

Integrating Industrial Control System (ICS/OT) Cybersecurity and Geospatial Reasoning into Power Systems Engineering Education: A Design-Based Framework for Scenario-Driven Learning

Amirhossein Rezaeian

Master's Student, Engineering Education | Department of Engineering Sciences | University of Tehran, Tehran, Iran

ORCID: 0009-0009-4398-1703

Email: rezaeian.develop@gmail.com | Website: <https://autorz.ir/>

Abstract

The electric power engineer of the next decade will increasingly work with systems whose electrical, digital, operational, and geographic states are interdependent. Yet these dimensions are still commonly taught in separate curricular spaces: power-system analysis emphasizes electrical state, cybersecurity courses emphasize information and network security, and geographic information system (GIS) activities often remain disconnected from the electrical engineering decision process. This separation creates a pedagogical problem rather than simply a content gap: students may learn the components of a modern grid without learning how evidence from one representation constrains decisions in the others. This paper develops GeoCyberTwin-PS, a design-based framework for integrating power-system simulation, GIS/spatial analysis, and industrial control system/operational technology (ICS/OT) cybersecurity into scenario-driven power engineering education. The framework is derived from a structured integrative synthesis of recent engineering-education literature, OT-security guidance, cyber-informed engineering curriculum guidance, and technical work on geospatial-power-system data mapping. The synthesis identifies five recurring needs: authentic cross-layer problems, hands-on or simulation-mediated experience, explicit systems reasoning, evidence-based assessment, and safe separation of educational cyber exercises from operational environments. GeoCyberTwin-PS operationalizes these requirements through a four-layer architecture, a competency model, a reusable scenario grammar, a 12-week curriculum, and a transfer-oriented assessment protocol. The paper does not report fabricated classroom results; instead, it defines research propositions and an evaluation design specified in sufficient detail for future pre-registration for future empirical testing. The contribution is therefore not a claim that the proposed framework is already effective, but a testable educational architecture that makes the interaction among electrical state, spatial context, and OT cyber risk visible and assessable.

Index Terms—power systems engineering education; cybersecurity education; operational technology; industrial control systems; geographic information systems; geospatial reasoning; cyber-physical systems; digital twins; systems thinking; project-based learning; engineering curriculum

Highlights

- Integrates power-system simulation, GIS, and ICS/OT cybersecurity in one learning architecture.
- Treats spatial context as an engineering reasoning layer rather than a visualization add-on.
- Maps cross-layer competencies to observable evidence and contemporary engineering outcomes.
- Provides a reusable scenario grammar and a reproducible 12-week implementation blueprint.
- Defines an empirical evaluation plan without inventing student data or learning effects.

1. Introduction

The modernization of electric power systems has altered not only the technologies used by engineers but also the kinds of reasoning that professional practice requires. Contemporary substations and distribution systems increasingly depend on digital protection, communications, supervisory control, remote terminal units (RTUs), intelligent electronic devices (IEDs), distributed energy resources (DERs), automated switching, and software-mediated operational workflows. These changes create a cyber-physical system in which a disturbance can propagate across electrical, computational, communication, and organizational boundaries. NIST's OT security guidance explicitly frames operational technology as systems that interact directly with the physical environment and emphasizes performance, reliability, and safety constraints alongside cybersecurity [1]. The implication for education is substantial: engineers need more than generic cybersecurity awareness; they need the ability to interpret cyber risk in the same physical and operational language used to analyze the grid.

Power engineering education has a strong tradition of simulation and laboratory learning. Interactive power-system simulators, virtual laboratories, and real-time distribution simulation have been used to expose students to load flow, protection, operations, and control-room decisions without requiring every learner to access a utility-scale physical facility [22-26]. More recent work has extended this trajectory through digital twins, immersive substation simulation, and project-based learning [17-20,34]. At the same time, smart-grid cybersecurity education has developed its own hands-on traditions, including modular training platforms, remote industrial laboratories, and testbeds [9-15,42]. These literatures are valuable, but they are still largely organized around one dominant representation at a time: the electrical model, the cyber range, or the industrial-control laboratory.

A parallel development is the growing use of geospatial data in power-system research. Recent technical studies demonstrate that linking electrical network models with geospatial representations is non-trivial because data are often created asynchronously, use inconsistent identifiers, and encode different notions of topology and location [27,28]. Yet this difficulty is educationally productive. The actual engineering question in resilience and restoration is rarely simply "Which bus is connected to which line?" It is often "Which geographically situated asset matters most under a given hazard, communication constraint, or service priority, and what evidence supports that judgment?" GIS can make that reasoning explicit.

The missing link is therefore pedagogical integration. Existing work suggests that active learning, systems thinking, project-based learning, and experiential environments can support deeper engineering reasoning [30-38]. Recent cyber-informed engineering guidance goes further by arguing that digital risk should be considered throughout the engineering life cycle rather than treated as a specialist add-on [6]. For power engineering education, this principle suggests a new design opportunity: cybersecurity can be taught through engineering consequences, while GIS can be used to expose the spatial context in which those consequences occur.

This paper proposes GeoCyberTwin-PS, a design-based educational framework that synchronizes three representations of the same engineered system: (1) a power-system state model, (2) a geospatial context model, and (3) an OT/cyber model. The framework is intentionally technology-neutral. Its purpose is not to prescribe one simulator, GIS package, or cybersecurity platform, but to define the instructional relationships that must remain stable when the underlying software changes. The resulting learning activities are scenario-driven: students establish a baseline operating state, inspect spatial context, interpret cyber/OT evidence, trace a plausible causal chain, estimate consequences, and defend a mitigation decision.

1.1. Research questions and contribution

RQ1. Which cross-domain competencies become visible when power-system engineering, spatial analysis, and OT cybersecurity are designed as one learning problem?

RQ2. How can these competencies be embedded in a power-engineering curriculum without reducing the course to a survey of disconnected technologies?

RQ3. What scenario structure can help students trace a cyber event from geographically situated assets to electrical or operational consequences?

RQ4. How should learning and transfer be assessed so that a future empirical study can distinguish tool proficiency from systems reasoning?

The paper makes four principal contributions. First, it synthesizes a research base that spans engineering education, power-system laboratories, OT cybersecurity education, GIS-power-system integration, and cyber-informed engineering. Second, it proposes an explicit architecture and competency model for their intersection. Third, it supplies a reusable curriculum and scenario grammar that can be implemented at different resource levels. Fourth, it specifies a future empirical validation protocol so that the framework can move from a conceptual proposal toward design-based research with measurable outcomes. The manuscript deliberately does not report unobserved educational effects.

