Received: 29 Apr. 2026 | Revised: 02 May. 2026 | Accepted: 06 May. 2026 | Published online: 25 May. 2026

RESEARCH ARTICLE

Contemporary Education and Teaching Research
2026, Vol. 7 (5)145-149
DOI: 10.61360/BoniCETR262020070503

Reform of Laboratory Safety Education Curriculum for Information Undergraduate Majors Based on AI

Yiyu Liu[1,*]
[1]*College of Artificial Intelligence, Neijiang Normal University, P.R. China*

Abstract: By analyzing the current curriculum syllabus of laboratory safety education for several information undergraduate majors in a university, it is found that the current curriculum system has some problems, such as the lack of differentiation based on major content, serious homogenization and so on. From the risk characteristics of all aspects faced by the information laboratory, this paper puts forward a set of modular curriculum reform ideas of "multi unit and professional promotion". The idea is to reform and optimize the curriculum system, teaching methods and evaluation mechanism. The purpose is to provide a theoretical framework and implementation ideas for the transformation of laboratory safety education of information undergraduate specialty from homogeneous teaching to professional characteristics, which will promote the curriculum reform in Colleges and universities, and has positive significance.

Keywords: local universities, information laboratory, construction dilemmas, reform strategies

1. Introduction

With the rapid development of information technology, especially AI technology, the security of university information specialty laboratory is facing great challenges. In addition to the traditional physical security and data security, its security risks also extend to emerging fields such as ethical security and algorithm security, with compound risk characteristics. Through the preliminary analysis of the 2023-2025 "laboratory safety education" curriculum syllabus of several information undergraduate majors in a university, it is found that the current laboratory safety education curriculum system and the contents of the professional courses are almost the same in terms of teaching objectives and content settings, and the homogenization phenomenon is obvious, which fails to adapt to the changes of the times in time, and also fails to fully reflect the differentiated risk needs of various majors based on safety.

From the perspective of the content of the existing laboratory teaching materials, they are mostly concentrated in the field of traditional science and engineering, focusing on the safety of physical meaning, such as fire safety, gas safety, equipment safety, instruments and equipment (Huang & Zhao, 2021; Li, 2022). With the progress of the times, many colleges and universities have opened artificial intelligence related majors, and the professional teaching content of the traditional information specialty has been constantly updated.

The construction of related laboratories is endless, but the research on safety education is relatively lacking. From a practical perspective, most colleges and universities are limited by teachers and other factors, so it is difficult to meet the needs of students of different majors for professional safety knowledge and skills, and still adopt the "one size fits all" safety education mode. Therefore, it has important theoretical value and practical significance to systematically analyze the problems of the existing curriculum system, face the characteristics of each specialty, and reconstruct the laboratory safety education system differently.

2. Status Analysis

The current syllabus of laboratory safety education for software engineering, computer science and technology, intelligent science and technology, and artificial intelligence majors in a university was reviewed, and the course objectives and teaching contents were compared and analyzed.

2.1. Course objectives

The course syllabus of these four majors has characteristics for the description of the "course objectives" part:

The goal focuses on "Mastering the basic

Corresponding Author: Yiyu Liu
College of Artificial Intelligence, Neijiang Normal University, P.R. China

knowledge of security" and "cultivating security awareness". There is no specific description of the characteristics of each major. The characteristics of homogeneity are obvious. Some cutting-edge professional complete problems, such as algorithmic ethics of artificial intelligence and data privacy, are not reflected in the syllabus of relevant majors.

In addition, the relevance between teaching objectives and teaching requirements is not clear. For example, the artificial intelligence specialty is associated with "design/development solutions", with a weight of 0.5. For example, the principle that software engineering majors associate the course objectives with "using modern tools", with a weight of 0.25, different relevance and different teaching requirements, is not reflected. This shows that different majors have different understanding of the positioning of safety education, and there are obvious differences in the design of the supporting relationship for the curriculum objectives.

