Partnering with Community College Faculty to Co-Design Intelligent Tutoring Systems for Cybersecurity Workforce Training

Anonymous Name
Anonymous Institution
City
Country
anonymous@institution.edu

Anonymous Name
Anonymous Institution
City
Country
anonymous@institution.edu

Anonymous Name
Anonymous Institution
City
Country
anonymous@institution.edu

Abstract

This experience report describes a partnership between community college faculty and learning scientists to co-design Intelligent Tutoring Systems (ITSs) addressing challenges in cybersecurity workforce training. Our co-design approach combined collaborative reflection on student difficulties from prior course offerings with systematic curricular analysis to identify high-impact intervention points. We targeted two challenge areas: strengthening students' ability to contrast key cybersecurity taxonomies, and providing realistic hands-on training without costly infrastructure. The resulting ITSs include: one employing exercises that scaffold comparison of conceptual categories, and another using lightweight simulations to provide experiential learning while circumventing typical cost and time overhead. Both systems incorporate instructional principles grounded in learning science research, including evidence-based features associated with ITS efficacy such as timely hints and feedback. Through iterative classroom deployment and refinement—including adding task-loop adaptivity to offer repeated practice until mastery—we observed encouraging learning outcomes, alongside insights into mitigating "gaming the system" behaviors. We detail our co-design process and formative evaluations—procedures, outcomes, and cautious interpretation due to the limited number of consented learners—and share lessons learned to inform scalable, replicable ITS development for cybersecurity workforce training in resource-constrained settings.

CCS Concepts

• **Social and professional topics** → **Adult education**; **Computing education**; • **Applied computing** → **Interactive learning environments**.

Keywords

Intelligent tutoring systems, community colleges, cybersecurity, computer science education, learning analytics

Conference'17, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

ACM Reference Format:
Anonymous Name, Anonymous Name, and Anonymous Name. 2025. Partnering with Community College Faculty to Co-Design Intelligent Tutoring Systems for Cybersecurity Workforce Training. In . ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Community colleges in the United States play a vital role in workforce training, particularly in addressing the growing demand for cybersecurity professionals, and are accessible to tens of millions of American workers. They have proven effective in teaching technical subjects, generating returns comparable to four-year programs [30]. However, these institutions face significant resource constraints [18, 28, 34], motivating the adoption of effective and scalable teaching methods such as Intelligent Tutoring Systems (ITSs).

2 Related Work

2.1 ITS and Adaptive Learning

Extensive research supports the efficacy of ITSs. For example, Kulik and Fletcher's meta-analysis reported that ITS implementations consistently outperform traditional classroom instruction, with the largest gains when assessments are locally developed and aligned with instructional objectives [27]. Similarly, VanLehn's meta-analysis found that the average effect size of ITSs across domains is on par with human tutoring [35]. One evidence-based approach to designing effective ITSs is to incorporate adaptive learning following the "Adaptivity Grid" framework by Aleven et al. [3], which delineates three forms of adaptivity: (i) *step-loop adaptivity* (within a problem), where the system responds to individual student actions within an instructional task; (ii) *task-loop adaptivity* (between problems), where the system personalizes subsequent tasks for the learner; and (iii) *design-loop adaptivity* (between material versions), where course designers update the content and system based on data-driven reflection. This three-tiered framework has guided many empirical studies examining how different forms of adaptivity affect learning outcomes. In particular, research shows that when task-loop adaptivity is incorporated effectively, they can accelerate learning by tailoring subsequent practice based on individual progress [8, 13, 26].

2.2 Co-Design with Community College Faculty

Co-design is a collaborative design method that involves stakeholders as partners throughout the design process, rather than as "sources of information" [33]. In educational contexts, researchers

collaborate with instructors and other stakeholders to design educational tools, environments, or materials. This approach centers the voices, needs, and experiences of instructors and learners. Successful co-design with instructors requires building trust, establishing safe spaces, and incorporating flexibility into the design process [22]. An example of successful co-design is Lumilo, an augmented reality tool co-designed with instructors that supports real-time monitoring of student engagement and performance in intelligent tutors [17]. In computing education, successful co-design has also been demonstrated through instructors' self-reported personal and professional growth, along with their recognition of the method's value [11, 20]. Also, researchers have partnered with community college faculty to collaboratively revise math lessons [14] and design content for combating misinformation [22]. These collaborations fostered trust and produced well-aligned educational materials.

3 Our Iterative Instructional Co-Design

This section details our iterative co-design approach for developing ITSs to enhance community college cybersecurity workforce training. We outline a replicable collaboration process between faculty and learning scientists, informed by faculty teaching experiences, research literature, and community college resource constraints.

3.1 Instructional Design Context

The target learner population comprises students at a large, public two-year community college located in a populous urban county in the northeastern United States. Our instructional co-design grounds in the authentic needs of a core cybersecurity course serving both workforce certificate and associate degree pathways. Positioned midway through these programs, this course functions as a critical gateway to advanced cybersecurity topics, building upon prerequisite coursework in networking and system administration. Course objectives are aligned with those specified for CompTIA Security+ [16], a foundational credential widely recognized in the cybersecurity job market, and also approved by the U.S. Department of Defense (DoD) to fulfill directive 8140/8570.01-M requirements [9].

3.2 Identification of Actionable & High-Impact Intervention Opportunities

Given the resource constraints faced by community colleges, our co-design approach strategically begins by identifying high-priority cybersecurity concepts and skills before investing substantial effort in ITS implementation. We identify high-impact intervention opportunities through two complementary approaches: collaborative reflection on student struggles and systematic curricular analysis.

3.2.1 Collaborative Reflection on Student Struggles. The first approach involved structured discussions with faculty to surface persistent student difficulties observed across multiple semesters. Alongside regular meetings between learning scientists and community college faculty throughout the project, we conducted focused collaborative reflection sessions to identify and document key student struggles. These pain points were derived from faculty insights and longitudinal observations of student difficulties across multiple semesters. To systematically structure our co-reflection sessions and document outcomes, we developed a framework (detailed in Table 1) that facilitates documenting student struggles and ranking their priority based on instructional impact.

Table 1: Student Struggle Identification Framework

Column	Description
Week	Course week when topic is taught
Learning Objective	Measurable competency defined with Bloom's taxonomy [25] (e.g., "Analyze", "Interpret")
Evaluation Method	Assessment instruments (e.g., graded assignments, quizzes)
Difficulty Level	Faculty rating of difficulty (high/medium/low)
Curricular Relevance	Faculty rating of relevance to future coursework in certificate/associate degree curricula (critical/important/less important/not relevant)
Workforce Relevance	Faculty rating of relevance in real-world jobs (critical/important/less important/not relevant)
Additional Notes	Qualitative insights on specific challenges and contextual factors

This structured process culminated in a tangible artifact documenting 35 distinct learning objectives with which students struggled in the cybersecurity course. This artifact then served as the foundation for subsequent co-design activities and the prioritization of ITS development.

3.2.2 Systematic Curricular Analysis. Building on the collaborative identification of 35 distinct learning objectives where students struggled, we employed systematic curricular analysis to strategically prioritize objectives for ITS development based on two criteria: *high instructional impact* and *feasibility within resource constraints*. This analysis comprised two key components: first, we utilized curriculum mapping—a systematic method for evaluating and aligning course content with desired learning outcomes to ensure coherent knowledge progression [21, 31]; second, we decomposed high-level learning objectives into fine-grained knowledge components (KCs) that align with ITS granularity requirements. KCs represent discrete cognitive functions that can be attained through learning events and observed through assessments [24]. Through this process, we identified two primary types of student struggles along with their associated instructional challenges and opportunities for ITS intervention (detailed in Table 2).

These gaps represented high-leverage opportunities for ITS intervention, informing the design and development of two ITSs: the first tutor scaffolds contrastive reasoning for conceptual distinctions through tailored exercises; the second provides experiential learning through lightweight simulations that replicate workplace tasks while circumventing high costs and time requirements. The following sections detail each tutor's design features, deployment in classroom settings, evaluation outcomes, and how reflective insights informed iterative refinements.

3.3 Security Control Tutor: Conceptual Distinctions through Contrastive Reasoning

During the ITS design phase, faculty and learning scientists collaboratively analyzed the course textbook (CompTIA Security+ Cert Guide [16]) to identify instructional gaps contributing to student

Table 2: Instructional Challenges Identified through Systematic Curricular Analysis and Corresponding ITS Solutions

Student Struggle Theme	Contextual Factors Faced by Community College Students	High-Impact Example	Solution Using ITS
Comparing taxonomies	Business-as-usual textbook lacks tailored instructional design for understanding/contrasting taxonomies	Comparing security control types and categories	Scaffolding contrastive reasoning through tailored exercises
Developing practical skills	Delivering realistic cybersecurity experiences is typically expensive and infeasible for community colleges	Detecting, analyzing, and remedying DDoS attacks	Providing experiential learning through lightweight simulations of workplace tasks

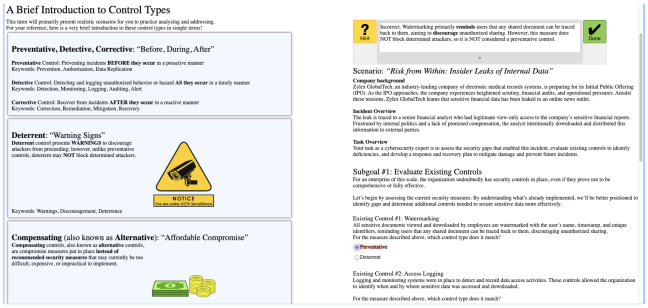

Figure 1: Security Control Tutor. Left: Introduction to taxonomies using plain language with comparative scaffolding, supplemented by visual aids. Right: Active learning components. Top-right: Hint box providing multi-level hints, and immediate misconception-targeted feedback. Bottom-right: scenario-based MCQs requiring contrastive reasoning.

difficulties. This analysis revealed a recurring pedagogical limitation of the textbook: it confines cybersecurity taxonomies to isolated subsections without comparison across them. For example, in Chapter 1 each control type (e.g., preventive, detective, corrective) is introduced in its own subsection, with definitions and examples presented independently. Likewise, each control category (e.g., managerial, operational, technical) is presented in isolation without any comparison. This gap is particularly consequential given its misalignment with target assessments—the textbook's evaluation instruments rely heavily on classification-based multiple-choice questions (MCQs). For example, 17 of 20 questions in Chapter 1's pre/post quizzes required students to classify functional descriptions or contextual examples into specific taxonomy terms (e.g., "What control category is designed to increase individual and group system security?" or "What control type is intended to discourage someone from violating policies?"). To address this gap, the Security Control Tutor (as illustrated by Figure 1) was developed to scaffold contrastive reasoning to meet assessment requirements by presenting exercises in which learners compare and justify classifications across categories within authentic scenarios.

3.3.1 Evaluation of First Iteration. The Security Control Tutor was developed using the Cognitive Tutor Authoring Tools (CTAT) [1, 2] and first deployed in Fall 2024 within a cybersecurity course enrolling 19 students. The course was offered in both in-person and remote modalities, with 12 students attending in-person and 7 participating remotely. To explore the efficacy of ITS, we conducted a small-scale randomized controlled trial (RCT) using a between-group pre-post design. Students in the experimental group used the Security Control Tutor, while those in the control group engaged with digitally presented CompTIA Security+ textbook content via the CTAT platform. Though presented as a CTAT problem set, the control condition lacked core ITS features: it provided no tailored multi-level hints or targeted feedback. Instead, answers from the textbook's answer section were used to serve as both hints (upon request) and feedback (after incorrect attempts). Two distinct yet equivalent 10-item quizzes served as pre- and post-tests. No feedback (including correctness) was given during the pre-test. This evaluation design aimed to mitigate potential biases and ensure any observed differences in learning outcomes could be attributed to the ITS intervention, rather than variations in assessment difficulty or practice effects from the pre-test. Learning logs generated in both the experimental and control conditions were collected in DataShop [23] to support our evaluation.

Five students (4 experimental and 1 control) consented to the use of their learning data for research purposes and completed all required learning activities. Table 3 shows individual pre-test and post-test scores for these participants.

Table 3: Pre/Post Results for Security Control Tutor

Condition	Student	Pre-test (%)	Post-test (%)
Experimental	S1	20	30
Experimental	S2	30	20
Experimental	S3	70	70
Experimental	S4	40	100
Control	S5	60	50

Given the limited sample size (n=5), we emphasize these results should be interpreted as exploratory rather than conclusive. 4 participants showed minimal change (±1 correct answer on a 10-item test), while we note with encouragement that 1 student in the experimental condition (S4) improved dramatically from 40% to 100%. This outcome is encouraging in that it suggests the ITS, when maximally utilized, may potentially support substantial learning gains for some learners. However, the lack of improvement in the majority of participants indicates that further investigation is needed to understand the factors that mediate the effectiveness of the tutor.

3.3.2 Engagement as a Potential Mediator of ITS Efficacy. To better understand the observed variation in learning outcomes, we analyzed student interaction patterns to infer (dis)engagement behaviors that might mediate ITS efficacy. This analytical approach

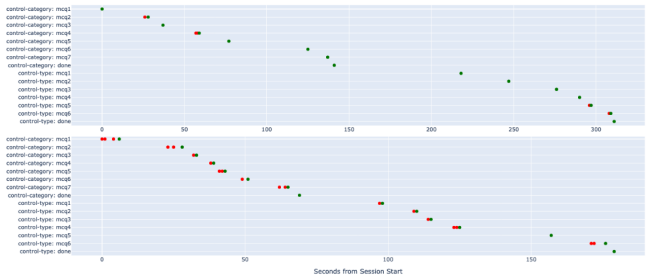

Figure 2: Representative learning events timelines for learners using the Security Control Tutor. The horizontal axis indicates seconds from session start; the vertical axis lists practice steps. Each marker denotes a step attempt: green for correct and red for incorrect. The upper panel shows the interaction of the high-performing learner (S4), while the lower panel shows a learner with minimal gain (S1), characterized by repeated incorrect attempts on multiple steps.

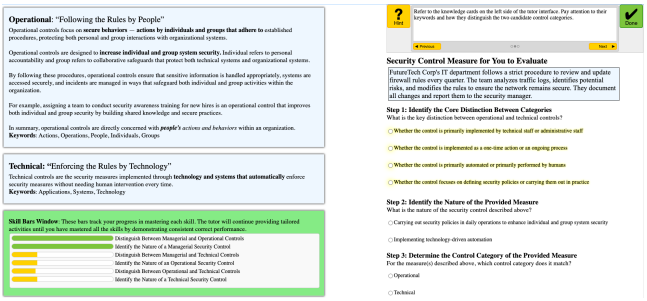

Figure 3: Refined Security Control Tutor. Bottom-left: Skill bars track mastery progress for each skill, enabling adaptive practice selection. Bottom-right: Contrastive reasoning restructured into a scaffolded three-step comparison process. Top-left: Instructional content area maintains previous layout with refined material. Top-right: Hint box retains original layout but features updated hints and feedback aligned with the three-step reasoning process.

was informed by extensive prior research examining student misuse of ITS. "Gaming the system" behaviors—where students exploit system features to progress without learning—are consistently documented across ITS studies, with 10–40% of students engaging in such behaviors at least intermittently [4]. Critically, these behaviors are associated with poorer learning gains [6, 7], potentially explaining why one student achieved perfect performance while others showed minimal change despite identical instructional exposure.

One established method for identifying disengagement is to employ machine learning. For instance, Baker et al. [5] engineered 24 features from ITS logs to train a Latent Response Model [29] for detecting student misuse of ITSs. However, we opted against this approach due to its reliance on large datasets (e.g., 70 students in [5]'s study)—a requirement incompatible with our small sample size. We therefore adopted human-defined heuristics inspired by [15, 32], which offer interpretable indicators of disengagement that maintain transparency while accommodating our data constraints.

To operationalize this approach, we visualized fine-grained interaction data through timeline views, inspired by [12] who demonstrated that timeline visualizations of learning events can yield meaningful and actionable insights worthy of investigation for faculty. Figure 2 contrasts representative timelines.

We want to emphasize that these patterns should not be interpreted as conclusive evidence, but rather as potential signals for instructors to investigate further and intervene as appropriate. These patterns should also not be used to dichotomize students into "successful" versus "unsuccessful" learners, since some students whose timeline patterns resemble those associated with successful outcomes nevertheless show minimal knowledge gains. That said, our community college faculty reviewed these learning-event timelines and agreed that certain patterns may indicate disengagement. Consistent with Du et al.'s [12] approach, we treat learning-event timelines as one component of a holistic assessment rather than relying on them alone for definitive conclusions. For example, triangulating multiple data points for S1—including substantially lower time-on-task (179 seconds, $z = -1.20$) compared to the group mean (300.75 seconds, $SD = 101.66$), low pre-test scores (indicating limited prior knowledge), and minimal learning gain—led faculty to identify this learner as potentially at-risk. Based on this multifaceted evidence, the faculty deemed follow-up conversations and interventions as appropriate pedagogical responses.

3.3.3 Instructional Refinement Through Co-Design. Informed by the "Adaptivity Grid" framework by Aleven et al.[3] (discussed in Section 2.1), the learning scientist and faculty collaborated to systematically incorporate evidence-based features into the tutor, leveraging all three adaptivity loops. In the initial iteration of the Security Control Tutor, we implemented comprehensive *step-loop* adaptivity through multi-level hints and targeted feedback to address common misconceptions. Subsequent analysis of learner outcomes informed a redesign with several added features, including *task-loop* adaptivity: by integrating Bayesian Knowledge Tracing [10], an algorithm that continuously updates its estimate of a learner's skill mastery based on real-time performance, the refined tutor is able to tailor subsequent practice activities until mastery is achieved. This data-driven refinement process also exemplifies *design-loop* adaptivity. Figure 3 illustrates this refined iteration, with the added features described in the caption.

3.3.4 Evaluation of Second Iteration. To evaluate the refined tutor, we deployed it in the Spring 2025 offering of the cybersecurity course with 9 enrolled students, employing a mixed-methods evaluation approach. Quantitatively, we maintained the between-group pre-post design from the first iteration. Students in the experimental condition used the enhanced Security Control Tutor, while the control group again engaged with the digitally presented CompTIA Security+ textbook content. While preserving the structure of two equivalent quizzes, we conducted a new round of KC modeling that identified one quiz item assessing multiple KCs simultaneously. This item was replaced with three separate questions, each targeting a single KC, increasing the total quiz items from 10 to 12.

4 students (2 experimental and 2 control) consented to the use of their learning data for research purposes and completed required

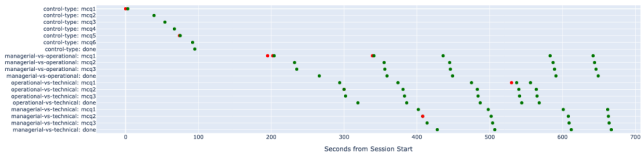

Figure 4: Representative learning-event timeline for a high-performing learner using the refined Security Control Tutor with task-loop adaptivity. The horizontal axis indicates seconds since session start; the vertical axis lists individual practice steps. Each marker denotes a step attempt (green for correct, red for incorrect). The repeated markers on steps illustrates repeated practice until mastery is achieved.

activities. Table 4 shows individual pre-test and post-test scores for these participants. Of the two students in the experimental group, one improved substantially and achieved a full score on the post-test, while the other showed no gain. Both students in the control group demonstrated moderate gains.

Table 4: Pre/Post Results for Refined Security Control Tutor

Condition	Student	Pre-test (%)	Post-test (%)
Experimental	S1	66	100
Experimental	S2	58	58
Control	S3	75	91
Control	S4	66	83

To visualize learner engagement, we generated timeline views of student interactions. Figure 4 illustrates the learning-event timeline for the high-performing experimental student (S1). The timeline shows repeated practice on steps until mastery was achieved, demonstrating the task-loop adaptivity in action. We also examined the timeline for the experimental student who showed no gain (S2) but did not observe notable differences in the interaction pattern compared to the high performer.

Given the small sample size, we supplemented our evaluation by collecting open-ended responses from students in the experimental group after using the tutor. The feedback revealed several themes regarding the perceived strengths and weaknesses of the tutor.

When asked what they liked about the tutor, one student (S1) reported that "it was useful that it targeted topics that need improvement dynamically," and the other (S2) described the tutor as "very engaging, instead of just reading books." Additionally, when asked how the tutor aided their learning of the cybersecurity taxonomies , S1 stated, "The tutor helped me learn about the managerial, operational, and technical categories. The explanation and question/knowledge verification features helped clarify for me." S2 noted, "The way the tutor gave out questions and examples really helped." When particularly asked about task-loop adaptivity, both participants characterized it as "helpful." S1 added that "it's useful to target areas of weak understanding," and S2 noted that they "learned a lot from the practice." Meanwhile, both students commented that the practice "was repetitive," and S2 commented that the tutor asked "too much of the same question." These responses indicate that while students appreciated the dynamic personalization, the existing question pool, containing three distinct scenarios per KC, may require further diversification to mitigate perceptions of repetition.

3.3.5 Summary. In this section, we detailed the co-design and refinement of the Security Control Tutor to bridge the gap between textbook presentations of cybersecurity taxonomies and the contrastive reasoning required for certification-aligned assessments. We evolved the tutor from providing step-level scaffolding to incorporating task-loop adaptivity that tailors practice to individual mastery levels. While limited sample sizes warrant cautious interpretation, we observed promising outcomes, including perfect post-test performance for some students, alongside overall positive feedback on the tutor's adaptive features. Meanwhile, student feedback regarding scenario diversity highlighted clear opportunities for further refinement to mitigate perceptions of repetition associated with repeated practice via task-loop adaptivity. This co-design process demonstrates that faculty-researcher collaboration can yield instructional innovations aligned with both learning needs and institutional constraints.

3.4 DDoS Incident Response Tutor: Lightweight Simulations for Experiential Learning

Besides conceptual challenges like comparing taxonomies, our co-design process identified a second critical instructional challenge: the expense and logistical complexity of delivering realistic cybersecurity experiences in community college settings. To address this, we developed a DDoS Incident Response Tutor that provides experiential learning through lightweight simulations of workplace tasks within an ITS framework. Similar to the Security Control Tutor, this second tutor underwent two design iterations. Our design aligns with recent recommendations by Choi et al. [30], who advocate that experiential learning and technical simulation are two foremost instructional design strategies to promote transfer of skills acquired in classroom to the workplace. In this section, we highlight its unique features, the challenges encountered, and the co-design solutions we implemented.

Figure 5 illustrates the DDoS Incident Response Tutor, which simulates IT infrastructure under a DDoS attack without requiring physical or cloud resources. Developed in collaboration with faculty, the tutor guides students through a systematic workflow to detect, analyze, respond to, and reflect on a DDoS attack—a high-priority workforce competency identified through curriculum mapping.

3.4.1 Evaluation of First Iteration. We first deployed this tutor in the Spring 2025 offering of the cybersecurity course, employing the same between-group pre–post evaluation design used for the initial Security Control Tutor iteration. All the 9 enrolled students (5 experimental and 4 control) consented to the research and completed required learning activities. Table 5 shows individual pre-test and post-test scores. We observed results similar to those in the first iteration of the Security Control Tutor: one student in the experimental condition (S2) improved substantially, achieving a perfect post-test score, while all other participants in both groups showed minimal change (±1 correct answer on the 10-item test).

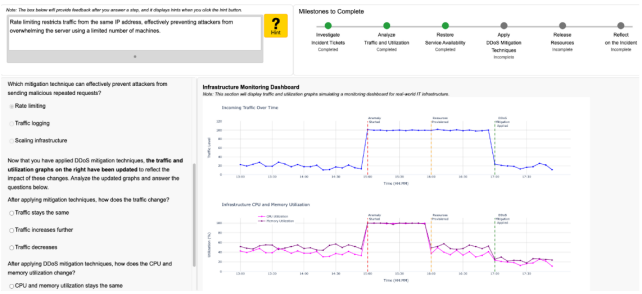

Figure 5: DDoS Incident Response Tutor. Top left: hint box offering multi-level hints and immediate feedback. Top right: milestone tracker segments the complex DDoS response workflow into milestones and indicates student progress for reflection. Bottom left: steps for the current milestone guides the student through the procedure. Bottom right: simulation dashboard presenting interactive network-traffic and resource-utilization graphs that update in response to mitigation techniques applied by students.

Table 5: Pre/Post Results for DDoS Incident Response Tutor

Condition	Student	Pre-test (%)	Post-test (%)
Experimental	S1	40	50
Experimental	S2	70	100
Experimental	S3	50	60
Experimental	S4	60	60
Experimental	S5	60	70
Control	S6	70	60
Control	S7	70	80
Control	S8	70	70
Control	S9	70	80

3.4.2 Instructional Refinement Through Co-Design. We also generated student interaction timeline views to visualize learner engagement. Figure 6 contrasts representative examples. Mirroring findings in Security Control Tutor, some students with negligible learning gains exhibit patterns of repeated mistakes across multiple steps. However, other students, despite patterns resembling those linked to successful outcomes, show minimal knowledge gains.

Based on previous data-driven reflection from the Security Control Tutor and similar observations of student "gaming the system" behaviors, faculty recognized the value of also integrating task-loop adaptivity into this DDoS Incident Response Tutor. However, implementing task-loop adaptivity in this tutor presented a unique challenge. Traditionally, task-loop adaptivity selects subsequent practice items from a pool based on associated KC—for example, presenting a "managerial versus operational control" problem when the KC for contrasting those categories has not yet been mastered. In contrast, this tutor employs a single many-step problem covering all KCs. Repeating this monolithic problem until all KCs were mastered would risk overpractice. To address this, we modified the static interface so that it dynamically adapts to skill-mastery estimates. Once learners complete the initial practice rounds, the system may initiate additional rounds. In these extra rounds, any step associated with a skill already marked as mastered is automatically completed, enabling learners to focus solely on steps requiring

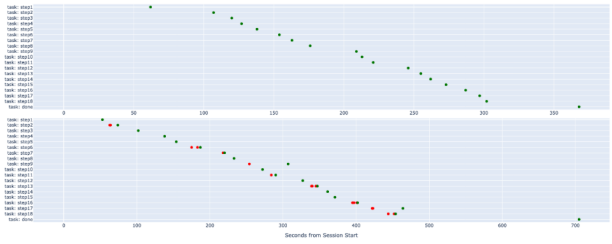

Figure 6: Representative learning events timelines for learners using the DDoS Incident Response Tutor. The horizontal axis indicates seconds from session start; the vertical axis lists practice steps. Each marker denotes a step attempt: green for correct and red for incorrect. The upper panel shows the interaction of the high-performing learner (S2), while the lower panel shows a learner with minimal gain (S5), characterized by repeated incorrect attempts on multiple steps.

further practice. When all skills reach mastery, completing that round marks the activity as finished. This dynamic interface design draws inspiration from on dynamic ITSs such as that of Huang et al. [19], presenting additional fine-grained steps only when learners struggle with complex tasks, thereby supporting integration and preventing overpractice of mastered fundamental KCs. While our solution similarly updates the interface in response to performance, our implementation operates at the task-loop by (disabling steps when skills are mastered), whereas [19]'s approach operated at the step-loop (by providing immediate scaffolding in response to errors). Though fully implemented and faculty-reviewed, this second iteration awaits classroom evaluation—a focus of future work.

4 Conclusion

Community college faculty face a critical practical question: not just whether evidence-based instructional innovations *could* improve learning, but whether they are *feasible* and *worthwhile* given pervasive resource constraints. While our small-N evaluations (totaling 18 consented participants among 28 enrolled students) preclude definitive statistical conclusions, this experience report demonstrates how iterative co-design between learning scientists and faculty can yield actionable insights within these constraints.

Our work produced two key contributions: (1) a replicable co-design process for identifying high-impact intervention opportunities through collaborative reflection and curricular analysis, and (2) two tangible ITS implementations whose designs may extend to other contexts: one scaffolding conceptual distinctions, and the other providing experiential learning via lightweight simulations.

We share our co-design approach, tutor implementations, and formative evaluation procedures—with cautious interpretation of outcomes—to enable replication. By treating small-N studies as an inherent characteristic of community college settings rather than a mere limitation, we present how faculty–researcher partnerships can adapt pedagogical innovations to real-world constraints. We hope these insights contribute to a shared understanding within the CSEd community and inform the development of scalable, context-sensitive instructional innovations for workforce training in community colleges.

References

[1] Vincent Aleven, Bruce McLaren, Jonathan Sewall, and Kenneth R Koedinger. 2009. Example-tracing tutors: A new paradigm for intelligent tutoring systems. (2009).

[2] Vincent Aleven, Bruce M McLaren, Jonathan Sewall, and Kenneth R Koedinger. 2006. The cognitive tutor authoring tools (CTAT): Preliminary evaluation of efficiency gains. In Intelligent Tutoring Systems: 8th International Conference, ITS 2006, Jhongli, Taiwan, June 26-30, 2006. Proceedings 8. Springer, 61–70.

[3] Vincent Aleven, Elizabeth A McLaughlin, R Amos Glenn, and Kenneth R Koedinger. 2016. Instruction based on adaptive learning technologies. Handbook of research on learning and instruction 2 (2016), 522–560.

[4] Ryan Baker, Jason Walonoski, Neil Heffernan, Ido Roll, Albert Corbett, and Kenneth Koedinger. 2008. Why students engage in "gaming the system" behavior in interactive learning environments. Journal of Interactive Learning Research 19, 2 (2008), 185–224.

[5] Ryan Shaun Baker, Albert T. Corbett, and Kenneth R. Koedinger. 2004. Detecting Student Misuse of Intelligent Tutoring Systems. In Intelligent Tutoring Systems, David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Dough Tygar, Moshe Y. Vardi, Gerhard Weikum, James C. Lester, Rosa Maria Vicari, and Fábio Paraguaçu (Eds.). Vol. 3220. Springer Berlin Heidelberg, Berlin, Heidelberg, 531–540. doi:10.1007/978-3-540-30139-4_50 Series Title: Lecture Notes in Computer Science.

[6] Ryan Shaun Baker, Albert T Corbett, Kenneth R Koedinger, and Angela Z Wagner. 2004. Off-task behavior in the cognitive tutor classroom: When students" game the system". In Proceedings of the SIGCHI conference on Human factors in computing systems. 383–390.

[7] Ryan Shaun Baker, Ido Roll, Albert T Corbett, and Kenneth R Koedinger. 2005. Do performance goals lead students to game the system?. In AIED. 57–64.

[8] Matthew L Bernacki, Meghan J Greene, and Nikki G Lobczowski. 2021. A systematic review of research on personalized learning: Personalized by whom, to what, how, and for what purpose (s)? Educational Psychology Review 33, 4 (2021), 1675–1715.

[9] CompTIA Partners. 2025. CompTIA Security+ certification overview. https://partners.comptia.org/certifications/security Accessed June 14, 2025.

[10] Albert T Corbett and John R Anderson. 1994. Knowledge tracing: Modeling the acquisition of procedural knowledge. User modeling and user-adapted interaction 4 (1994), 253–278.

[11] Diego Dermeval and Ig Ibert Bittencourt. 2020. Co-designing gamified intelligent tutoring systems with teachers. Revista Brasileira De Informática Na Educação 28 (2020), 73–91.

[12] Jiameng Du, Yifan Song, Mingxiao An, Marshall An, Christopher Bogart, and Majd Sakr. 2022. Cheating Detection in Online Assessments via Timeline Analysis. In Proceedings of the 53rd ACM Technical Symposium on Computer Science Education - Volume 1 (Providence, RI, USA) (SIGCSE 2022). Association for Computing Machinery, New York, NY, USA, 98–104. doi:10.1145/3478431.3499368

[13] Luke G Eglington and Philip I Pavlik Jr. 2023. How to optimize student learning using student models that adapt rapidly to individual differences. International Journal of Artificial Intelligence in Education 33, 3 (2023), 497–518.

[14] Susan R. Goldman, Andrea Gomoll, Hall Hmelo-Silver, Cindy, Allison Hall H., Monica Mon-Lin Ko, Angela Joy Fortune, Eleni A. Kyza, Andrea Agesilaou, Kimberly Gomez, Louis Gomez, and Emily Pressman. 2019. Technology-Mediated Teacher-Researcher Collaborations: Professional Learning Through Co-Design. In The International Conference on Computer-Supported Collaborative Learning (CSCL).

[15] Yue Gong, J Beck, Neil T Heffernan, and Elijah Forbes-Summers. 2010. The impact of gaming (?) on learning at the fine-grained level. In Proceedings of the 10th International Conference on Intelligent Tutoring Systems (ITS2010) Part, Vol. 1. 194–203.

[16] Lewis Heuermann. 2024. CompTIA Security+ SY0-701 Cert Guide. Pearson IT Certification.

[17] Kenneth Holstein, Bruce M. McLaren, and Vincent Aleven. 2019. Co-Designing a Real-Time Classroom Orchestration Tool to Support Teacher–AI Complementarity. Journal of Learning Analytics 6, 2 (2019), 27–52.

[18] Harry J Holzer, Rachel Lipson, and Greg Wright. 2023. Community Colleges and Workforce Development: Are They Achieving Their Potential? (2023).

[19] Yun Huang, Nikki G. Lobczowski, J. Elizabeth Richey, Elizabeth A. McLaughlin, Michael W. Asher, Judith M. Harackiewicz, Vincent Aleven, and Kenneth R. Koedinger. 2021. A General Multi-method Approach to Data-Driven Redesign of Tutoring Systems. In LAK21: 11th International Learning Analytics and Knowledge Conference. ACM, Irvine CA USA, 161–172. doi:10.1145/3448139.3448155

[20] Gayithri Jayathirtha, Gail Chapman, and Joanna Goode. 2024. Holding a Safe Space with Mutual Respect and Politicized Trust: Essentials to co-designing a justice-oriented high school curricular program with teachers. In Proceedings of the 2024 on RESPECT Annual Conference (Atlanta, GA, USA) (RESPECT 2024). Association for Computing Machinery, New York, NY, USA, 215–223. doi:10.1145/3653666.3656090

[21] Helen S Joyner. 2016. Curriculum mapping: A method to assess and refine undergraduate degree programs. Journal of Food Science Education 15, 3 (2016), 83–100.

[22] Eunhye Grace Ko, Rotem Landesman, Jason C Young, Ahmer Arif, Katie Davis, and Angela D. R. Smith. 2025. Domain Experts, Design Novices: How Community Practitioners Enact Participatory Design Values. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25). Association for Computing Machinery, New York, NY, USA, Article 800, 16 pages. doi:10.1145/3706598.3714060

[23] Kenneth R Koedinger, Ryan SJd Baker, Kyle Cunningham, Alida Skogsholm, Brett Leber, and John Stamper. 2010. A data repository for the EDM community: The PSLC DataShop. Handbook of educational data mining 43 (2010), 43–56.

[24] Kenneth R Koedinger, Albert T Corbett, and Charles Perfetti. 2012. The Knowledge-Learning-Instruction framework: Bridging the science-practice chasm to enhance robust student learning. Cognitive science 36, 5 (2012), 757–798.

[25] David R Krathwohl. 2002. A revision of Bloom's taxonomy: An overview. Theory into practice 41, 4 (2002), 212–218.

[26] Kunyanuth Kularbphettong, Pubet Kedsiribut, and Pattarapan Roonrakwit. 2015. Developing an adaptive web-based intelligent tutoring system using mastery learning technique. Procedia-Social and Behavioral Sciences 191 (2015), 686–691.

[27] James A. Kulik and J. D. Fletcher. 2016. Effectiveness of Intelligent Tutoring Systems: A Meta-Analytic Review. Review of Educational Research 86, 1 (March 2016), 42–78. doi:10.3102/0034654315581420

[28] Oleg Legusov, Rosalind Latiner Raby, Leping Mou, Francisca Gómez-Gajardo, and Yanan Zhou. 2022. How community colleges and other TVET institutions contribute to the United Nations sustainable development goals. Journal of Further and Higher Education 46, 1 (2022), 89–106.

[29] Eric Maris. 1995. Psychometric latent response models. Psychometrika 60, 4 (1995), 523–547.

[30] Judeth Oden Choi, Rotem Guttman, Matthew Kisow, Carolyn Rosé, William Nichols, James Winyard, Bruce Li, Lee Branstetter, and Lauren Herckis. 2025. Bridging the Community College Cybersecurity Classroom and Workplace with the CyberSim Lab. In Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (Pittsburgh, PA, USA) (SIGCSETS 2025). Association for Computing Machinery, New York, NY, USA, 875–881. doi:10.1145/3641554.3701834

[31] Monday U Okojie, Mert Bastas, and Fatma Miralay. 2022. Using Curriculum Mapping as a Tool to Match Student Learning Outcomes and Social Studies Curricula. Frontiers in Psychology 13 (2022), 850264.

[32] Luc Paquette, Adriana MJB de Carvalho, and Ryan Shaun Baker. 2014. Towards Understanding Expert Coding of Student Disengagement in Online Learning. In CogSci.

[33] Juan Pablo Sarmiento and Alyssa Friend Wise. 2022. Participatory and Co-Design of Learning Analytics: An Initial Review of the Literature. In LAK22: 12th International Learning Analytics and Knowledge Conference (Online, USA) (LAK22). Association for Computing Machinery, New York, NY, USA, 535–541. doi:10.1145/3506860.3506910

[34] Aleksandr Sergeyev, Mark Bradley Kinney, Scott A Kuhl, Nasser Alaraje, Mark Highum, and Prince Mehandiratta. 2019. University, Community College, and Industry Partnership: Revamping Robotics Education to Meet 21st Century Workforce Needs–NSF-sponsored Project Final Report. In 2019 ASEE Annual Conference & Exposition.

[35] Kurt VanLehn. 2011. The relative effectiveness of human tutoring, intelligent tutoring systems, and other tutoring systems. Educational psychologist 46, 4 (2011), 197–221.