack is not a credible near-term risk there. The nation-state military attack that would sit above Tier 3 is judged not to apply here and is handled in the parent series (Appendix A). What follows describes each threat as it rises across the three tiers.

Cyber

The cyber threat is range-independent: an attacker over the network is not limited by where the plant sits, which is why it is present at Tier 1 whatever the location. It rises across the tiers through greater access and coordination, not proximity — from commodity break-in attempts against the business and operational networks at Tier 1, through detectable positioning and supply-chain or credential spoofing at Tier 2, to a coordinated attempt that assumes a prior foothold, possibly with insider help, timed with a physical attack at Tier 3. The controlling defense at every tier is architectural: the safety-critical functions are fully walled off from — and cannot be reached through — the operational network an attacker can touch.

Physical

The physical threat is the one most tied to location, and therefore the one the Tier 1 setting most reduces for this SMR. Where it is credible, its damage path runs through the shared above-ground equipment that the below-ground safety modules do not protect — the switchyard, the grid connection point, and the cooling-water intake — because a precise strike there can trip the reactor and cut the island grid without ever challenging the radioactive containment. It rises from no credible near-term attack at Tier 1; through a possible but non-imminent precise threat at Tier 2 that warrants hardening the shared above-ground plant; to a worst-case precise strike, possibly with insider help, at Tier 3 against that same shared above-ground equipment.

Uncrewed Aircraft Systems (UAS)

The drone threat, like the cyber threat, is present at Tier 1 regardless of location, because off-the-shelf platforms are widely available and need no adversary near the site. It rises from small-platform overflight and surveillance at Tier 1; through more capable, payload-credible platforms showing denial behavior at Tier 2; to coordinated, possibly multi-drone use at worst-case payload at Tier 3. The drone threat is treated throughout as a 10 CFR Part 73 physical-protection and life-safety matter: a drone over the protected area is a hazard to detect and stop whoever is flying it. The one thing today's law does not give a commercial operator — authority to defeat it — is flagged in the Gap Assessment and revisited in the Way Forward.

The three threats and three tiers combine as follows:

Threat	Tier 1 — Low	Tier 2 — Elevated	Tier 3 — High
Cyber	Commodity break-in attempts against business/operational networks; safety layer out of reach. Baseline separation and monitoring are enough.	Detectable positioning; supply-chain and credential staging. Step up monitoring and integrity checks.	Coordinated cyber-plus-physical attempt at worst severity, assuming a prior foothold. Separation of the deterministic safety layer is the controlling defense.

Threat	Tier 1 — Low	Tier 2 — Elevated	Tier 3 — High
Physical	No credible near-term physical attack. Part 73 perimeter baseline.	Possible, non-imminent precise threat to shared above-ground equipment (switchyard, grid connection point, intake). Hardening is warranted.	Worst-case precise strike on shared above-ground equipment. Hardening that equipment is the controlling measure.
Drone (UAS)	Small commercial drones overflying and watching the site, present anywhere. Detect and report under Part 73.	More capable, payload-credible drones showing denial behavior. Detect and move to mitigation.	Coordinated drones at worst credible severity. Passive standoff barriers over above-ground safety equipment; active defeat capability also needed (a gap in the law).