2.2. Comparative analysis of teaching content structure

The teaching contents of the four majors adopt the "six lecture system" structure, and the theoretical teaching contents (4 class hours) are: overview of safety education, fire safety, electricity safety and information safety. The practical teaching contents (4 class hours) are: fire fighting and escape drill and emergency rescue technology; None of them reflected the characteristic content of combining specialty. The four syllabuses are completely consistent in terms of chapter setting, class hour allocation and key points of content, and have the characteristics of general laboratory safety education course (Li, 2022), ignoring the essential differences in equipment types, use scenarios and risk characteristics of information laboratories. It has formed an obvious phenomenon of "content homogeneity".

2.3. Analysis of the lack of risk coverage dimension

From the perspective of laboratory security risks involved in the four outlines, it mainly focuses on physical security (fire protection, power consumption) and basic network security, and lacks the increasingly important dimensions of data security, algorithm security, and ethical security in information laboratories. Especially in the major of artificial intelligence, emerging risks such as algorithm bias, data privacy and model security are not fully reflected in the course content, and the risk coverage is insufficient (Shen, 2021).

3. Theoretical Basis and Design Principles of Reform Assumption

The curriculum reform envisages taking "compound risk response" and "professional ability construction" as the core guidance, combining with the characteristics of engineering education certification (Higher Education Steering Committee of the Ministry of Education, 2018), integrating compound risk theory, professional education theory and ability based education concept, and following the principles of "systematicness, diversity, practicality and foresight", aiming to build a curriculum system that can not only lay a solid foundation for safety and general education, but also deepen professional risk cognition and enhance comprehensive practical ability (Wang & Liu, 2021).

3.1. Theoretical basis

The construction of curriculum reform is based on the following three theories:

The first is the compound risk theory. The security risks of information laboratories are multidimensional, interrelated and dynamic. There are risks such as physical equipment security, data leakage, algorithm bias and ethical anomie, and they may be intertwined and cause and effect each other, such as physical intrusion on the server, equipment damage, data theft, model leakage and privacy ethical issues (Du, 2024). Therefore, the safety education of information laboratory needs to go beyond the traditional single dimension and build a new risk cognition framework, so that students can understand and deal with such complex risk scenarios.

The second is the theory of professional education. Laboratory safety education should distinguish its risk types and prevention and control focus according to the professional characteristics of different specialties in the laboratory environment, technical tools and application scenarios, not stay in the general safety knowledge education, and realize the deep integration with professional characteristics. For example, AI majors need to focus on data privacy and algorithm interpretability, human ethics (Du, 2024), while software engineering majors pay more attention to code security and supply chain risk management. The theory of professional education requires that the curriculum design reflect the discipline characteristics and realize the transformation from "universal discipline" to "professional empowerment" (China Engineering Education Professional Certification Association, 2024).

The third is the concept of ability based education. The concept emphasizes the guidance of students' actual safety ability, and guides students to actively build a safety knowledge system through project practice, reflection and discussion, case simulation, etc., so as to improve their problem-solving ability and decision-making literacy in dynamic and complex environments (Liu & Yang, 2025).

3.2. Design principles

Based on the above theory, the reform follows the following four design principles:

(1) Systematic

The course should form a teaching system that is progressive layer by layer and connected before and after, covering the whole process of laboratory safety education from cognition, protection to literacy. For example, when introducing data security, we should introduce encryption methods, guide students to understand data ethics and social responsibility, and realize the integrated education of knowledge, ability and values.

(2) Difference

The risk characteristics of laboratory use scenarios of each specialty are also different, and the design of teaching module should be professional and targeted. For example, the specialty of intelligent science and technology has set up the topic of "system security and physical protection", and the specialty of artificial intelligence has added the unit of "algorithm fairness" to avoid the "one size fits all" teaching content.

(3) Practicality

Pay attention to integrating theory with practice, combine real case analysis and simulation training, and improve students' practical ability and emergency response level. For example, in the "network security foundation" module, the attack and defense simulation platform can be introduced to allow students to practice vulnerability screening and security reinforcement operations.

(4) Forward looking

The course content should have a certain degree of risk predictability and timely incorporate emerging risk types and protection technologies. For example, with the popularity of artificial intelligence, in-depth forgery detection, AI-generated content security verification and other content need to be supplemented to ensure that educational content and technology development are updated simultaneously.

4. Core Content of Reform Assumption

4.1. Curriculum system design of "basic multi unit and professional promotion"

The following three-tier modular curriculum structure will be reconstructed while keeping the total 8 class hours unchanged:

(1) Level 1: core module of compound risk foundation (3 class hours)

It aims to help students establish an overall understanding of the risks in five aspects of physics, network, data, algorithm and ethics of information laboratories, and master basic safety specifications and general emergency skills.

Module 1: new cognition of laboratory safety in the information age (1 class hour)

Combining with the security accident of scientific research data leakage caused by vulnerability intrusion in a university data center, this paper systematically explains the connotation and relationship of five aspects of risk, and guides students to think that it engineers in the information age should bear ethical responsibilities in system development, and strengthen their social responsibility and legal awareness (Anderson, 2020).

Module 2: infrastructure and general protection technology (1 class hour)

Combined with physical demonstration and video teaching, explain the laboratory power wiring specification, fire equipment operation, network basic topology and firewall configuration. Students can carry out practical training such as "circuit overload troubleshooting" or "network access control strategy configuration" through the simulated operation platform to consolidate the basic protection skills at the physical and network levels.

Module 3: emergency foundation and safety culture cultivation (1 class hour)

Design scenario simulation activities such as laboratory fire evacuation and data recovery emergency, and organize students to complete role play tasks in groups. After the drill, carry out reflection and discussion, summarize the deficiencies in emergency response, and discuss how to build a continuous improvement safety culture through daily code of conduct, Safety log management and other means.

(2) Level 2: professional characteristic risk module (3 class hours)

Taking the artificial intelligence specialty as an example, the risk module with the specialty characteristics is given below for differentiated and in-depth safety knowledge teaching and practical training.

Data and model security unit (1.5 class hours): it involves the introduction of the principles of

privacy protection technology such as lifecycle management, and the theory of security threats such as reverse attacks. Use open source tools (such as IBM AI fairness 360) to try to generate confrontation samples to understand the model vulnerability (National Institute of Standards and Technology [NIST], 2018) and other practical aspects.

Algorithmic ethics and governance unit (1.5 class hours): analyze cases of real ethical disputes and guide students to explore algorithmic fairness (Laine et al., 2025).

(3) Level 3: interdisciplinary comprehensive practice module (2 class hours)

Through the interdisciplinary cooperation project, cultivate students' ability to comprehensively use various safety knowledge to solve complex problems, such as the design project: "integrated safety planning of intelligent laboratory".

The project requirement is to design an intelligent laboratory security scheme supporting AI training and software development, covering five aspects of physics, network, data, algorithm and ethics. Through the implementation of such projects, students can integrate the knowledge learned by each module and understand the laboratory security strategies from different professional perspectives.

4.2. Innovative design of teaching methods

In order to complete the above curriculum system, the following three types of teaching method reforms are proposed:

(1) Deepening the application of case teaching method

With the support of the college project, the subject case library corresponding to each major is built, and each module contains a number of real cases. During the teaching process, attention is paid to the four steps of case introduction, risk identification, multi scheme deduction and summary and refinement, so as to cultivate students' independent analysis and decision-making ability.

(2) Integrated application of virtual simulation technology

Develop modular virtual experiment resources, such as "data privacy protection simulation environment". Design progressive training tasks, and gradually transition from cognitive experiment to comprehensive experiment. Through the online and offline hybrid mode, students can learn the basic operation by themselves through the virtual platform before class, and the classroom time will focus on the difficulty discussion and teacher guidance.

(3) System design of project based learning

The project tasks represented by "intelligent laboratory safety planning" emphasize authenticity, openness and collaboration. The teacher's role has changed from a knowledge imparter to a project consultant, guiding students to continuously improve the program through periodic review, group discussion, etc.

4.3. Reform and design of evaluation system

In order to support the effective operation of the curriculum system, we should simultaneously promote the reform of teaching methods and evaluation mechanism. In terms of teaching methods, a hybrid teaching mode of "case leading, simulation supporting and project driving" is constructed. In terms of evaluation mechanism, a three-dimensional comprehensive evaluation system of "knowledge skills literacy" is established to highlight the ability orientation. In terms of knowledge understanding, the weight accounts for 30%, which is evaluated by unit tests, written assignments, classroom questions, etc. the main assessment is: mastery of core concepts, depth of principle understanding, etc. Skill application: the weight accounts for 40%, which is evaluated by means of experimental report, project results, simulation exercise performance, etc. the main assessment is: the standardization of tool operation, the effectiveness of problem solving, etc; In terms of literacy performance: the weight accounts for 30%, which is evaluated by means of teacher observation records, reflection logs, peer review questionnaires, etc. the main assessment includes: safety awareness, responsibility attitude, team cooperation ability, etc.

5. Implementation Path and Guarantee Mechanism

The curriculum reform involves a wide range of knowledge and content. It needs organizational guarantee, resource guarantee and system guarantee. It will be steadily promoted in four stages of "preparation - Development - Pilot - promotion", and the implementation plan for each stage will be formulated. At the initial stage, an interdisciplinary teaching team was established to complete the demand survey and standard setting; In the medium term, we will focus on the development of modular teaching materials, cases and simulation resources, and carry out teacher training; In the later stage, pilot teaching was carried out in 1-2 specialties to collect feedback and optimize the design, and finally gradually extended to the whole hospital.

6. Analysis of Expected Results and Challenges

The expected results of this curriculum reform

are as follows: (1) change the previous homogeneous teaching appearance and form the differentiated curriculum content of "one major and one policy"; (2) Improve students' ability to identify, assess and deal with professional related risks; (3) To build an iterative and reproducible laboratory safety education mode, and provide practical reference for similar colleges and universities. If the above reform is implemented, it may face challenges such as insufficient teaching resources, long resource construction cycle, complex multi-disciplinary coordination, and insufficient teachers' ability. It is necessary to plan corresponding training support, step-by-step construction, and flexible management strategies.

7. Conclusion

The construction of modular curriculum system is the core of this reform idea. Based on practical teaching and ability evaluation, it responds to the practical problems such as lack of professionalism and lack of practicality faced by the laboratory safety education of information specialty in the era of compound risks. Through innovative design and step-by-step implementation, it is expected to promote the transformation of laboratory safety education curriculum from theoretical to professional and competency, realize the deep integration of safety education and professional training, and provide systematic support for the cultivation of new engineering talents with high risk awareness and comprehensive protection ability.

Conflict of Interest

The author declares that he has no conflicts of interest to this work.

Acknowledgement

This research was funded by: The key project of the Sichuan provincial education informatization application and development research center of the Sichuan Provincial Department of Education, "Research on the new mode of talent cultivation of colleges and universities" (No. jyxx19-007).

References

Anderson, R. Security Engineering (2020).*A Guide to Building Dependable Distributed Systems (3rd ed.)*. Wiley Press.

China Engineering Education Professional Certification Association (2024). *Engineering education certification standard.* (2022-05) https://www.ceeaa.org.cn/.

Du Yanyong (2024). *Artificial intelligence ethics case collection* . Shanghai People's publishing house.

Higher Education Steering Committee of the Ministry of Education (2018). *National standard for teaching quality of undergraduate majors in Colleges and universities (Part I)* . Higher Education Press.

Huang, Zhibin, & Zhao, Yingsheng (2021). *General course of laboratory safety in Colleges and universities*. Nanjing University Press.

Laine, J., Minkkinen, M., & Mäntymäki, M (2025). Understanding the Ethics of Generative AI: Established and New Ethical Principles. *Communications of the Association for Information Systems*, 56: 1-25.

Li, Haihong (2022). *Laboratory safety and management* . Chemical Industry Press.

Liu Li, Yang Lei (2025). The dilemma and way out of the undergraduate teaching reform of "student centered". *Education and Teaching Forum,* (46): 73-76.

National Institute of Standards and Technology (NIST) (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)* . Gaithersburg, MD: U.S. Department of Commerce.

Shen Yushi (2021). *Artificial intelligence ethics and security*. Beijing: Tsinghua University Press.

Wang Jing, Liu Yong(2021).Research on the innovation of university laboratory safety education system under the background of new engineering. *Experimental technology and management, 38* (5): 1-5.

How to Cite: Liu, Y. (2026). Reform of Laboratory Safety Education Curriculum for Information Undergraduate Majors Based on AI. *Contemporary Education and Teaching Research, 07*(05), 145-149.
https://doi.org/10.61360/BoniCETR262020070503