OPEN ACCESS Freely available online

ISSN 2737-5315
Volume 6
Issue 1
Educational Innovations and Emerging Technologies

Article

Construction of an Educational Ecosystem for Safety Engineering Curriculum in Industrial Internet Context

He Wu*, Na Yang

School of Safety Engineering and Emergency Management, Nantong Institute of Technology, Nantong 226000, China; 836752644@qq.com
* Correspondence: 20239131@ntit.edu.cn

Received: May 23, 2025; **Revised:** Jun 29, 2025; **Accepted:** Jul 08, 2025; **Published:** Mar 30, 2026

Abstract: In the context of swift Industrial Internet advancement, safety engineering education encounters significant obstacles, such as the divergence between theoretical instruction and industrial requirements, along with the inadequate development of multidisciplinary talent. Conventional educational frameworks, which excessively focus on general safety theories, fail to address the complex competency demands of security professionals in Industrial Internet-driven industrial ecosystems. This study advocates for the development of a safety engineering education curriculum ecosystem based on the Industrial Internet, which amalgamates industrial, academic, research, and application resources to create a dynamically adaptive teaching system that responds to technological advancements and industry requirements. The framework employs a "theory-technology-scenario" dynamic closed-loop design paradigm, utilising an onion model to organize a three-tiered curricular ecosystem consisting of a core layer in safety engineering, a technology convergence layer, and a scenario application layer. This is supplemented by four modular clusters: foundational theory, technical convergence, scenario application, and practical innovation. The implementation adopts a tiered strategy: a short-term emphasis on curriculum piloting and faculty development; a medium-term building of a "Industrial Internet + Security Laboratory" innovation platform; and a long-term creation of a cohesive industry-academia-research-application ecosystem. The study, bolstered by regulatory incentives and industry collaboration, tackles the hardware-centric bias of traditional education and enables the shift of safety engineers' roles from reactive incident management to proactive risk prediction. Significant improvements encompass an interdisciplinary educational framework, mechanisms for technology-tracking curriculum iteration, and scenario-driven pedagogical models, collectively offering theoretical and practical avenues for developing safety engineers in the Industrial Internet era. These contributions enhance the sustainable development and worldwide competitiveness of China's Industrial Internet ecosystem.

Keywords: Industrial internet; Safety engineering education; Educational ecosystem; Interdisciplinary integration; Talent cultivation

1. Introduction

Industrial Internet has become a crucial facilitator of the Fourth Industrial Revolution, substantially altering the digital transformation trajectory of global industrial systems (Selepe, 2025). This technological framework achieves systemic convergence by integrating contemporary information technologies with industrial architecture, forming a technological matrix that includes IoT networks, big data analytics, cloud computing infrastructure, and intelligent sensing devices (Stoiber & Schönig, 2024). This convergence facilitates intelligent reconfiguration of production processes and engenders multidimensional advancements in manufacturing resource allocation, operational model innovation, and industrial collaboration optimization (Tang et al., 2022).

Safety Engineering Education refers to a discipline dedicated to educating professionals capable of integrating safety science fundamentals (e.g., risk assessment, emergency response) with domain-specific technical knowledge to ensure operational safety in industrial environments. Within the Industrial Internet context, this discipline expands to include competencies in cybersecurity, data governance, and predictive risk modeling for cyber-physical systems. Amid the rapid advancement of Industrial Internet technologies, safety engineering education faces significant developmental challenges within modern industrial ecosystems (Velichko et al., 2025). Contemporary safety engineering educational frameworks typically follow a knowledge construction model centered on generic safety theories, with curricula predominantly focused on traditional safety science principles, classical safety management techniques, and fundamental training in accident prevention and emergency response protocols (Woodrow et al., 2020). This traditional pedagogical framework has established an extensive knowledge transmission system within safety engineering

disciplines, yet its limitations become increasingly evident within the new industrial ecosystems enabled by Industrial Internet technologies (Wang et al., 2024). These constraints are systematically illustrated in Fig. 1.