The digital instrumentation-and-control (I&C) system behind these claims rests on a strict separation by function. Backup power to the I&C — an independent battery or UPS — is sized to a set coping time, long enough to reach safe passive shutdown but not to run indefinitely. After that window, safety is held by passive features that need no power at all. The safety-critical layer — the protection and passive-actuation functions the safety case depends on — is built in logic that is deterministic, self-contained, fail-safe, and fully verifiable across every credible input, and it is physically and logically separated from the operational layer and from any shared part an attacker could reach. This is the same separation the electric sector calls its Physical and Electronic Security Perimeters; here it rests on the NRC's own I&C independence and cybersecurity rules (IEEE 603; 10 CFR 73.54), under the same NRC/NERC boundary that FERC Order 706-B draws. That separation is what makes the cyber tier tractable: a cyber break-in on the operational layer cannot reach the protection functions, because those functions neither depend on that layer nor can be reached from it. What qualifies a function for the safety path is determinism and verifiability — the same bar a reactor protection system already meets. A function built with machine learning is allowed on those same terms: reduced to a fixed, fully specified artifact whose complete input-output behavior is checked against the safety spec, with no online or adaptive learning and no inference that cannot be proven. Qualified that way, it is no longer machine learning that learns while running, but verified deterministic safety logic that happens to have a machine-learning origin. What the safety envelope shuts out is a property, not a technology: adaptive or online learning, whose behavior changes after qualification and defeats the verification; inference that cannot be verified; and generative AI, whose non-deterministic output cannot be checked against a repeatable spec. The adversarial frame sharpens this line rather than softening it, because determinism and formal verification are exactly what bound a function under the rare and adversarial inputs an attacker would force — the very conditions under which an opaque model is least trustworthy.

Two engineering consequences follow.

1. Where machine learning supports mission continuity or optimization but does not meet the safety bar, it is allowed only in a non-safety role, under a conservative rule: any output that could influence a physical action is held to the safe side of the operating envelope and cannot widen it.
2. And even where a learned function could qualify for the safety path, safety practice favors the simplest provable version. A fixed learned artifact usually carries more complexity — and a larger verification and common-cause-failure surface — than the function needs, so the conservative choice is usually the simpler deterministic one.

This posture is not added after the fact; it is a design-basis property, provable at licensing review. It is what lets the SMR passive-safety argument in the next section hold under the combined-threat tiers, not just under the ordinary accident envelope.

4. Passive-Safety Adequacy Across the Threat Spectrum

The conclusion here is deliberately bounded, not a blanket claim of sufficiency, because the bounded claim is the one that survives expert and regulatory challenge. Passive safety decisively settles the decay-heat and loss-of-cooling problems that dominate the ordinary envelope, and it raises the effort an attacker needs across most threats by removing the active systems an attacker would target. The honest reading across the three tiers is this: the reference SMR is adequate as designed at the Low and Elevated tiers (Tiers 1 and 2), and it carries a bounded residual risk at the High tier (Tier 3). That residual risk comes from an attacker’s persistence and denial of access — a sustained loss of access that outlasts the passive coping margin, or a strike on shared equipment that cuts the island while the reactor stays safely shut down. The risk is real, but it is closed by a small, defined set of changes, not by any reactor redesign.

Four changes close the High-tier residual risk. None is a new reactor-physics requirement.

a. Shared above-ground equipment — switchyard, grid connection point, and cooling-water intake — must be hardened to the same storm-surge and wind standard the below-ground reactor modules already meet, and, against drones, fitted with passive standoff barriers over those parts. That barrier is available today (from the DBA-UxS cross-sector work, §8.2) and needs no power, operator action, or defeat authority — so neither a storm nor a precise strike can trip the reactor and cut the island through the one unhardened path.

b. The campus I&C system must apply the separation and diversity described above at the campus level, with the safety layer clearly independent of the operational layer and of any shared part an attacker could pre-position within (see, for example, CISA's CI Fortify guidance on isolating vital systems, 2026). This is the single most important change, because the community life-safety mission rests on it.

c. Bridge power — right-sized hospital backup generation or a second anchor — must be provided to carry life-safety loads across the gap between a protective shutdown and the return of normal power.

d. Active counter-drone authority must be available to the operator under defined threat conditions. This needs a change in law, because commercial nuclear operators, like all private operators, lack defeat authority today.