2. Literature review and research gap

2.1. Power systems engineering education: from calculation to operational reasoning

Traditional power-system education is effective at teaching mathematical and physical foundations, but the contemporary engineering task increasingly involves operational judgment across software-supported environments. Allen et al. demonstrated early use of interactive object-oriented simulation for power-system education, illustrating the value of graphical and computational experimentation for complex network phenomena [26]. Shahnian et al. later described practical and computer-based activities that complemented lectures in power-system protection, emphasizing motivation and application-oriented learning [24]. Mohamed et al. demonstrated a simplified virtual power-system laboratory designed to support distance learning and ABET-oriented outcomes [23]. More recently, Anderson et al. used real-time distribution simulation and application development to expose students to control-room-like decision environments and open-source power-system software [22].

These studies establish three design propositions relevant to GeoCyberTwin-PS. First, simulation is most educationally valuable when students make engineering decisions rather than simply observe plots. Second, virtual and remote environments can expand access when physical laboratories are scarce. Third, laboratory authenticity is not solely a function of physical hardware; it also depends on the fidelity of the decision context. The recent virtual-substation work by Li et al., for example, explicitly links structural understanding, operational drills, spatial comprehension, and collaborative practice in a multimodal training environment [20].

The limitation is that these power-system education studies do not, as a group, make cyber risk and geospatial evidence coequal objects of reasoning. A student may learn to calculate a fault current, operate a simulated substation, or identify a relay event without being asked to determine how a malicious telemetry condition, the location of a critical load, and a restoration constraint jointly affect the engineering decision.

2.2. Cybersecurity and OT education: authentic environments and the IT/OT boundary

The educational literature on ICS and OT cybersecurity consistently emphasizes the difficulty of teaching security without understanding the controlled process. Yardley et al. developed a modular smart-grid cybersecurity education platform around active learning, project-based learning, and learning-by-doing [10]. Del

Canto et al. presented a remote laboratory in which learners interacted with industrial equipment and practiced vulnerability analysis in a safe environment [11]. Domínguez et al. described a laboratory using real control equipment to bridge the knowledge gap between control-system specialists and cybersecurity practitioners [12]. Later work on remote training reported positive learner perceptions while also noting the importance of platform design and instructional scaffolding [13]. Hands-on industrial cybersecurity training for a multidisciplinary master's program similarly found value in practical exposure while emphasizing the need to calibrate difficulty and support to student confidence [42].

At a broader level, Francia et al. argued that pedagogical resources for ICS security must be deliberately designed, conveyed, and evaluated rather than assembled as an ad hoc collection of attack demonstrations [15]. Torgersen et al.'s 2025 scoping review is especially relevant: across 132 included studies, only a subset focused explicitly on OT, while the literature used testbeds, simulations, digital twins, and related environments in varied ways and did not consistently apply performance measures [8]. This finding strengthens the case for assessment models that evaluate observable cross-domain performance rather than self-reported confidence alone.

The implication for power engineering is that OT cybersecurity should be taught in operational language. Students should learn to distinguish a vulnerability from an attack path, an attack path from a physical consequence, and a security control from a safe engineering response. NIST SP 800-82 Rev. 3, IEC 62443-2-1:2024, MITRE ATT&CK for ICS, and CISA's Cybersecurity Performance Goals provide complementary vocabularies for this purpose [1-5]. In an educational environment, these should not be treated as compliance checklists; they should become structured prompts for reasoning about zones, assets, dependencies, evidence, and mitigations.

2.3. Digital twins and simulation-mediated learning

Digital twins have become an increasingly visible educational technology because they allow engineering learners to interact with dynamic representations of systems that may be expensive, hazardous, or inaccessible in physical form. Kotecha et al.'s systematized review identified recurring themes around theory-practice connections, remote/hybrid learning, learning experience, and cross-disciplinary collaboration, while also emphasizing infrastructure and faculty-development barriers [17]. Blackwell and Rocke's domain-focused review of digital twins in undergraduate control engineering similarly identified opportunities for service-rich, learning-theory-informed digital-twin design but noted the scarcity of education-focused evidence [18]. Speicher et al. provided a recent experiential case in which learners combined digital twins, data collection, and decision-making in an industrial setting [19]. A 2026 quasi-experimental study also examined project-based learning supported by digital twins, underscoring the need for empirical evaluation instead of relying on technology novelty as a proxy for educational value [34].

For GeoCyberTwin-PS, the term digital twin is used in a constrained instructional sense. A simple static power-flow model is not automatically a digital twin. The proposed learning environment becomes twin-like when the electrical, spatial, and OT representations share stable identities and are synchronized at the scenario level. This distinction is important because educational value depends less on the label than on whether learners can move coherently between representations of the same state.

2.4. GIS and spatial reasoning in engineering

GIS has a long history in engineering education, where the pedagogical value of spatial reasoning and hands-on analysis has been documented since at least the late 1990s [29]. In the power domain, geospatial mapping is not merely a visualization task. Li et al. showed that connecting power-system model elements with geospatial data requires explicit data-mapping workflows because electrical and GIS representations are often built for different purposes and contain

heterogeneous identifiers [27]. Salbanya et al. recently demonstrated how harmonized distribution-network geospatial data can support network, resilience, and community-level analysis at regional scale [28].

These developments suggest that GIS can function as a cognitive artifact. A student who marks a substation as "critical" should be able to defend that classification using observable spatial and electrical evidence: the location of critical customers, road accessibility, hazard exposure, communication dependencies, network centrality, redundancy, or restoration constraints. Such tasks require interpretation rather than button-clicking. They also create opportunities for uncertainty management, since spatial datasets are incomplete and may not align perfectly with electrical models.

2.5. Systems thinking, active learning, and project-based learning

Systems thinking is a strong theoretical fit because the instructional challenge is explicitly about interactions and boundaries. Monat et al. argue that systems thinking should be integrated into undergraduate engineering education rather than isolated in a specialist course [30]. Azad and Moore's work with engineering students similarly illustrates how system mapping can help learners explore ambiguous and wicked problem spaces [31]. Freeman et al.'s meta-analysis across STEM courses provides broader evidence that active-learning approaches improve performance relative to traditional lecturing, while Prince's review provides a foundational engineering-education synthesis of active learning [36,37].

Project-based learning adds a structure for sustained decision-making. Recent reviews report that PBL in engineering education can support technical and non-technical competencies, particularly when students work with realistic problems, simulation, interdisciplinary content, and assessment aligned to project goals [32,33]. The 2026 quasi-experimental digital-twin study further illustrates why empirical testing is preferable to assuming that technology automatically improves learning [34]. For GeoCyberTwin-PS, PBL is not an end in itself. The project structure is used to create repeated cycles of modeling, diagnosis, evidence integration, decision, and reflection.

Constructive alignment provides the design discipline needed to avoid technology-driven curriculum inflation. Biggs' formulation links learning objectives, learning activities, and assessment so that each part of the course points toward the same level of performance [35]. In the present framework, the objective is not "learn GIS" or "learn cybersecurity" as isolated tool competencies. Instead, a higher-level objective is to explain and defend an engineering decision using consistent evidence across electrical, spatial, and OT representations.