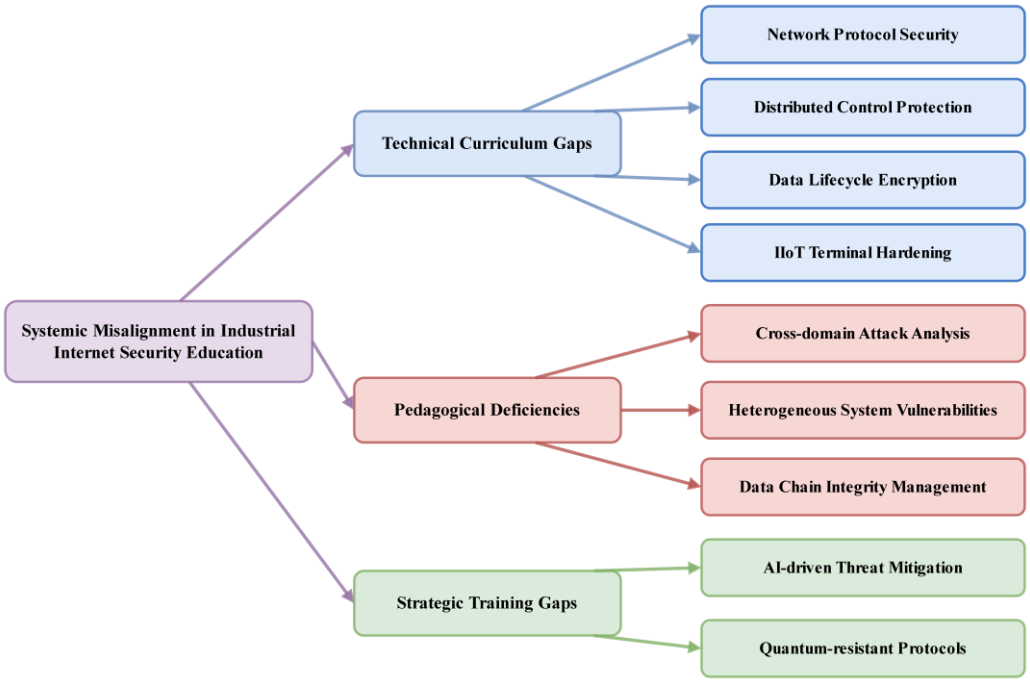

Fig. 1. Paradigmatic constraints in conventional safety engineering frameworks.

A significant difficulty exists in the marked disparity between traditional safety engineering education and actual industrial production environments (Bjelland et al, 2024). This divergence has created a structural disparity between the training of safety engineering specialists and the practical requirements of Industrial Internet sectors. This discrepancy is evident in the following manner (Osborne et al., 2024): Industries urgently need interdisciplinary safety engineering experts with (1) strong security scientific knowledge, (2) fluency in Industrial Internet IT, and (3) scenario-specific cognitive skills. This composite expertise is crucial for tackling emerging industrial security threats stemming from the profound convergence of next-generation information technologies and industrial production systems, thereby ensuring the operational stability of industrial systems, the sustainability of production efficiency, and the cybersecurity of digital-physical environments.

This study provides a novel paradigm for creating an Industrial Internet-based safety engineering education ecosystem. The framework seeks to surpass the constraints of traditional safety engineering education by integrating Industrial Internet technologies with safety instruction, thus creating a comprehensive, multi-layered, and dynamically responsive educational ecosystem. This ecosystem aims to develop interdisciplinary professionals who possess a safety science perspective, IT innovation skills, and practical experience in industrial contexts, directly responding to the pressing need for experts adept at managing Industry 4.0 security challenges.

This study provides a novel paradigm for creating an Industrial Internet-based safety engineering education ecosystem, conceptualized as a dynamic, interconnected, and adaptive system integrating industry, academia, research, and application components to holistically cultivate talent. By promoting synergistic development between safety engineering education and Industrial Internet sectors, it creates a virtuous cycle in which educational institutions effectively address industrial needs while benefiting from technological breakthroughs in the industry. This dual-benefit method establishes a vital foundation for the sustainable development of China's Industrial Internet ecosystem and its competitive rise in the global industrial arena.

Therefore, the primary purpose of this research is to construct and propose a novel Industrial Internet-based safety engineering curriculum ecosystem framework. This framework is explicitly designed to overcome the critical limitations of traditional safety engineering education identified above – namely, the persistent theory-practice gap and the lack of interdisciplinary focus – thereby fundamentally enhancing the quality and relevance of safety engineering education to produce graduates equipped with a safety science perspective, IT innovation skills, and practical industrial context experience necessary to address the complex security challenges of Industry 4.0.

2. Development of an Industrial Internet-Based Curriculum Ecosystem

2.1. Curriculum System Design Principles

The curricular framework incorporates six complementary design principles, as seen in Table 1: (1) Objective-driven cultivation through tri-dimensional (knowledge-competency-literacy) development; (2) Interdisciplinary integration via vertical safety-technology coupling and horizontal IT-scenario-safety triad; (3) Hierarchical advancement from fundamental concepts to practical application; (4) Practical engagement through industry collaboration and competition-oriented learning; (5) Adaptive evolution through technology monitoring and annual curriculum revision; (6) Customised development facilitated by a modular "Core + Specialisation + Electives" framework. This framework methodically responds to industrial requirements for experts proficient in contemporary industrial security issues. To ensure the curriculum remains aligned with technological advancements and industrial demands, we establish an annual revision cycle based on adaptive evolution through technology monitoring and industry feedback.

Table 1. Curriculum system design principles.

Design Principle	Core Mechanism	Implementation Strategy
Goal Orientation	Cultivate interdisciplinary professionals with: • Safety science fundamentals • IT application skills • Industrial scenario expertise	• Tri-dimensional cultivation logic: - Knowledge (security architecture design) - Competency (risk assessment) - Literacy (emergency response)
Integration	Bridge safety science & Industrial Internet technologies	• Vertical integration: Safety principles + Technical implementations (e.g., OPC UA protocol security) • Horizontal integration: IT-scenario-safety triad (e.g., Edge Computing Security modules)
Hierarchy	Three-tier progressive structure	Foundational: Industrial Internet Intro (cognitive frameworks) Specialized: Industrial Cryptography (technical expertise) Applied: Digital Twin Security Labs (scenario implementation)
Practicality	Four-in-one implementation model	• ≥40% practical credits • Huawei/Siemens joint labs • Dual mentorship system • Security competition-incubation ecosystem
Dynamic Update	Triple feedback mechanism	• Tech tracking (Gartner Hype Cycles monitoring) • Annual industry review (Zero Trust/AI Security integration) • Iterative revisions (employer feedback analysis)
Personalization	Modular "Core + X" architecture	Core: Safety science fundamentals Specialization tracks: • Industrial Control System Security

• Industrial Big Data Security

Electives: AI Ethics, IIoT Regulations

2.2. *Curriculum Ecological Modeling*

This paper presents a curriculum ecosystem model, depicted in Fig. 2, which employs a Dynamic Onion Model to comprehensively outline a three-tier ecological framework for Industrial Internet security engineering.

1. Safety Engineering: Core functions as the theoretical framework, amalgamating safety science principles with Industrial Internet architecture and integrating the MITRE ATT&CK ICS threat intelligence library.

2. Technological Convergence: Layer develops industrial big data analytics and AI-driven risk prediction capabilities via technical modules such as safety system models (Bowtie/STAMP), industrial protocol security (OPC UA/Modbus TCP), and digital twin simulations.

3. Application of Scenarios: Layer converts technical skills into practical applications, like smart industrial security design and energy internet protection, utilising scenario injection procedures through open-source case repositories.

This tri-layered structure constitutes a 'Theory-Technology-Scenario' dynamic closed-loop system. Critically, this design directly enhances safety engineering education by: (1) ensuring foundational safety principles are modernized and relevant (Core Layer); (2) systematically bridging safety science with essential Industrial Internet technologies, enhancing students' interdisciplinary integration capabilities (Technology Convergence Layer); and (3) transforming knowledge into demonstrable competency through authentic, industry-aligned projects, significantly enhancing practical problem-solving skills and contextual understanding (Scenario Application Layer). The real-time data flow between layers enables iterative optimization, continuously enhancing the curriculum's alignment with technological advancements and industry needs.

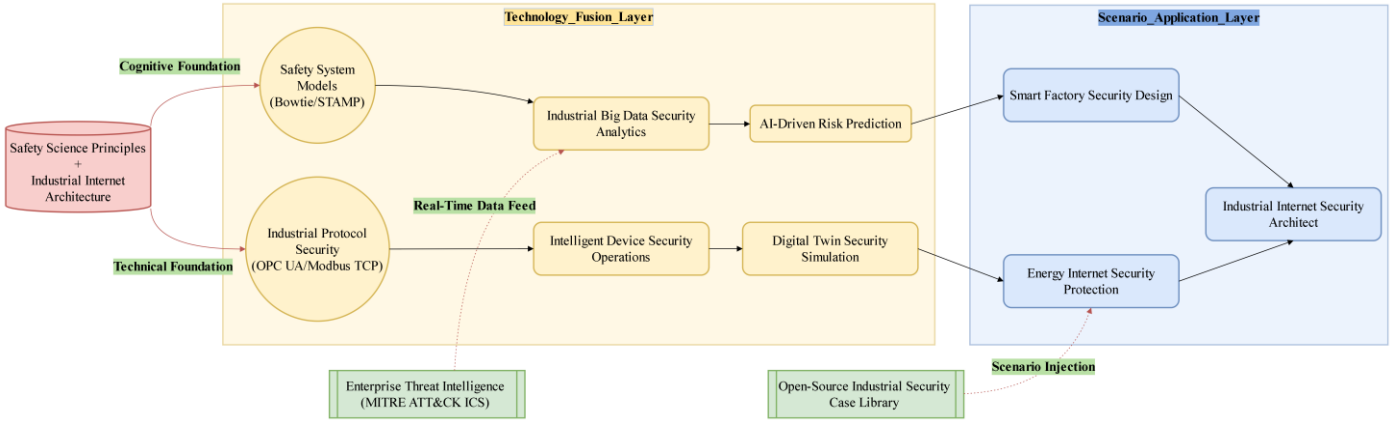

Fig. 2. Curriculum ecological design model.

2.3. *Curriculum Module Design*

2.3.1 Foundational Theory Module Cluster

The basic theory module cluster is the twin cornerstone for developing safety science literacy and Industrial Internet understanding in the ecological curriculum system for Industrial Internet security engineering education.

The Introduction to Industrial Internet Security serves as a foundational course that thoroughly examines the Industrial Internet of Things (IIoT), Time-Sensitive Networking (TSN), and 5G private networks. It offers students a comprehensive overview of the field, presenting initial insights into the technology framework and security prerequisites intrinsic to Industrial Internet ecosystems. The Safety Systems Engineering course effectively combines Bowtie models with Industrial Internet risk mapping, allowing students to methodically examine risk propagation pathways and mitigation strategies through a systems-thinking perspective, thus enhancing their analytical and design skills for intricate safety systems. The analysis of Industrial Control Protocol Security concentrates on prevalent protocols like OPC UA and Modbus TCP. By engaging in protocol reverse engineering and vulnerability mining exercises, students acquire deep understanding of the fundamental principles of protocol security mechanisms, enabling them to effectively discover and mitigate hidden security vulnerabilities in industrial control protocols.

This module cluster seeks to create a solid theoretical foundation, ensuring students have an organized cognitive framework and substantial theoretical literacy for advanced specialized studies and practical applications. It establishes the essential foundation for cultivating multidisciplinary experts skilled in safety science and Industrial Internet technologies. This module's pedagogical implementation employs a dual-track progressive model, as illustrated in Fig. 3.

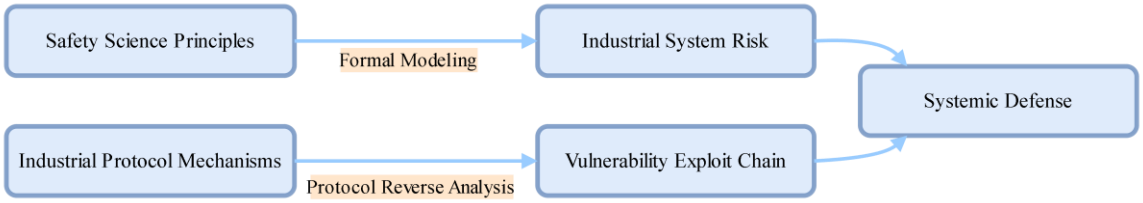

Fig. 3. Dual-Track progressive model.

2.3.2 Foundational Theory Module Cluster

To attain the cultivation goal of bidirectional "safety + IT" penetration capabilities, the Technology Convergence Module Cluster creates a complex curriculum framework, meticulously refining students' cross-domain technological integration skills. The precise layout of the Technology Convergence Module Cluster is outlined in Table 2.

Table 2. Technology convergence module cluster framework.

Module Type	Course	Technical Focus	Cultivated Competencies	Core Outcomes
Vertical Integration	Industrial Big Data Security Governance	• Spark secure computing	Vertical Integration	Industrial Big Data Security Governance
	Edge Computing Security Technologies	• MEC node protection	Edge Computing Security Technologies	• MEC node protection
Horizontal Integration	AI-Driven Industrial Safety Decision-Making	• Federated learning security	Horizontal Integration	AI-Driven Industrial Safety Decision-Making
	Industrial Digital Twin Security Modeling	• Unity3D/MATLAB simulation	Industrial Digital Twin Security Modeling	• Unity3D/MATLAB simulation
Synthetic Outcomes	-	Cross-domain technological convergence	• Transdisciplinary problem-solving	Synthetic Outcomes

1. Vertical Integration Programs

Industrial Big Data Security Governance emphasizes the secure administration of industrial big data, integrating Spark-based secure computing with privacy preservation methodologies. This provides students with robust processing and analytical skills for extensive industrial datasets, guaranteeing secure data transmission and adherence to regulations within Industrial Internet environments.

Edge Computing Security Technologies pertains to Multi-access Edge Computing (MEC) contexts, including node safeguarding techniques and efficient encryption methods. Students acquire the skills to establish security perimeters at data-proximate edge nodes, successfully addressing intricate security concerns encountered by industrial edge devices.

2. Horizontal Integration Programs

AI-Driven Industrial Safety Decision-Making utilizes federated learning security frameworks and anomaly detection algorithms, enabling students to improve the accuracy and sophistication of industrial safety choices via AI technologies. This facilitates prompt detection and alleviation of irregular security incidents.

Industrial Digital Twin Security Modelling employs Unity3D and MATLAB platforms to create digital twin settings for attack-defense simulations. Students acquire deep understanding of security vulnerabilities and countermeasures for industrial digital twin systems, facilitating proactive identification and prevention of hidden security threats.

3. Outcomes

Through deliberate interaction with this module cluster, students surpass conventional safety-IT disciplinary boundaries, developing complete technological convergence competencies. This offers strong technological support and creative frameworks for enhanced professional practice and the resolution of intricate security issues in Industrial Internet sectors.

Collectively, the Technology Convergence Module Cluster moves beyond traditional siloed learning, fundamentally enhancing safety engineering education by cultivating the critical ability to fuse safety science principles with cutting-edge Industrial Internet technologies. This enhanced cross-domain competency is essential for tackling the complex, technology-driven security challenges defining modern industrial ecosystems.

2.3.3 Scenario Application Module Cluster

The Scenario Application Module Cluster is closely aligned with the practical application scenarios of the Industrial Internet, aiming to transform students' theoretical knowledge into practical capabilities. Centered on project-based courses, this module cluster has been meticulously designed with diversified practical training components, as detailed in Fig. 4.

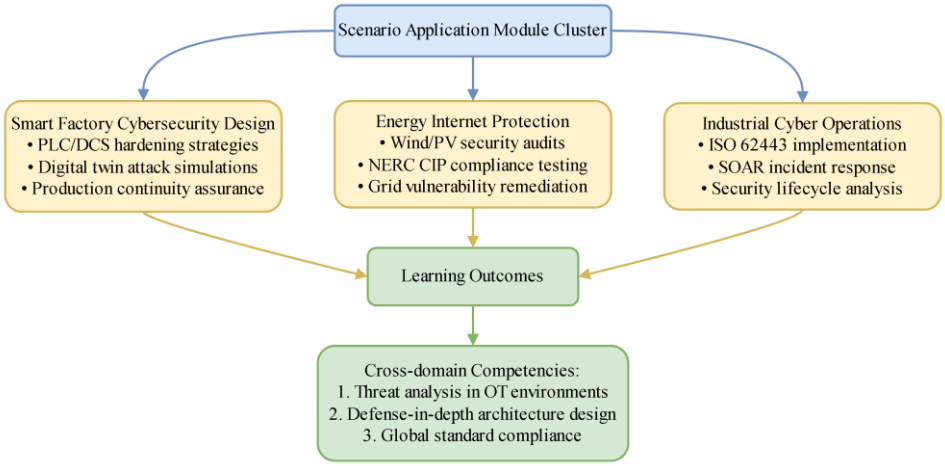

Fig. 4. Cybersecurity competency framework for industrial iot education.

The Smart Factory Cybersecurity Design emphasizes secure smart industrial settings. By engaging in real-world projects, students acquire the ability to identify and neutralise potential threats to smart factory control systems, thus gaining essential skills for ensuring the secure and stable functioning of production processes. The Energy Internet Protection course prepares students to evaluate the cybersecurity of renewable energy installations, identify and rectify security weaknesses, and guarantee the continuity and dependability of energy output. The Industrial Cyber Operations course highlights compliance management competencies. Students acquire expertise in essential components of security operations, including security monitoring, incident response, and emergency management, through practical experience and case studies, thereby equipping them to formulate efficient solutions for business security operations.

Through the Scenario Application Module Cluster, students develop practical skills across various typical industrial scenarios, thoroughly preparing them for professional jobs in the Industrial Internet security sector.

2.3.4 Practical Innovation Module Cluster

The Practical Innovation Module Cluster aims to offer students varied possibilities for practical innovation, enhancing their practical skills and inventive thinking in the realm of Industrial Internet security. This module cluster employs three implementation methods—"industry-academia collaboration platforms," "competition-driven mechanisms," and "innovation and entrepreneurship incubation"—to effectively assist students in applying their learnt knowledge to real-world situations. Students participate in frontline enterprise projects and practical industrial security initiatives through industry-academia collaboration platforms, gaining valuable experience while working alongside industry experts and engineers to expand their professional networks and perspectives. The competition-driven system enhances students' competitive awareness and innovative capabilities by facilitating participation in diverse Industrial Internet security competitions, hence fostering collaboration and problem-solving skills. Regarding innovation and entrepreneurship incubation, institutions furnish students with conducive entrepreneurial ecosystems and resources, promoting the creation of industrial security-related applications to convert innovative concepts into concrete products or services, thereby revitalising the Industrial Internet security sector.

3. Implementation Path and Safeguard Mechanisms

3.1. Phased Implementation Strategy

3.1.1 Short-Term Phase

In the short-term phase, initiatives focus on pilot programs and faculty development to establish a foundation for enhancing the curricular ecosystem. Core courses—such as Introduction to Industrial Internet Security and Safety Systems Engineering—are initially piloted with selected cohorts of second- and third-year undergraduate students. This phased implementation enables structured collection of student feedback and rigorous evaluation of pedagogical effectiveness, thereby facilitating continuous improvement of course materials and instructional strategies to inform scalable adoption. Concurrently, faculty expertise is strengthened through active participation in academic conferences on Industrial Internet security, industry immersion programs, and specialized technical training. Industry experts and corporate practitioners are engaged to deliver targeted lectures and workshops, equipping educators with cutting-edge subject-matter expertise and applied engineering competencies. These synergistic efforts cultivate a robust faculty cohort possessing both theoretical proficiency and practical acumen, ensuring faithful execution of the revised curriculum framework.

3.1.2 Medium-Term Phase

The medium-term goal is to create a "Industrial Internet + Security Laboratory" as a central platform for applied education and research innovation. The laboratory development plan is collaboratively designed with prominent companies in the Industrial Internet security sector to meet industrial requirements and technical advancements. The laboratory features sophisticated Industrial Internet devices, security systems, and specialized data analysis tools, facilitating experimental scenarios that replicate authentic industrial production settings, such as smart factory production lines, energy internet systems, and industrial big data platforms.

Utilising the laboratory, a range of practical courses and research projects—such as experiments for the Intelligent Factory Security Design Practice course and research on vulnerability detection and exploitation in Industrial Internet systems—are conducted. These programs facilitate students' enhancement of theoretical knowledge through practical application, foster extensive problem-solving abilities for intricate security issues, and offer hardware assistance for faculty research. Furthermore, they enable the conversion of research findings into practical applications, so augmenting the institution's impact in the Industrial Internet security sector.

3.1.3 Long-Term Phase

The effort seeks to create a cohesive ecosystem that integrates industry, academia, research, and application, utilising the curricular ecosystem to propel industrial progress in the long run. Expanding upon the Industrial Internet + Security Laboratory, collaboration with businesses and research institutions will be intensified to forge strong, long-term alliances. Collaborative initiatives with industry partners will concentrate on technology research and development, product innovation, and standardisation to tackle significant technical issues in Industrial Internet security, converting scientific advancements into tangible productivity. Faculty-directed student involvement in enterprise projects will offer internships and employment opportunities, allowing students to acquire practical experience and expand their professional prospects while supplying enterprises with proficient talent.

Moreover, enhanced collaboration with business associations and governmental bodies would promote active participation in the creation of industrial policy. Technical exchange events and industry forums will draw more participation from businesses and

research organisations, cultivating a holistic ecosystem that integrates education, research, industry, and application. This comprehensive strategy guarantees the reciprocal enhancement of talent development, technological advancement, and industrial progress, establishing a virtuous cycle that ensures sustainable growth in the Industrial Internet security industry.

3.2. Resource Safeguards

3.2.1 Policy Support

At the policy level, actively engaging with the Ministry of Education's Emerging Engineering Education (3E) Research and Practice Projects is essential for obtaining resource assurances. The 3E project emphasizes educational innovation and advancement in burgeoning engineering and technical domains, closely aligning with the establishment of the Industrial Internet Security Engineering Education curriculum ecosystem. The initiative seeks to obtain financial backing and regulatory approval from the Ministry by diligently crafting project applications that outline the ecosystem's innovation, practicality, and expected results. This method alleviates cost burdens associated with curriculum development, laboratory equipment acquisition, and faculty training, while simultaneously ensuring alignment with national educational reform initiatives. This alignment draws high-caliber resources to the subject, so creating a strong policy and budgetary basis for the methodical enhancement of the curriculum framework.

3.2.2 Industry Collaboration

Industry participation is an essential element of resource protection. Collaborating with pertinent firms to co-develop courses and internship programs facilitates profound integration of industry and academic resources. Partnering with prominent companies in the Industrial Internet security domain facilitates the co-development of practical course material grounded in real company processes and technical specifications. Industry experts may assist in the development of case studies for courses like Industrial Internet Security Operations, incorporating genuine project scenarios into educational materials to ensure conformity with industry standards and to familiarise students with advanced technologies and real-world operational contexts. Simultaneously, the creation of collaborative internship facilities offers students practical experience in genuine Industrial Internet environments. Enterprise mentors assist students in practical initiatives, such as Industrial Internet penetration testing and security system implementation, facilitating the acquisition of hands-on experience and improving employability. This collaborative methodology concurrently provides businesses with potential talent streams, resulting in mutually advantageous outcomes and enhancing industrial momentum in the ongoing refinement of the curricular environment.

3.2.3 Synergistic Effects of Policy Support and Industry Collaboration

Policy support and industrial partnership mutually reinforce one another, producing significant synergistic impacts. Policy assistance creates a conducive external environment and incentive structures for industrial collaboration. Government initiatives, such as tax incentives for industry-academia integration and specialized subsidies for university-enterprise collaboration programs, can diminish the expenses associated with corporate involvement in educational partnerships, consequently augmenting corporate engagement and excitement. The results and requirements arising from industry engagement provide tangible proof and strategic direction for policy enhancement. This allows policies to concentrate more accurately on essential areas and vulnerabilities in Industrial Internet security engineering education, thereby enhancing the policy framework, optimising resource distribution, and collectively offering extensive and sustainable resource protections for the development and execution of the curriculum ecosystem.

4. Discussion

4.1 Innovative Advantages

Within Industrial Internet contexts, 'security' encompasses both cyber-physical system protection (e.g., protocol vulnerabilities) and operational 'safety' assurance (e.g., accident prevention), addressing holistic risk landscapes. The proposed curriculum ecosystem represents a significant enhancement over traditional safety engineering education models, primarily through two key innovations that address long-standing deficiencies:

1. Rectifying the Conventional "Hardware-Centric" Bias in Safety Engineering Education: Historically, traditional safety engineering education has prioritised hardware security, neglecting software security. In the era of the Industrial Internet, software assumes an increasingly vital role in industrial systems. This curricular ecosystem amalgamates software and hardware security expertise with courses like Introduction to Industrial Internet Security and Edge Computing Security Technologies. For example, in the analysis of industrial control protocol security, students explore both hardware communication structures and software protocol

security techniques. This integration allows students to comprehensively assess security concerns from a systemic viewpoint, successfully closing the software security gap in traditional safety engineering education and developing experts prepared to meet contemporary industrial requirements.

2. Facilitating the Role Transition of Safety Engineers: In Industrial Internet contexts, safety engineers must transform from reactive "incident responders" to proactive "risk predictors." The courses in this ecosystem, such as AI-Driven Industrial Safety Decision-Making and Industrial Big Data Security Governance, focus on developing students' skills in using big data analytics and artificial intelligence for predictive risk assessment. These courses enable students to proactively identify potential dangers, devise preventive strategies, and mitigate the probability of safety events. This change raises the strategic importance of safety engineers and improves the operational stability of industrial systems via data-driven protections.

4.2 Implementation Challenges and Mitigation Strategies

Despite its innovations, the ecosystem faces critical implementation challenges:

Table 3. Implementation challenges and mitigation strategies.

Challenge	Specific Manifestations	Solutions
Faculty Competency Gaps	• 65% interdisciplinary knowledge deficit • 42% proficiency in industrial protocol analysis	• Industry-Academia Co-Training: Implement dual-appointment professorships (e.g., corporate security directors + academic supervisors)
Rapid Technological Shifts	• 1.5-year lag in curriculum updates vs. technological advancements	• Faculty Immersion Program: Mandate ≥160 annual industry engagement hours
Assessment Limitations	• Traditional exams fail to evaluatepractical ability • <30% quantifiable industry-academia outcomes	• Dynamic Curriculum Model: Gartner Hype Cycle-driven course iteration

Industrial Internet security engineering is an interdisciplinary domain necessitating that educators have substantial competence in the Industrial Internet as well as fluency in safety engineering principles and practices. Nonetheless, a shortage of faculty members proficient in both fields continues to exist among higher education institutions. Training such educators requires significant time and resource commitments, including involvement in technical training, academic conferences, and industrial immersion programs. Moreover, swift technical progress in the Industrial Internet and safety engineering requires ongoing faculty development to ensure the relevance and application of educational material.

Collaborative training programs between universities and industries, together with faculty immersion initiatives, effectively bridge competency gaps. Institutions may forge strategic alliances with Industrial Internet security firms to collaboratively develop frameworks for enhancing faculty capabilities. Industry specialists, acting as adjunct faculty, provide practical assistance and technical seminars through collaborative training, while faculty members partake in industrial immersion programs to engage in research and development projects and security management operations. This reciprocal engagement allows instructors to gain practical experience with advanced Industrial Internet security technologies, assimilate evolving industry demands through direct enterprise interaction, and incorporate genuine case studies and engineering practices into classroom instruction. These projects improve educational relevance and effectiveness, connecting academic theory with industry practice.

The contribution of industrial Internet to safety engineering education is reflected in three dimensions: (1) technology empowerment: real-time feedback of safety experiments through edge computing (such as millisecond response of pressure vessel stress monitoring experiments); (2) Ecological Connection: Building a secure data sharing platform between enterprises, universities, and regulatory agencies, such as collaborating with a petrochemical company to develop a teaching case of 'leak source localization algorithm'; (3) Cognitive upgrading: based on the predictive maintenance data of the industrial Internet, train students to transform their safety thinking from 'post disposal' to 'pre prevention'. "

This educational ecosystem strengthens the effectiveness of safety engineering education through a triple mechanism: (1) Security capability internalization: integrate industrial Internet security standards into core courses, such as adding the topic of

'functional security and information security integration' in Industrial Control System Security; (2) Coupling of technical scenarios: realize the linkage between virtual factories and physical equipment through the industrial Internet platform, for example, students simulate the emergency response of chemical leakage accidents in the digital twin system; (3) Knowledge iteration automation: use the OTA technical characteristics of the industrial Internet to establish a cloud based dynamic update mechanism for course content.

5. Conclusions

This study presents a novel framework for developing a safety engineering education ecosystem based on the Industrial Internet, targeting significant deficiencies in conventional teaching methodologies. The curriculum ecosystem integrates industry Internet technology with safety science concepts, creating a three-tiered "Theory-Technology-Scenario" framework that connects disparate disciplines and aligns educational results with industry requirements. The ecosystem's fundamental breakthroughs are in its dynamic adaptability, cross-domain convergence mechanisms, and scenario-driven practical immersion, successfully addressing the persistent gap between theoretical teaching and real-world industrial security concerns.

This framework delineates a clear roadmap for educational institutions through a phased implementation strategy, encompassing short-term course pilots and faculty development, medium-term establishment of an industrial internet and security laboratory, and long-term formation of an integrated ecosystem encompassing industry, academia, research, and application. The resource protections, encompassing regulatory assistance and industrial engagement, enhance the feasibility and sustainability of the environment.

This work addresses critical limitations in conventional safety engineering curricula—which prioritize generic workplace scenarios while neglecting Industrial Internet-specific threats—by establishing a purpose-built educational ecosystem. As depicted in Fig.1, traditional frameworks fail to develop competencies like industrial protocol security or AI-driven risk prediction. Our ecosystem directly fulfills industry's demand for interdisciplinary specialists through: (1) The dynamic "Theory-Technology-Scenario" framework（Fig.2） integrating safety science with Industrial Internet technologies; (2) Scenario-driven modules (Section 2.3.3) simulating real-world environments (e.g., smart factories, energy grids).These contributions substantiate our ecosystem's role in advancing industrial internet security education. It establishes a robust foundation for developing a new cohort of safety engineering professionals capable of adeptly navigating the security landscape of the industrial internet era, thereby fostering the sustainable advancement of China's industrial internet ecosystem and augmenting its global competitiveness.

Future endeavours will concentrate on expanding the ecosystem via cross-institutional partnerships and formulating standardized assessment metrics for transdisciplinary competency evaluation. This framework offers a theoretical basis and practical guide for global institutions aiming to match safety engineering education with the evolving requirements of Industrial Internet ecosystems.

Author Contributions: Conceptualization: H. Wu; Methodology: H. Wu, N. Yang; Data Collection and Analysis: H. Wu, N. Yang; Writing – Original Draft: H. Wu; Writing – Review and Editing: H. Wu, N. Yang; Supervision: H. Wu.

Funding: This research was supported by the Nantong Institute of Technology through the research project Optimization of Fire Emergency Response and Evacuation Strategies in Subway Stations (Grant No. 2024XK(Z)25).

Acknowledgments: We appreciate and thank all participants involved in this research whose contributions were invaluable to the completion of this study.

Conflicts of Interest: Competing interests The authors declare no competing interests.

References

1. Bjelland, H., Gehandler, J., et al. (2024). Tunnel fire safety management and systems thinking: Adapting engineering practice through regulations and education. *Fire Safety Journal*, 146, 104140. https://doi.org/10.1016/j.firesaf.2024.104140
2. Osborne, M., et al. (2024). Understanding safety engineering practice: Comparing safety engineering practice as desired, as required, and as observed. *Safety Science*, 172, 106424. https://doi.org/10.1016/j.ssci.2024.106424
3. Selepe, R. L., Makinde, O. A., & Munyai, T. T. (2025). Application of Fourth Industrial Revolution technologies to enhance supply chain sourcing: A systematic literature review. *Journal of Transport and Supply Chain Management*, 19(0), e1–e10. https://doi.org/10.4102/jtscm.v19i0.1111
4. Stoiber, C., & Schönig, S. (2024). Leveraging the industrial internet of things for business process improvement: A metamodel and patterns. *Information Systems and e-Business Management*, 22(2), 285–313. https://doi.org/10.1007/s10257-024-00676-0
5. Tang, C., Wu, X., et al. (2022). Research on the development of the industrial internet in the post-epidemic era. *Industrial Engineering and Innovation Management*, 5(13). https://doi.org/10.23977/IEIM.2022.051305

6. Velichko, Y. V., Igaikina, I. I., & Kulakova, E. V. (2025). Contemporary approaches to safety studies in engineering education. *Journal of Machinery Manufacture and Reliability*, 53(Suppl 2), S239–S242. https://doi.org/10.1134/S1052618824701565
7. Wang, B., Peng, J., & Cui, M. (2024). Secure access technology for industrial internet of things. *Concurrency and Computation: Practice and Experience*, 36(25), e8231. https://doi.org/10.1002/cpe.8231
8. Woodrow, M., Gillen, A. L., et al. (2020). Investigating varied pedagogical approaches for problem-based learning in a fire safety engineering course. *International Journal of Engineering Education*, 36(5), 1605–1614.