Each of these is an integration, hardening, provisioning, or authority step aimed at a specific residual risk the analysis names — not a change to the reactor's safety physics. That is the heart of the topic-4 claim: passive-safety SMR designs are already adequate at the Low and Elevated tiers and need only small, well-defined changes to close the bounded High-tier residual. The reactor's protected-shutdown envelope stays inviolate at all times and is never traded for availability; what the changes protect is the community resilience mission that sits outside that envelope. The faster-licensing case in Section D rests on this result: a developed adversarial design basis, supplied before any specific application, replaces first-of-a-kind analysis with review of an existing framework.

D. Way Forward

The analysis converts directly into a path forward. Its core contribution — a developed Design Basis Accident for the near-term SMR that spans both the accident envelope and the adversarial threat tiers — is supplied before any specific license application precisely so it can shorten the review that would otherwise have to build it. This section states the faster-licensing case and the recommendations the Gap Assessment supports.

1. The Expedited-Licensing Case

The value of a developed Design Basis Accident supplied ahead of the application is that the applicant and the NRC review an existing framework instead of doing a first-of-a-kind analysis. For the Part 52 combined-license path the near-term SMR uses, the adversarial design basis here can be folded into the application as a referenceable element, or set up through a generic communication that several SMR applicants can cite. Either route replaces per-application development of the threat case with review of a shared framework — and that is where NRC review time is saved. The risk-informed Part 53 path, now in effect, fits a framework like this even better, because it is built to credit a developed, performance-based safety case rather than re-derive a prescriptive one.

For Texas, the benefit is direct — and it is why the State funded the path. The Texas Advanced Nuclear Development Fund pays out against the federal licensing milestones a project reaches, so shortening NRC review turns set-aside state money into power on the grid sooner. That power is what ERCOT needs most and increasingly lacks: steady, fuel-secure generation with the spinning inertia that steadies grid frequency, available when wind and solar are not, and able to form a regional island grid for community resilience. A faster, better-assured licensing path is therefore not just an administrative convenience — it is how the State's nuclear investment reaches the grid in time to matter.

2. Recommendations

Four recommendations follow from the gaps this report identifies. Each names the party positioned to act.

a) **To the NRC, with Nuclear Energy Institute support.** Adopt the SMR adversarial design basis as a referenceable licensing element — folded into the combined-license application, or into the proposed Part 57 application for a low-consequence design, or set by generic communication — so the cyber, physical, and drone threat tiers are assessed once, as a shared framework, rather than rebuilt for each application. This is the action that most directly speeds NRC review.

b) **To Congress.** Enact authority for commercial nuclear operators to use active counter-drone tools under defined threat conditions, on 10 CFR Part 73 physical-protection grounds, modeled on the federal authority that already exists for designated assets. Because airspace and counter-drone authority are federal, this is the one gap an operator cannot close on its own and no licensing action can supply. It is the report's main legislative recommendation.

c) **To the NRC, the Texas grid authorities (the Public Utility Commission and ERCOT), and the Texas Advanced Nuclear Energy Office.** Set up the NRC / Public-Utility-Commission coordination framework that the in-state ERCOT grid needs and that FERC Order 706-B does not supply, and study the multi-module SMR simultaneous-shutdown event — a drop of about 300 MWe in a single sequence — within ERCOT's reliability planning.

d) **To the SMR developer and operator.** Make the small set of changes that close the High-tier residual risk: harden the shared above-ground equipment — switchyard, grid connection point, and cooling-water intake — to the storm-surge and wind standard the below-ground modules already meet, and add passive standoff barriers over those parts against drones (DBA-UxS §8.2), a measure available now without defeat authority; separate the campus I&C network so the safety layer is independent of the operational layer; and provide bridge power to carry life-safety loads between a protective shutdown and the return of normal power. None of these is a new reactor-physics requirement.

Taken together, these steps make the case the report set out to support. Passive-safety SMR designs are adequate to the credible adversarial threat range at the Low and Elevated tiers, and, with small, well-defined changes, at the High tier. A developed Design Basis Accident, supplied before the application, is the tool that shows that adequacy to the NRC quickly rather than slowly. For a Texas committed by law and by capital to leading the nuclear renaissance, the result is a faster, better-assured path to the firm, resilient power the grid needs — for the benefit of all Texans.