2.6. Synthesis of the research gap

TABLE I summarizes the most relevant evidence streams. The gap is not that no prior study combines technologies. Rather, the gap is the absence of a clearly specified, power-engineering educational architecture in which GIS, OT cybersecurity, and power-system state are intentionally coupled as evidence sources in the same assessed learning task. This is a narrower and more defensible novelty claim than asserting that no one has ever used any two of these technologies together.

TABLE I
Literature evidence streams and the remaining integration gap.

Evidence stream	Representative work	What it establishes	What remains under-specified
Power-system simulation / virtual labs	Allen et al. [26]; Mohamed et al. [23]; Anderson et al. [22]	Simulation and virtual environments can support analysis, experimentation, and operational reasoning.	Cyber evidence and spatial context are usually secondary or absent.
Power protection / substation practice	Shahnia et al. [24]; Li et al. [20]; Pires et al. [21]	Authentic or simulated operation can improve practical engagement and decision practice.	No explicit integration of spatial risk and OT threat evidence in the same task.

Evidence stream	Representative work	What it establishes	What remains under-specified
Smart-grid / ICS cybersecurity education	Yardley et al. [10]; Del Canto et al. [11]; Domínguez et al. [12,13]; Prada et al. [42]; Francia et al. [15]	Hands-on, remote, and project-based ICS/security education is feasible and pedagogically valuable.	Power-system reasoning and GIS are rarely first-class learning objects.
OT cybersecurity evidence synthesis	Torgersen et al. [8]	Training is diverse; testbeds, simulations and digital twins are used, but performance measurement is inconsistent.	Need for role-specific, evidence-based cross-layer assessment remains.
Digital-twin engineering education	Kotecha et al. [17]; Blackwell & Roche [18]; Speicher et al. [19]; Lara Muñoz et al. [34]	Digital twins can connect theory, practice, remote learning and interdisciplinary work.	Cross-domain synchronization rules for power + GIS + OT education are not defined.
Power-system geospatial integration	Li et al. [27]; Salbanya et al. [28]	Electrical and spatial datasets can be harmonized for resilience and network analysis.	The educational use of this mapping as a reasoning artifact is underdeveloped.
Cyber-informed engineering education	INL CIE Guide [6]; Aranzazu-Suescun & Zapata-Rivera [16]	Cyber risk can be incorporated into engineering design and curricula.	The role of geospatial evidence and power-system state coupling is not specified.

3. Method: structured integrative synthesis and design-based framework construction

The paper uses a structured integrative synthesis rather than a formal systematic review or meta-analysis. This choice is deliberate. The research question is design-oriented: it asks what an educational architecture should contain when evidence from multiple technical and pedagogical domains is brought together. The evidence base was therefore organized into four source classes: (A) engineering-education research on power systems, active learning, systems thinking, PBL, virtual laboratories, and digital twins; (B) OT/ICS cybersecurity education studies and reviews; (C) authoritative technical and curricular frameworks; and (D) technical research on the relationship between geospatial and power-system models. An integrative review is appropriate here because the aim is to synthesize heterogeneous evidence into a researchable design rather than to estimate a pooled effect [43,44].

The targeted search strategy used combinations of the following concept groups: ("power system*" OR "smart grid" OR substation) AND (education OR curriculum OR laboratory OR simulation OR "engineering education"); ("industrial control system*" OR OT OR SCADA) AND (education OR training OR laboratory OR curriculum); (GIS OR geospatial OR spatial) AND ("power system*" OR electric distribution OR grid); and ("digital twin") AND (engineering education OR power OR control). Priority was given to peer-reviewed journal and conference papers, official standards, and government/national-laboratory guidance. Older seminal pedagogical sources were retained when they establish a theoretical construct still used in current engineering-education research. The review approach follows established guidance for rigorous integrative reviews rather than claiming formal systematic-review status [43,44].

The synthesis was coded using four dimensions: (1) domain knowledge, (2) engineering action, (3) observable learner behavior, and (4) evidence artifact. A framework component was retained when it could be translated into an observable task and a reviewable student artifact. This criterion is intended to prevent the framework from becoming a catalog of fashionable technologies. For example, "GIS literacy" is too broad as a learning outcome, whereas "use spatial evidence to rank substation restoration priorities under a specified hazard and justify the ranking" is observable.

The resulting framework follows design-based research logic: identify a consequential educational problem, derive design requirements from prior evidence and practice, construct an intervention architecture, define observable outcomes, and formulate propositions that can be empirically tested [45]. No human-participant data, performance statistics, or causal claims are reported in this paper.

3.1. Design requirements derived from the literature

TABLE II
Design requirements derived from the literature and their framework response.

Requirement	Rationale from literature	GeoCyberTwin-PS response
Authenticity without unsafe exposure	ICS education benefits from hands-on practice, but operational environments impose safety and security constraints [1,10-13,15,42].	Use isolated, synthetic, reversible scenarios; expose attack evidence rather than real operational systems.
Cross-layer traceability	Systems thinking and cyber-informed engineering emphasize relationships across system boundaries [6,30,31].	Stable asset IDs connect power, GIS and OT objects.
Decision-centered learning	Power labs and PBL are more valuable when students analyze and decide rather than follow recipes [23,24,32,33].	Every scenario ends in a defensible engineering decision.
Assessment of reasoning, not tool use	OT education reviews report inconsistent performance measurement [8].	Rubrics separately score technical correctness, evidence integration, uncertainty, and communication.
Scalable implementation	Digital-twin and remote-lab literature notes infrastructure and faculty burdens [16,17].	Three implementation tiers support software-only, emulation, or hybrid physical testbeds.
Alignment with professional outcomes	ABET emphasizes complex problem solving, design, communication, ethics, teamwork, experimentation, and lifelong learning [7].	Learning outcomes and assessments explicitly map to these capabilities.

4. GeoCyberTwin-PS framework

4.1. Conceptual architecture

GeoCyberTwin-PS consists of four coupled representations. The Power-System State Model (PSSM) describes electrical topology and operating state; the Geo-Spatial Context Model (GSCM) describes physical location, hazards, accessibility, customers, and spatial dependencies; the OT/Cyber Model (OCM) describes control assets, zones, conduits, telemetry, security evidence, and threat-informed events; and the Learning Orchestration Layer (LOL) specifies the scenario, task sequence, evidence package, and assessment rules. The architecture is shown in Fig. 1.

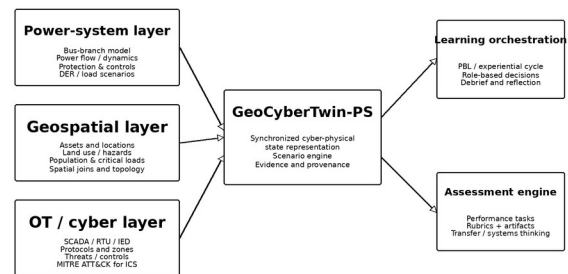


Fig. 1. GeoCyberTwin-PS reference architecture. The learning orchestration layer couples electrical state, spatial context, and OT/cyber evidence without requiring a single commercial platform.

The key architectural principle is referential integrity rather than technological integration for its own sake. An asset such as a substation may appear as a node in the electrical graph, a point feature in GIS, and an OT site containing RTU and IED assets. These records need a stable identifier so that a learner's statement can be traced across representations. A simple implementation can use CSV/GeoPackage/JSON files; a more advanced implementation can use a relational database or event-driven data service. The educational invariant is the identity relationship, not the software stack.

4.2. Shared data contract and minimal interoperability model

A minimal cross-model schema is proposed to keep interoperability teachable. Each asset record should include: `asset_id`, `asset_type`, geographic coordinates where applicable, `electrical_node` or feeder identifiers where applicable, `OT_zone`, `communication_dependency`, `criticality` attributes, `data_provenance`, and `scenario_state`. Learners can therefore see that data integration is itself an engineering problem. A map that cannot be reconciled to the electrical topology is not merely inconvenient; it is evidence of uncertainty that must be documented.

TABLE III
Minimum shared data contract for electrical, geospatial, and OT representations.

Field	Type	Purpose	Example
<code>asset_id</code>	String	Stable identity across representations	S07-RTU-01
<code>asset_type</code>	Controlled vocabulary	Common semantic meaning	RTU / IED / substation
<code>electrical_ref</code>	String / null	Link to power-system object	BUS_17 / FDR_03
<code>latitude, longitude</code>	Float / null	Spatial location	35.71, 51.42
<code>ot_zone</code>	String	Security segmentation context	ZONE_CTRL_2
<code>criticality</code>	Ordinal / categorical	Service or mission importance	High
<code>comm_dependency</code>	List	Communications relied upon	RTU->SCADA-HMI
<code>data_provenance</code>	String	Traceability / source	Synthetic scenario v1.2
<code>scenario_state</code>	Controlled state	Dynamic scenario condition	Telemetry_degraded

4.3. Competency model

The competency model deliberately moves from domain competence to cross-layer synthesis. Eight competencies are proposed. C1-C3 establish disciplinary foundations; C4-C6 concern integration; C7 addresses professional communication and uncertainty; C8 addresses reflective improvement. This progression aligns with the logic of constructive alignment and with ABET's emphasis on complex problem solving, design, communication, ethics, teamwork, experimentation, and continued learning [7,35].

TABLE IV
Cross-layer competency model and observable evidence.

ID	Competency	Observable performance	Evidence artifact
C1	Power-system reasoning	Interpret operating state, topology, contingencies, protection, DER, and service constraints.	Annotated power model + state explanation
C2	OT/ICS literacy	Identify control assets, zones, dependencies, and operational constraints.	OT architecture + asset role map

ID	Competency	Observable performance	Evidence artifact
C3	Spatial reasoning	Use location, hazards, accessibility, customer context, and network geography to support a decision.	GIS map + spatial analysis memo
C4	Cross-layer correlation	Trace a common asset/state across electrical, GIS, and OT representations.	Cross-model evidence matrix
C5	Threat-informed diagnosis	Construct a plausible threat path using bounded evidence and a recognized taxonomy.	ATT&CK-informed event chain
C6	Resilience-oriented design	Recommend mitigations that balance security, safety, availability, restoration, and service.	Ranked mitigation decision
C7	Engineering communication	Brief technical and mixed audiences with explicit assumptions and uncertainty.	Briefing + technical memo
C8	Reflective systems reasoning	Explain what evidence changed the decision and where model uncertainty remains.	Reflection / post-mortem

4.4. Learning progression

The progression follows three stages. Stage 1 is representation: students learn each model separately and establish a shared vocabulary. Stage 2 is correlation: they join two representations and identify mismatches, dependencies, and causal claims. Stage 3 is decision: they work on unseen scenarios in which no single model provides enough evidence. The progression is shown in Fig. 3.

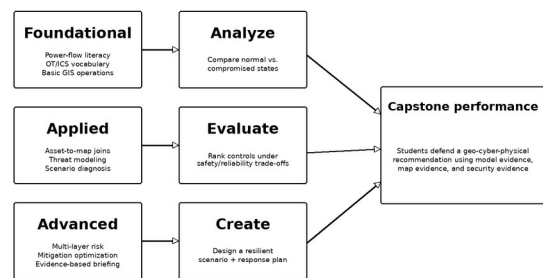


Fig. 3. GeoCyberTwin-PS learning progression from single-domain representation to cross-layer decision and reflection.

4.5. Scenario grammar

A reusable scenario grammar prevents the course from becoming a collection of unrelated demonstrations. Each scenario contains seven components: S1 baseline operating state; S2 spatial context; S3 cyber/OT trigger; S4 observed evidence; S5 electrical or operational consequence; S6 decision constraints; and S7 required evidence artifact. The instructor can vary any component while preserving the learning logic.

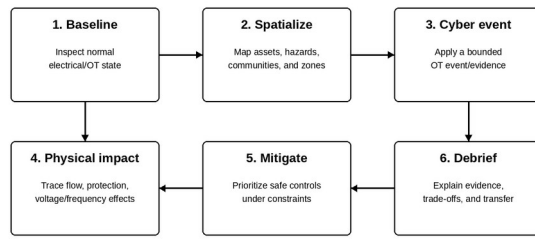


Fig. 2. Scenario learning cycle. Students move from baseline state to evidence integration, decision, justification, and post-scenario reflection.

4.6. Illustrative integrated scenario

Scenario GCPS-07, "Substation S-07 under constrained restoration," illustrates the intended level of integration. Students receive a medium-voltage distribution model containing 18 buses, three feeders, two distributed-PV clusters, one battery energy storage system, and four critical loads. A synthetic GIS package includes roads, a flood-risk layer, a hospital, a water-treatment facility, and a communications cabinet. The OT view identifies the RTU, a small set of IEDs, the supervisory channel, and the site security zone. The baseline state is feasible but has limited redundancy.

The cyber trigger is deliberately non-destructive. Students are told that one RTU's telemetry has become intermittent and that one IED reports a sequence inconsistent with the electrical state. They receive synthetic event logs and a simplified ATT&CK-for-ICS mapping rather than an executable exploit. The task is to determine whether the dominant problem is electrical, communications-related, cyber-related, or mixed; identify affected assets; use spatial context to estimate service consequences; and propose a mitigation sequence that respects safety and restoration constraints.

The assessment requires five artifacts: an annotated map; a short electrical-state explanation; an OT threat/evidence chain; a ranked mitigation table; and a two-minute briefing. The instructor's debrief asks which claims are observations, which are inferences, and which depend on assumptions. This distinction is central to the framework because cross-layer engineering decisions often fail not because a tool is used incorrectly, but because an inference is mistaken for an observation.

5. Curriculum implementation blueprint

The framework can be inserted into an existing power-system analysis or protection course, a special-topics graduate course, or a multidisciplinary engineering module. TABLE IV describes a 12-week version that assumes students already know basic circuits and introductory power-system concepts. The course is intentionally designed so that the first half can run without a physical OT laboratory.

TABLE V
Twelve-week curriculum implementation blueprint.

Week	Focus	Core activity	Primary evidence
1	Systems framing and baseline grid	Build and validate a small power-system model.	Individual concept map + baseline model
2	OT architecture and safety	Identify SCADA, RTU, IED, HMI, zones and operational constraints.	OT architecture annotation
3	GIS fundamentals for power engineers	Load spatial layers; perform proximity and service-area analysis.	Map + spatial reasoning memo

Week	Focus	Core activity	Primary evidence
4	Electrical-spatial linkage	Map buses/feeders/substations to GIS features; document mismatches.	Cross-model data audit
5	Threat-informed OT reasoning	Interpret synthetic events using ATT&CK for ICS and NIST/IEC concepts.	Threat/evidence chain
6	Scenario 1: telemetry anomaly	Diagnose an ambiguous cyber-physical event.	Team incident analysis
7	Scenario 2: protection / configuration event	Analyze an event with protection and operational constraints.	Protection verification memo
8	Scenario 3: hazard + cyber interaction	Combine hazard exposure, accessibility, and telemetry uncertainty.	Spatial resilience analysis
9	Resilience and mitigation design	Compare engineered controls, segmentation, monitoring, and restoration actions.	Mitigation decision matrix
10	Unseen transfer task	Solve a new cross-layer scenario individually.	Individual transfer performance
11	Capstone integration	Develop a complete scenario response in teams.	Map + model + cyber evidence + briefing
12	Defense and reflection	Present decisions; analyze uncertainty and trade-offs.	Defense, reflection, peer review

5.1. Implementation tiers

TABLE VI
Implementation tiers and technology requirements.

Tier	Technology pattern	Appropriate use	Resource burden
Tier 1: simulation-first	Power-system simulator + GIS + synthetic OT logs	Foundational and applied learning; no executable cyber activity required.	Low
Tier 2: emulation	Tier 1 + virtual PLC/RTU/SCADA components + isolated network emulation	Advanced diagnosis, network/OT reasoning, controlled packet/log analysis.	Moderate
Tier 3: hybrid testbed	Tier 2 + physical IED/PLC/RTU or HIL equipment	Capstone, instructor demonstrations, advanced experimental work.	High

The framework recommends that learning outcomes remain invariant across tiers. This is particularly important for institutions with limited laboratory budgets. A student who can correctly trace a synthetic telemetry anomaly to an operational consequence using a simulation-only environment can be assessed on the same higher-level reasoning construct as a student working with a physical testbed. The fidelity of the environment may affect motivation and certain procedural skills, but it should not define the core curriculum.

5.2. Instructor and laboratory requirements

The principal implementation constraint is faculty expertise. The course sits at the intersection of power engineering, OT cybersecurity,

GIS, and engineering education. A single instructor may not need deep expertise in all four areas, but the program should ensure access to complementary expertise or well-curated instructional resources. The instructor should also maintain a versioned scenario library because threat taxonomies, standards, and software environments evolve [1-6].

A safe laboratory architecture should have no route to production or campus operational networks. Exercises should use synthetic assets, simulated or sandboxed protocols, and resettable virtual machines. When students analyze offensive behavior, they should be given pre-generated artifacts or an isolated range rather than asked to scan or exploit real systems. This boundary is not a secondary ethics point; it is part of the engineering design of the educational environment.

6. Assessment and empirical validation protocol

A central design principle is to evaluate cross-layer reasoning separately from tool proficiency. Students can often learn to perform a GIS operation or execute a script without understanding why the resulting evidence matters. Conversely, a student may understand the engineering decision while being slower with a particular software package. The assessment system therefore uses multiple evidence types.

TABLE VII
Assessment rubric for the integrated capstone task.

Criterion	Weight	Excellent evidence	Minimum acceptable evidence
Problem framing	15%	States decision, boundaries, stakeholders, and required evidence.	Defines a plausible decision but misses one key boundary.
Power-system analysis	20%	Correctly interprets state, constraints, and consequence.	Technically plausible interpretation with minor omissions.
OT/cyber reasoning	15%	Constructs an evidence-supported threat path without overclaiming.	Identifies relevant asset/event relationships.
Spatial reasoning	15%	Uses spatial evidence to change or justify the decision.	Provides relevant location/hazard evidence.
Cross-layer integration	20%	Explains causal and evidential links across all models.	Connects at least two representations coherently.
Mitigation and professional judgment	10%	Balances security, safety, availability, restoration and uncertainty.	Proposes a feasible mitigation with basic justification.
Communication and reflection	5%	Separates observation, inference and assumption; communicates clearly.	Presents a coherent summary with limited reflection.

6.1. Proposed research design for future implementation

The educational effectiveness of GeoCyberTwin-PS should be tested rather than inferred from the quality of the technology. A feasible study is a quasi-experimental or randomized classroom comparison in which one cohort receives separated instruction (power laboratory + cybersecurity mini-module + GIS exercise) and another receives matched content through integrated scenarios. The primary dependent variable should be transfer performance on an unseen cross-layer problem, not satisfaction alone.

A mixed-methods evaluation can include four instruments: (1) a cross-layer concept inventory, (2) an individual transfer task scored with the same analytic rubric, (3) structured think-aloud or interview evidence on decision reasoning, and (4) a brief measure of perceived confidence and workload. A delayed transfer task would be especially

valuable because the educational claim concerns systems competence rather than immediate task familiarity. Inter-rater reliability should be established for the rubric before outcome analysis, and the research protocol should receive institutional ethics review when student data are collected.

TABLE VIII
Proposed instruments and analysis plan for future empirical validation.

Instrument	Construct	Timing	Primary analysis
Cross-layer concept inventory	Conceptual integration and boundary recognition	Pre/post	Within/between group change
Transfer performance task	Unseen systems reasoning	Post + delayed	Rubric score; effect size with confidence interval
Reasoning trace	Evidence use, causal reasoning, uncertainty	During selected tasks	Qualitative coding
Workload/self-efficacy	Perceived difficulty and confidence	Selected weeks	Descriptive + exploratory correlations
Artifact analysis	Quality of maps, models, threat chains, decisions	Throughout	Artifact rubric + progression analysis

6.2. Research propositions

- P1. Students exposed to integrated scenarios will demonstrate stronger transfer on unseen cross-layer problems than students receiving equivalent domain content in separated tasks.
- P2. Explicit use of spatial evidence will improve students' ability to justify asset criticality and restoration priorities when compared with decisions based only on electrical topology.
- P3. Assessment that requires students to distinguish observation, inference, and assumption will reduce unsupported causal claims in cyber-physical diagnosis.
- P4. The educational benefits of higher-fidelity testbeds will be conditional on adequate scaffolding; increased realism without instructional support may increase workload without improving transfer.
- P5. Students' cross-layer systems reasoning will predict professional-quality decision artifacts more strongly than software-specific tool proficiency alone.

7. Discussion

7.1. Why the integration matters pedagogically

The contribution of GeoCyberTwin-PS is best understood as a change in the unit of learning. Conventional labs often treat a bus, relay, or PLC as the object of study. The proposed framework treats an engineering decision under uncertainty as the object of study. That shift makes it possible for the same scenario to activate multiple disciplinary forms of evidence without turning the course into a generic technology survey.

The framework also provides a principled role for GIS. Spatial analysis is valuable when it changes the engineering question. For example, if a feeder serves a geographically concentrated set of critical customers, or if access to a substation is constrained by a hazard, a spatial layer can change restoration priorities. If the map merely decorates a single-line diagram, its educational value is low. This distinction helps prevent tool-driven curriculum expansion.

A parallel argument applies to cybersecurity. The course should not attempt to transform power engineers into full-time penetration testers. Rather, it should develop cyber-informed engineering judgment: awareness of how digital assets create failure pathways, how evidence can indicate compromise, and how engineering controls can reduce consequence. This aligns closely with the CIE Curriculum Guide's emphasis on integrating digital-risk thinking into normal engineering design and analysis [6].

7.2. Relation to current standards and professional expectations

The proposed competency model is compatible with multiple contemporary frameworks. NIST SP 800-82 Rev. 3 supplies the OT vocabulary and emphasizes performance, reliability, and safety [1]. IEC 62443-2-1:2024 frames asset-owner security programs and recognizes long-lived and legacy industrial assets [3]. MITRE ATT&CK for ICS provides a threat-oriented language for describing adversary behaviors [4]. CISA's Cybersecurity Performance Goals supply prioritized, actionable baseline practices for critical infrastructure [5]. At the curriculum level, the 2025 CIE Curriculum Guide provides explicit examples for lecture-, course-, and certificate-scale integration and encourages progressive adoption [6]. ABET's current engineering criteria provide the outcome framework around complex problem solving, design, communication, ethics, teamwork, experimentation, and continued learning [7].

The value of this alignment is not compliance. It is traceability. An instructor should be able to show why a particular scenario exists, which professional capability it develops, which artifact demonstrates attainment, and how the result contributes to continuous improvement. That traceability is especially important for a multidisciplinary course where the educational purpose could otherwise become difficult to defend.

7.3. Expected benefits and likely failure modes

TABLE IX
Expected benefits, failure modes, and design responses.

Potential benefit	Why it may occur	Likely failure mode	Design response
Stronger systems thinking	Students must reconcile multiple models and evidence sources.	Cognitive overload; students focus on software mechanics.	Scaffold representations before integration; limit scenario complexity.
Better cyber-informed engineering judgment	Cyber events are tied to physical and operational consequences.	Course drifts into generic cybersecurity or offensive technique.	Keep engineering consequence and safe mitigation as the assessment target.
More meaningful GIS use	Spatial evidence affects criticality, hazards, access or service.	Maps become decorative outputs.	Require spatial evidence to change or justify the decision.
Improved professional communication	Teams brief mixed technical audiences under uncertainty.	Students produce polished visuals without defensible reasoning.	Score evidence chain and assumptions separately from presentation quality.
Scalability across institutions	Three fidelity tiers preserve learning objectives.	Different tools create inequivalent experiences.	Use a technology-neutral data contract and common assessment rubric.

8. Safety, ethics, accessibility, and data governance

Because the topic concerns critical infrastructure, the educational design must treat safety and security as learning constraints. First, all cyber exercises should be isolated from production systems and campus networks. Second, real utility data should not be required; synthetic or appropriately transformed datasets are preferable unless data governance, licensing, and security review explicitly authorize their use. Third, students should learn that a technically effective cyber action may still be unacceptable if it creates unsafe operational conditions or violates restoration, privacy, or service obligations.

Accessibility also matters. GIS and cyber-physical interfaces can rely heavily on color, spatial positioning, or specialized controls. Each essential learning artifact should therefore have a textual or tabular equivalent, and map interpretation should not depend on color alone. Virtual environments should expose keyboard-accessible workflows wherever feasible. These choices are consistent with the broader engineering-education goal of making evidence and decision quality the focus rather than interface dexterity.

9. Limitations

Five limitations should temper interpretation. First, this paper is a design framework rather than an empirical effectiveness study. Its propositions require testing. Second, the targeted evidence synthesis is structured but not a formal systematic review; a future review should use a registered protocol and reproducible database screening if a stronger evidence claim is required. Third, the integrated approach may increase cognitive load, especially for students with uneven backgrounds in power engineering, GIS, or cybersecurity. Fourth, cross-model data integration is technically demanding and can become a hidden engineering project for instructors. Fifth, standards, threat taxonomies, software environments, and educational practices change; the scenario library must therefore be versioned and maintained.

The novelty claim is intentionally bounded. GeoCyberTwin-PS is not claimed to be the first educational environment to use power simulation, GIS, cybersecurity, or digital twins. Each component has prior educational and technical literature. The claimed contribution is the explicit instructional architecture that treats the three representations as co-equal evidence sources for power-engineering decisions and translates that architecture into learning outcomes, scenarios, assessment, and an empirical validation plan.

10. Future research agenda

A coherent research program can now proceed in stages. Phase 1 should pilot a small number of scenarios with expert review focused on content validity, data consistency, cognitive load, and safety. Phase 2 should compare separated and integrated instructional designs using transfer tasks. Phase 3 should test retention and transfer after a delay and across different levels of laboratory fidelity. Phase 4 should examine adoption across institutions with different toolchains and student backgrounds. Finally, the framework could be extended to other critical infrastructure domains, such as water and transportation, while preserving the central design principle that cyber risk is interpreted through physical consequence and operational context.

11. Conclusion

Power-system engineering education is entering a period in which electrical models, software-defined control, cybersecurity, and geographic context can no longer be treated as independent professional worlds. The educational challenge is not simply to add one more cybersecurity lecture or one GIS exercise. It is to help students reason across representations of the same engineered system and to justify decisions under uncertainty.

GeoCyberTwin-PS responds by coupling a power-system state model, a geospatial context model, an OT/cyber model, and a learning-orchestration layer. It turns these elements into scenario-based tasks that require students to model, map, diagnose, correlate, mitigate, and communicate. The framework is grounded in contemporary literature on power-system education, ICS/OT cybersecurity training, digital twins, spatial power-system data, active learning, systems thinking, project-based learning, and cyber-informed engineering. Its strongest research value is that it converts a broad interdisciplinary idea into a set of testable educational constructs and artifacts.

The next step is empirical. The proposed architecture should be implemented with synthetic and safely isolated scenarios, evaluated against explicit transfer measures, and revised through iterative design-based research. Until that work is completed, the framework should be interpreted as a researchable educational design proposal rather than as evidence of effectiveness. That boundary is a strength of the present manuscript: it keeps the claims aligned with the evidence while providing a concrete path toward validation.

Declarations

Funding. No external funding is reported for the present conceptual manuscript.

Competing interests. The author declares no known competing financial interests or personal relationships that could have influenced the work.

Ethics statement. This manuscript reports no original human-participant data. Any future classroom evaluation should obtain the required institutional ethics approval and informed consent.

Data availability. No original empirical dataset is reported. A future implementation should release synthetic scenario data, assessment instruments, and versioned configuration/code where security and licensing allow. Associated research resource: <https://doi.org/10.6084/m9.figshare.34065654>.

Code availability. No executable cyber tooling is required for the conceptual framework. Future releases should prioritize reproducibility, sandboxing, and safe educational use.

Author contributions (CRediT). Conceptualization; methodology; literature synthesis; framework design; visualization; writing - original draft; writing - review and editing: Amirhossein Rezaeian.

References

- [1] Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) Security (NIST SP 800-82 Rev. 3). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-82r3>
- [2] National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource and Overview Guide (NIST SP 1299). <https://doi.org/10.6028/NIST.SP.1299>
- [3] International Electrotechnical Commission. (2024). IEC 62443-2-1:2024: Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners. IEC.
- [4] MITRE. (2026). ATT&CK for ICS: Matrix and tactics. MITRE ATT&CK. <https://attack.mitre.org/matrices/ics/>
- [5] Cybersecurity and Infrastructure Security Agency. (2024). Cross-Sector Cybersecurity Performance Goals. U.S. Department of Homeland Security. <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>
- [6] Idaho National Laboratory. (2025). CIE Curriculum Guide, Version 2.0 (INL/RPT-25-88269). U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response.
- [7] ABET. (2025). Criteria for Accrediting Engineering Programs, 2025-2026. ABET Engineering Accreditation Commission.
- [8] Torgersen, L. N. S., Noble, E. R., Ask, T. F., & Knox, B. J. (2025). Strengths and Knowledge Gaps Identified From Cybersecurity Education and Training Programs, and the Implications for Operational Technology Personnel in Critical Infrastructures: A Scoping Review. *IEEE Access*, 13, 138265-138312. <https://doi.org/10.1109/ACCESS.2025.3594045>
- [9] Pirta-Dreimane, R., Romanovs, A., Bikovska, J., Peksa, J., Vartiainen, T., Valliou, M., Kamsamrong, J., & Eltahawy, B. (2024). Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation. *Energies*, 17(8), 1876. <https://doi.org/10.3390/en17081876>
- [10] Yardley, T., Uludag, S., Nahrstedt, K., & Sauer, P. (2015). Developing a Smart Grid cybersecurity education platform and a preliminary assessment of its first application. *Proceedings - Frontiers in Education Conference*, 2015-February, 7044273. <https://doi.org/10.1109/FIE.2014.7044273>
- [11] Del Canto, C. J., Prada, M. A., Fuertes, J. J., Alonso, S., & Domínguez, M. (2015). Remote Laboratory for Cybersecurity of Industrial Control Systems. *IFAC-PapersOnLine*, 48(29), 13-18. <https://doi.org/10.1016/j.ifacol.2015.11.206>
- [12] Domínguez, M., Prada, M. A., Reguera, P., Fuertes, J. J., Alonso, S., & Morán, A. (2017). Cybersecurity training in control systems using real equipment. *IFAC-PapersOnLine*, 50(1), 12179-12184. <https://doi.org/10.1016/j.ifacol.2017.08.2151>
- [13] Domínguez, M., Pérez, D., Morán, A., Alonso, S., Prada, M. A., & Fuertes, J. J. (2022). Remote training in cybersecurity for industrial control systems. *IFAC-PapersOnLine*, 55(17), 320-325. <https://doi.org/10.1016/j.ifacol.2022.09.299>
- [14] Domínguez, M., Fuertes, J. J., Prada, M. A., Alonso, S., Morán, A., & Pérez, D. (2022). Design of Platforms for Experimentation in Industrial Cybersecurity. *Applied Sciences*, 12(13), 6520. <https://doi.org/10.3390/app12136520>
- [15] Francia, G. A., III, Randall, G., & Snellen, J. (2017). Pedagogical Resources for Industrial Control Systems Security: Design, Implementation, Conveyance, and Evaluation. *Journal of Cybersecurity Education, Research and Practice*, 2017(1), Article 2. <https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss1/2>
- [16] Aranzazu-Suescun, C., & Zapata-Rivera, L. F. (2025). Cyber-Informed Engineering Course Syllabus for Undergraduate Engineering Programs. 2025 ASEE Annual Conference & Exposition. <https://doi.org/10.18260/1-2--56192>
- [17] Kotecha, M. C., Dandridge, T. M., & Reid Smith, T. (2025). Digital Twins in Engineering and Design Education: A Systematized Review. 2025 ASEE Annual Conference & Exposition. <https://doi.org/10.18260/1-2--56296>
- [18] Blackwell, C., & Rocke, S. (2024). WIP: A Review of Digital Twin Technology in Undergraduate Control Engineering Education: Applications, Challenges, and Future Directions. 2024 IEEE Frontiers in Education Conference. <https://doi.org/10.1109/FIE61694.2024.10893435>
- [19] Speicher, T., DeFranco, J., Stricker, C., Kumara, S., & Bilén, S. (2026). Digital twin technology for engineering education: An experiential learning case study. *Industry and Higher Education*. <https://doi.org/10.1177/09504222261443589>
- [20] Li, B.-L., Quan, P., Wang, C.-J., Guo, H.-W., Wei, X., et al. (2026). Interactive Virtual Substation Simulation Training System for Enhancing Practical Competence in Engineering Education. *Computer Applications in Engineering Education*, 34(1), e70123. <https://doi.org/10.1002/cae.70123>
- [21] Pires, G. C. S., Villegas Guerrero, C. A., Passos, F. O., & Silveira, P. M. (2026). A Pedagogical Framework Proposal for Next-Generation Power System Protection Education: A Case Study on Digital Twin Integration at the Federal University of Itajubá in Brazil. *CIGRE Session Materials*, Ref. B5-11036.
- [22] Anderson, A. A., Barr, J. L., Sharma, P., Allwardt, C. H., Vadari, S. V., & Dubey, A. (2022). Real-time Distribution Simulation and Application Development for Power Systems Education. 2022 IEEE Power & Energy Society General Meeting. <https://doi.org/10.1109/PESGM48719.2022.9917004>
- [23] Mohamed, O., Bitar, Z., Abu-Sultaneh, A., & Abu Elhaija, W. (2023). A simplified virtual power system lab for distance learning and ABET accredited education systems. *International Journal of Electrical Engineering & Education*, 60(4), 397-426. <https://doi.org/10.1177/0020720921997064>
- [24] Shahnai, F., Moghbel, M., & Yengejeh, H. H. (2016). Motivating power system protection course students by practical and computer-based activities. *IEEE Transactions on Education*, 59(2), 81-90. <https://doi.org/10.1109/TE.2015.2448611>
- [25] Hu, Q., Li, F. F., & Chen, C.-f. (2015). A Smart Home Test Bed for Undergraduate Education to Bridge the Curriculum Gap From Traditional Power Systems to Modernized Smart Grids. *IEEE Transactions on Education*, 58(1), 32-38. <https://doi.org/10.1109/TE.2014.2321529>
- [26] Allen, E., LaWhite, N., Yoon, Y., Chapman, J., & Ilic, M. (2001). Interactive object-oriented simulation of interconnected power systems using SIMULINK. *IEEE Transactions on Education*, 44(1), 87-94. <https://doi.org/10.1109/13.912714>
- [27] Li, X., Guddanti, K. P., Acharya, S., Royer, P. D., Fan, X., & Elizondo, M. A. (2023). Smart Data Mapping for Connecting Power System Model and Geospatial Data. 2023 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT-LA), 45-49. <https://doi.org/10.1109/ISGT-LA56058.2023.10328353>
- [28] Salbanya, B., Nin, J., & Gras Alomà, R. (2026). Harmonized geospatial data to evaluate the Electric Distribution Networks in the US Northeast. *Scientific Data*, 13, 147. <https://doi.org/10.1038/s41597-025-06465-9>
- [29] Easa, S. M., Li, S., & Shi, Y. (1998). GIS Technology for Civil Engineering Education. *Journal of Professional Issues in Engineering Education and Practice*, 124(2), 40-47. [https://doi.org/10.1061/\(ASCE\)1052-3928\(1998\)124:2\(40\)](https://doi.org/10.1061/(ASCE)1052-3928(1998)124:2(40))
- [30] Monat, J. P., Gannon, T. F., & Amisshah, M. (2022). The Case for Systems Thinking in Undergraduate Engineering Education. *International Journal of Engineering Pedagogy*, 12(3), 50-88. <https://doi.org/10.3991/ijep.v12i3.25035>
- [31] Azad, A., & Moore, E. (2024). Lessons Learned From Teaching System Thinking To Engineering Students. *Proceedings of the Canadian Engineering Education Association*. <https://doi.org/10.24908/pceea.2023.17007>
- [32] Osunbunmi, I., & Fang, N. (2022). Work in Progress: An Early Look Into the Systematic Review of Project-Based Learning in Engineering Education. 2022 ASEE Annual Conference & Exposition. <https://doi.org/10.18260/1-2--40681>
- [33] Ferrari dos Santos, S. S. R., Martins de Resende, L. M., & Castanon Xavier, J. (2024). Project-Based Learning (PBL) as an Experiential Pedagogical Methodology in Engineering Education: A Review of the Literature. *Education Sciences*, 14(6), 617. <https://doi.org/10.3390/educsci14060617>
- [34] Lara Muñoz, E. M., Viveros Torres, I., & Galindo Cobos, J. A. (2026). Project-Based Learning with digital twins in engineering education: a quasi-experimental study. *RELIEVE*, 32(1). <https://doi.org/10.30827/relieve.v32i1.36282>
- [35] Biggs, J. (1996). Enhancing teaching through constructive alignment. *Higher Education*, 32, 347-364. <https://doi.org/10.1007/BF00138871>
- [36] Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences*, 111(23), 8410-8415. <https://doi.org/10.1073/pnas.1319030111>

- [37] Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education*, 93(3), 223-231. <https://doi.org/10.1002/j.2168-9830.2004.tb00809.x>
- [38] Kolb, D. A. (1984). *Experiential Learning: Experience as the Source of Learning and Development*. Prentice-Hall.
- [39] Sen, Ö., Ivanov, B., Kloos, C. D., Zöll, C., Lutat, P., Henze, M., Ulbig, A., & Andres, M. (2025). Simulation of multi-stage attack and defense mechanisms in smart grids. *International Journal of Critical Infrastructure Protection*, 48, 100727. <https://doi.org/10.1016/j.ijcip.2024.100727>
- [40] Muaan ur Rehman, M., & Bahşi, H. (2024). Process-aware security monitoring in industrial control systems: A systematic review and future directions. *International Journal of Critical Infrastructure Protection*, 47, 100719. <https://doi.org/10.1016/j.ijcip.2024.100719>
- [41] Abraham, D., Erceylan, G., Gkioulos, V., et al. (2025). Towards enhanced cybersecurity in industrial control systems: a systematic review of context-based modeling, digital twins, and machine learning approaches. *International Journal of Information Security*, 24, 243. <https://doi.org/10.1007/s10207-025-01158-1>
- [42] Prada, M. A., Fuertes, J. J., Rodríguez-Ossorio, J. R., González-Herbón, R., González-Mateos, G., & Domínguez, M. (2023). Hands-on training in industrial cybersecurity for a multidisciplinary Master's degree. *IFAC-PapersOnLine*, 56(2), 11217-11222. <https://doi.org/10.1016/j.ifacol.2023.10.850>
- [43] Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356-367. <https://doi.org/10.1177/1534484305278283>
- [44] Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. *Journal of Advanced Nursing*, 52(5), 546-553. <https://doi.org/10.1111/j.1365-2648.2005.03621.x>
- [45] The Design-Based Research Collective. (2003). Design-based research: An emerging paradigm for educational inquiry. *Educational Researcher*, 32(1), 5-8. <https://doi.org/10.3102/0013189X032001005>

Appendix A. Scenario authoring template

TABLE X
Scenario authoring template.

Field	Purpose	Illustrative content
Scenario ID / version	Traceability and revision control	GCPS-07 / v1.2
Learning outcomes	Two to four observable objectives	Trace OT anomaly to electrical consequence
Baseline state	Define normal operating condition	Power flow feasible; N-1 constraint active
Spatial context	Specify location-dependent evidence	Flood risk, hospital, roads, communications cabinet
Cyber/OT trigger	Introduce bounded event evidence	Intermittent telemetry + inconsistent IED sequence
Evidence package	Define what students can observe	Logs, model output, GIS layers, asset metadata
Decision constraints	Keep scenario realistic	Safety, restoration time, critical load priority
Student outputs	Make reasoning assessable	Map, model summary, evidence chain, decision matrix, briefing
Debrief question	Surface assumptions and uncertainty	What evidence would change your decision?

Appendix B. Instructor implementation checklist

- Define the engineering decision before selecting software.
- Create stable identifiers for electrical, spatial, and OT objects.
- Document assumptions, uncertainty, provenance, and scenario version.
- Build and validate the baseline state before introducing any cyber event.
- Use synthetic or authorized data and isolated environments only.
- Require at least one electrical and one spatial evidence artifact for integrated tasks.
- Use a rubric that separately scores technical correctness and cross-layer integration.
- Provide accessible textual/tabular alternatives to map-only outputs.
- Review scenarios against current NIST, IEC, MITRE, CISA, and institutional guidance before reuse.

Archive assessment instruments and de-identified evidence for continuous improvement.