E. References, Bibliography, and Appendices

The references and supporting sources cited throughout this report are provided in the appendix that follows. Appendix A consolidates the NRC and IAEA regulatory instruments, the hospital backup-power and ERCOT grid-reliability record, the SMR design and passive-safety documentation, and the counter-uncrewed-system statutory references on which the analysis draws.

Appendix A — References and Bibliography

NRC Regulatory Instruments Governing SMR Design Certification, Combined Licensing, Physical Security, And Cyber Security

- NRC 10 CFR Part 50 — Domestic Licensing of Production and Utilization Facilities
- NRC 10 CFR Part 52: Licenses, Certifications, and Approvals for Nuclear Power Plants (combined license and design certification)
- NRC 10 CFR Part 53: Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants. Final rule, 91 Fed. Reg. 15696 (Mar. 30, 2026); effective April 29, 2026.
- Proposed NRC 10 CFR Part 57: Licensing Requirements for Microreactors and Other Reactors with Comparable Risk Profiles. Proposed rule, 91 Fed. Reg. (May 1, 2026); comment period closed June 15, 2026. (Included as the adjacent microreactor framework; not the licensing pathway for the reference SMR.)
- NRC 10 CFR Part 73: Subpart F (§§73.40–73.55) Physical Protection of Plants and Materials
- NRC 10 CFR §73.54: Protection of digital computer and communication systems and networks (Cybersecurity)

IAEA Safety Standards On Design-Basis And Beyond-Design-Basis Assessment

- INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

- INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA, Vienna (2011).
- Roxey, T.E. (2026). "DBA-MA IAEA Framework (L1, v1.7) — Design Basis Expansion for Nuclear Power Plants Considering Acts of War: International Framework." https://drive.google.com/file/d/1VuPjcN9bln--Ly9Cza9Rmm6A0BAfE_F_/view
- Roxey, T.E. (2026). Military Action Applicability Framework (DBA-MA-AF), Version 0.2. Shared applicability module of the Design Basis Accident — Military Action (DBA-MA) series: four-filter applicability gate (§2) and applicability determination (§3).

Gulf Coast And Comparable Hospital Backup-Power Failure Record

Hurricane Katrina – Memorial Medical Center (New Orleans)	Fink, S. (2009, August 25). Strained by Katrina, a hospital faced deadly choices. The New York Times. Louisiana State University. (2016, July 5). Dead in the Water. Journal of Energy Law and Resources University at Buffalo, Multidisciplinary Center for Earthquake Engineering Research. (2006). Hospital Decision Making in the Wake of Katrina (MCEER Special Publication 06-SP01).
Hurricane Ike – University of Texas Medical Branch at Galveston (UTMB)	Federal Emergency Management Agency (FEMA), *Mitigation Assessment Team Report: Hurricane Ike in Texas and Louisiana*. (2009). The University of Texas Medical Branch. *Hurricane Ike Recovery Information*. (2008).
Hurricane Sandy – NYU Langone Medical Center (New York)	Hartocollis, A. (2012, November 1). With power out, hospitals choose to stay put or to evacuate. The New York Times. Federal Emergency Management Agency. (2013). *Hurricane Sandy FEMA After-Action Report*. FEMA.

Hurricane Harvey – Houston-area facilities	U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER). *Hurricane Harvey Situation Reports*. (2017). Federal Emergency Management Agency. *Texas Hurricane Harvey (DR-4332-TX) After-Action Reports*. (2017).
Hurricane Beryl – Houston regional outages	U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER). *Hurricane Beryl Situation Reports*. (2024). National Oceanic and Atmospheric Administration (NOAA). *Hurricane Beryl Brings Massive Power Outages to East Texas*. (2024, July 15). CenterPoint Energy. *Hurricane Beryl Restoration Updates*. (2024). Texas Public Utility Commission investigative report on CenterPoint Energy's Hurricane Beryl response (reported by The Texas Tribune). (2024).

ERCOT Grid-Reliability Reports Including The Winter Storm Uri After-Action Analyses

- Electric Reliability Council of Texas. (2021). Review of February 2021 extreme cold weather event. ERCOT.
- Electric Reliability Council of Texas. (2021). 2021 Long-Term System Assessment. ERCOT.
- Electric Reliability Council of Texas. (2021). Seasonal Assessment of Resource Adequacy (SARA): Summer 2021. ERCOT.
- Electric Reliability Council of Texas. (2022). 2022 Long-Term System Assessment. ERCOT.
- Electric Reliability Council of Texas. (2022). Seasonal Assessment of Resource Adequacy (SARA): Summer 2022. ERCOT.
- Electric Reliability Council of Texas. (2023). 2023 Long-Term System Assessment. ERCOT.

- Electric Reliability Council of Texas. (2023). Seasonal Assessment of Resource Adequacy (SARA): Summer 2023. ERCOT.
- Electric Reliability Council of Texas. (2024). 2024 Long-Term System Assessment. ERCOT.
- Electric Reliability Council of Texas. (2024). Seasonal Assessment of Resource Adequacy (SARA): Summer 2024. ERCOT.
- Electric Reliability Council of Texas. (2025). 2025 State of the Grid report. ERCOT.
- Electric Reliability Council of Texas. (2025). Seasonal Assessment of Resource Adequacy (SARA): Summer 2025. ERCOT.
- Electric Reliability Council of Texas. (2026). Post-event report: Winter Storm Fern (January 2026). ERCOT.

NERC Bulk-Power-System Reliability Guidance On Large Computational Loads

- North American Electric Reliability Corporation. (2026). Essential action to industry: Computational load modeling, studies, instrumentation, commissioning, operations, protection, and control [Level 3 NERC Alert]. NERC. https://www.nerc.com/globalassets/programs/bpsa/alerts/level-3-computational-load-alert.pdf

Near-Term Integral LWR SMR Design And (2026).Passive-Safety Documentation

- Cyber and Infrastructure Security Agency (CISA) -- CI Fortify — Advice for isolating vital systems (2026).
- International Atomic Energy Agency – *Advances in Small Modular Reactor Technology Developments: A Supplement to IAEA Advanced Reactors Information System (ARIS) (2024).
- SMR Regulators' Forum – Working Group on Design and Safety Assessment: Phase 2 Report. (2021). Working Group on Design and Safety Assessment: Phase 2 report. International Atomic Energy Agency.
- U.S. Nuclear Regulatory Commission – NuScale Design Certification. (2023). NuScale small modular reactor design certification: Final rule. Federal Register, 88(12), 3287–3311.
- U.S. Nuclear Regulatory Commission – NuScale US600 Design Certification. (2023). Design certification—NuScale US600. U.S. Nuclear Regulatory Commission.
- Welter, K., Reyes, J. N., & Youngblood, R. (2023). Unique safety features and licensing requirements of the NuScale small modular reactor. Frontiers in Energy Research, 11, Article 1160150.

- U.S. Department of Energy – Advanced Small Modular Reactors. (2025). Advanced Small Modular Reactors (SMRs). U.S. Department of Energy, Office of Nuclear Energy.

Counter-Uncrewed-System Statutory Airspace References and Authorities

- U.S. Department of Defense, Uncrewed Systems Integrated Roadmap, Office of the Under Secretary of Defense for Research and Engineering (current edition).
- DBA-MA-UxS-NA (v1.0) — Nuclear Implementation Annex: Uncrewed Systems Threat Considerations for Nuclear Facilities.
- Congress. (2025). SAFER SKIES Act, National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, tit. LXXXVI §§ 8601–8607, codified at 6 U.S.C. § 124n—Protection of certain facilities and assets from unmanned aircraft. United States Code. https://uscode.house.gov/view.xhtml?req=(title:6+section:124n+edition:prelim)
- Congress. (2025). 10 U.S.C. § 130i—Protection of certain facilities and assets from unmanned aircraft. United States Code. https://www.law.cornell.edu/uscode/text/10/130i
- Congress. (2025). 49 U.S.C. Subtitle VII—Aviation Programs. United States Code. https://uscode.house.gov/
- Congress. (2025). 49 U.S.C. § 44809—Exception for limited recreational operations of unmanned aircraft. United States Code.
- Congress. (2025). 49 U.S.C. §§ 44801–44835—Unmanned Aircraft Systems. United States Code.
- Congress. (2025). 18 U.S.C. § 32—Destruction of aircraft or aircraft facilities. United States Code.
- Congress. (2025). 18 U.S.C. § 1030—Fraud and related activity in connection with computers. United States Code.
- Congress. (2025). 18 U.S.C. § 1367—Interference with the operation of a satellite. United States Code.
- Congress. (2025). 18 U.S.C. Chapter 119—Wire and Electronic Communications Interception and Interception of Oral Communications. United States Code.
- Congress. (2025). 18 U.S.C. Chapter 206—Pen Registers and Trap and Trace Devices. United States Code.
- Federal Aviation Administration. (2024). 14 CFR Part 89—Remote Identification of Unmanned Aircraft. U.S. Department of Transportation.
- Federal Aviation Administration. (2024). 14 CFR Part 107—Small Unmanned Aircraft Systems. U.S. Department of Transportation.
- Federal Aviation Administration. (2024). 14 CFR Part 91—General Operating and Flight Rules. U.S. Department of Transportation.
- Federal Aviation Administration. (2023). UAS Detection, Mitigation, and Response at Airports. https://www.faa.gov/airports/new_entrants/uas_detection_mitigation_response
- Federal Aviation Administration. (2025). Counter-UAS (C-UAS). https://www.faa.gov/uas/resources/c_uas

Author Biographies

Dr. Michael Cohen is President of Raise Up LLC and Adjunct Professor at the University of Minnesota, where he teaches graduate students about the benefits, risks, and protection of nuclear power in U.S. critical infrastructure. A former Energy and Nuclear Sector liaison to the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security, he holds two U.S. patents on making GPS signals more resistant to denial, jamming, and spoofing. He is the National Sector Chief of InfraGard's Nuclear Sector. He previously served as a nuclear-power subject-matter expert for the Office of the Nuclear Sector-Specific Agency and as liaison to the DHS Nuclear Sector Coordinating Council, for which he received a certificate of appreciation. He also led the FEMA prime-contractor team that developed and field-tested the Federal Radiological Response Plan, and he designed the TRANSCOM radioactive-waste transportation system in Carlsbad, New Mexico. His current work applies AI to defending critical infrastructure against physical, cyber, and insider threats.

Tim Roxey is President of Eclectic Technologies. He retired from the North American Electric Reliability Corporation (NERC) as Vice President and Chief Security Officer, responsible for the cybersecurity of the North American bulk power system. Earlier he served as Technical Assistant to the Chair of the DHS Nuclear Sector Coordinating Council and as Technical Assistant, Security to the Vice Chair of Constellation Energy. He holds a Master of Science in Nuclear Engineering Sciences and brings fifty years of experience across the nuclear and electric sectors — the intersection this report addresses. He is a recipient of the SANS Institute Lifetime Achievement Award. His current work extends established nuclear-safety design-basis methods to protecting critical infrastructure against deliberate and adversarial threats — the framework behind this report.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Cohen, M., Roxey, T. (2026). Protection Guidance for the Layman to Accelerate the Licensing and Deployment of Small Modular Reactors into the Texas Grid (ERCOT). (Report No. 2026-1050). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/HSJYD

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY