

# Introducing Security in a Chemical Engineering Design Course Using Adaptive Online Learning

Ken Debelak, Larry Howard, Yuan Xue, Christina Lee, Janos Sztipanovits  
Vanderbilt University,  
Nashville, TN 37235 [kenneth.a.debelak@vanderbilt.edu](mailto:kenneth.a.debelak@vanderbilt.edu)

**Abstract** - The Education program of the NSF TRUST Science and Technology Center aims to develop and disseminate on-line learning resources that can be used by educators to address security issues in multiple disciplines and multi-disciplinary contexts. We report on a pilot project for this approach where an on-line module was created to introduce security issues in a chemical engineering capstone design course. The module teaches concepts developed for computer system security, specifically role-based access control, using a pedagogical approach known as anchored instruction. Adaptation is used in this module at multiple levels. At the design level, the module is based on an instructional design pattern for anchored inquiry that is independently reusable for other applications of this teaching style. At the content level, adaptive techniques are used to specialize learning resources for the module's audience. A web-based learning platform adaptively scaffolds learners as they progress through a set of learning activities in solving an overarching challenge. We reflect on the process of creating this module and discuss issues for creating other adaptive resources for TRUST.

*Index Terms* – chemical plant security, role-based access control, adaptive learning, instructional design patterns, TRUST STC.

## INTRODUCTION

In May of 2005 the Chemical Industry Data Exchange (CIDX) published its "Guidance for Addressing Cyber-Security in the Chemical Industry" [1] whose purpose is to guide and educate its chemical industry members and the public about cyber-security in the chemical industry. It included a self-assessment section and examples of implementations of cyber-security in the chemical industry. CIDX, a non-profit organization dedicated to improving the ease, speed and cost of securely conducting business electronically in the Chemical Industry, is the standards body responsible for developing cyber-security chemical sector guidance and practices.

The chemical industry has a history of proactively addressing safety issues. Since 9/11, through organizations like CIDX and the Cyber Security Information Sharing Forum (CISF) [2], the chemical industry has taken voluntary steps to share and implement best practices in both the areas of physical plant security and cyber security. These organizations and others, e.g., Center for Chemical Process Safety (CCPS),

have tried to establish industry-wide strategies that seek to establish standards for information and process control security.

Our senior capstone design course in chemical engineering is designed to teach students to investigate alternative choices in the design of a chemical process by developing the ability to design a system, component, or process to meet desired technical, economic, safety, and environmental criteria. A systematic procedure for the conceptual design of a process is introduced. The goal is to synthesize the best process. Since processing costs associated with various process alternatives can differ by an order of magnitude or more, the alternatives need to be carefully screened. Students approach this problem of analysis and synthesis through discussion of a hierarchy of design decisions. In this approach a complex process is decomposed into a number of smaller problems that are easier to handle. By focusing on the decisions that must be made on each level, existing technologies that could be used to solve the problem can be reviewed and an appropriate process configuration chosen. The best time to introduce and discuss safety issues is during this design phase. A principal objective in the design and operation of chemical processes is to maintain safe operating conditions for plant personnel and its neighbors. In the context of plant safety, cyber security will be among the issues new engineers will face during their careers. Since many engineering students have not had to think about cyber-security issues, we believed that the senior design course would be a good place to bring these issues to their attention. We began with the issue of access control.

Access control is the process of controlling who or what resources can access premises and systems and the type of access permitted. The misuse of data and systems may have serious consequences, including harm to human life, environmental damage, financial loss, and damaged corporate reputation. These risks are increased when employees, contractors or temporary personnel have unnecessary access to data and systems. With most chemical plants under some form of computer control, the minute to minute safe operation of the plant requires only authorized personnel access to these systems. As the plant distributed control systems become more integrated into the hierarchical structure, they can interact with scheduling, financial, marketing, and other systems of networked computers. Add the increased use of wireless sensors and other wireless field instruments to the network, the requirements for who has access to what systems, and

what systems are allowed/supposed to exchange data, the need for a robust strategy for cyber security and access control becomes a necessity.

There is a real time aspect to access control and an off-line aspect. The off-line activity is the first step in the process and includes defining the user privileges and resource needs for the user. These are based upon the role of the user and the job to be performed. The off-line process includes an approval step by a responsible party before the user account is configured to provide the proper access. The real time aspects of access control are the sequential steps of authentication and authorization. These take place at the time of the user request to access information. Authentication is generally the prerequisite to authorization.

In this paper, we describe the process of designing an online learning module that teaches access control concepts to chemical engineering students in our capstone design course. The design was a collaboration between a chemical engineering faculty member and participants from the Team for Research in Ubiquitous Secure Technology (TRUST), an NSF-funded Science and Technology Center (STC). We begin by introducing the TRUST STC and the objectives of its education program in enhancing security-related education. We proceed by describing role-based access control, a collection of concepts originating in computer system security that form the core of the instruction provided by the module. We then describe the module's pedagogical approach, provide a brief description of the learning technologies used to design and deliver it to learners, and the process of developing the module using these learning technologies. We conclude by reflecting on this design experience and discuss the implications for creating future security-related online modules for dissemination by TRUST.

#### TRUST SCIENCE AND TECHNOLOGY CENTER

The TRUST STC brings together an interdisciplinary team of researchers drawing on the expertise at Berkeley, Carnegie Mellon, Cornell, Stanford and Vanderbilt. The research agenda of the Center is motivated by the confluence of two parallel trends: a rapid increase in computer security attacks at all levels and the rapidly growing integration role of computing and communication in critical infrastructure systems, such as financial, energy distribution, telecommunication and transportation, which now have complex interdependencies rooted in information technologies. These trends make computer and network security an essential part of system design in all engineering disciplines, which presents strong challenges for engineering education. Our goal is to integrate security components into the engineering curriculum not as an "add-on" or a separate computer security course, but as an integral part of a discipline-specific secure systems science.

Security is not solely a technical issue, nor is it simply an information technology issue. Part of the mission of the education program of TRUST is to provide educational materials that can be used to raise awareness of security issues

in multiple domains and in multidisciplinary contexts. Whenever possible, it is desirable that these materials be provided by adapting existing materials rather than developing entirely new materials. The module design presented in this paper was pursued as a pilot study of this approach. And more than simply the reuse, by adaptation, of existing learning materials, this module reflects a transfer of concepts firmly established in information system security to the domain of chemical plant security. In the next section, we review these concepts.

#### ROLE-BASED ACCESS CONTROL

Role based access control (RBAC), as introduced in 1992 by Ferraiolo and Kuhn[3], has become the predominant model for advanced access control because it reduces the complexity and cost of security administration in large networked applications. In RBAC, users are granted membership into roles, access permissions are assigned to roles based on their responsibilities within the organization. The operations that a user is permitted to perform are based on the user's role. The relationship among user, role, and permissions are illustrated in Figure 1.

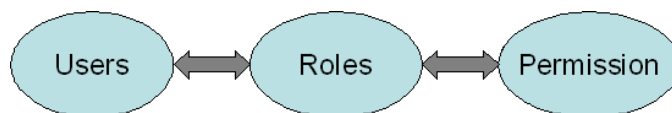


FIGURE 1: ROLE-BASED ACCESS CONTROL

The process of defining roles is usually based on analyzing the fundamental goals and structure of an organization and is usually linked to the security policy. Role hierarchies are used to organize roles to reflect authority, responsibility, and competency. For instance, as shown in Figure 2, in a chemical process control context the different roles of users may include process engineer, control engineer, process operator, etc.

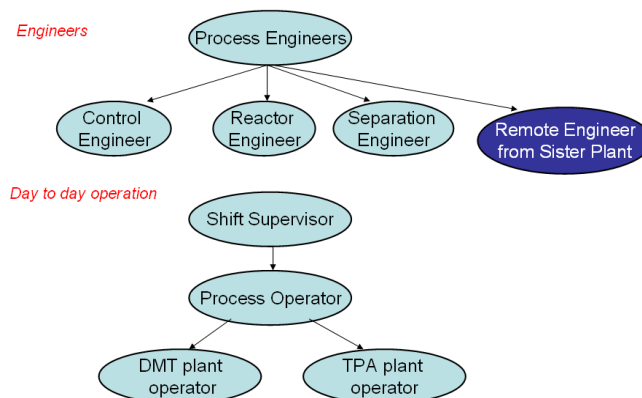


FIGURE 2: ROLE HIERARCHY IN CHEMICAL PROCESS CONTROL

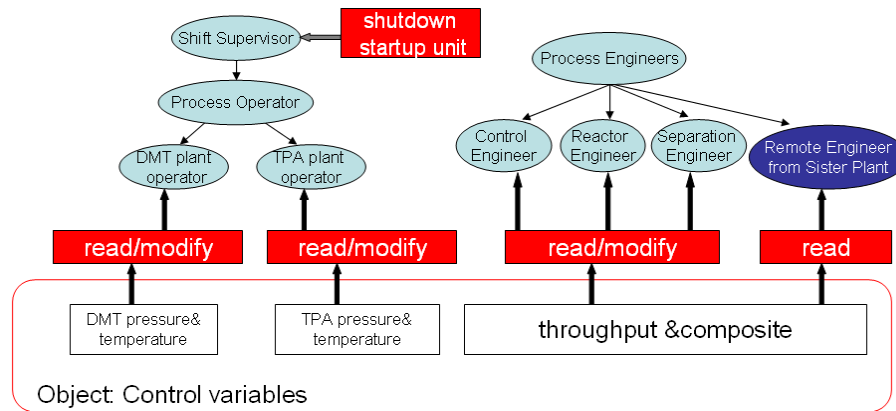


FIGURE 3: PERMISSIONS ASSIGNED TO ROLES IN A CHEMICAL PLANT

Obviously, these users require different levels of access permissions in order to perform their functions. Figure 3 shows an example of permission assignment.

While most information technology vendors have incorporated RBAC into their product line, its design and implementation needs to be tailored to a company's business model and security risk requirement. Accordingly, our objectives for this module are (1) to help learners understand the basic concepts of RBAC and (2) to provide them a detailed examination of the role definition and access constraints in the context of chemical process control.

**PEDAGOGICAL APPROACH**

The instructional design for the module is based on a pedagogical strategy known as *anchored instruction* [4]. This approach organizes the activities for the module into a set of phases “anchored” on a motivating challenge (Figure 4). The phases address various aspects of guiding a learner’s inquiry in solving the challenge.



FIGURE 4: CHALLENGE-BASED INQUIRY CYCLE

As shown in Figure 4, the particular inquiry cycle chosen for the module has six phases:

- **The Challenge:** introduces the challenge that is the focus for the remaining activities in the inquiry cycle;

- **Generate Ideas:** provides learners with an initial opportunity to reflect on the salient features of the challenge problem, including the identification of relevant current knowledge and “gaps” in their knowledge that will be subjects for new learning;
- **Multiple Perspectives:** helps learners refine their understanding of the challenge problem by providing resources that illuminate aspects of the problem from varied viewpoints;
- **Research and Revise:** supports inquiry by learners in solving the challenge by providing resources that address new learning;
- **Test Your Mettle:** supports reflection by learners on their mastery of concepts learned in the “Research and Revise” phase, motivating further inquiry or building confidence in the learner’s solution to the challenge;
- **Go Public:** allows a learner to declare their solution to the challenge and to reflect on what they have achieved during the learning experience.

In this cycle, two pairs of phases are strongly interrelated. “Generate Ideas” and “Multiple Perspectives” address *problem setting*; that is, they are used to recognize key features of the problem that inform the selection of solution strategy. “Research and Revise” and “Test Your Mettle” support inquiry and reflection, respectively. Anchored instruction emphasizes the availability of a multiplicity of resources for inquiry and the ability of the learner to direct their own use of these resources by reflecting on what they already know and additionally need to know. The “Research and Revise” phase provides the multiple learning resources and the “Test Your Mettle” phase provides opportunities for the learner to self-assess about the current state of their learning. These “active” features of anchored instruction focus on the development of learning (meta-cognitive) skills.

**ADAPTIVE LEARNING TECHNOLOGIES**

To design and implement the module, we employed learning technologies created by the NSF Engineering Research Center for Bioengineering Educational Technologies, called VANTH [5]. These technologies include a visual language-based

DEVELOPMENT PROCESS

authoring environment called CAPE—the Courseware Authoring and Packaging Environment [6]—and an adaptive online learning platform called eLMS—the experimental Learning Management System [7].

The CAPE authoring environment is used to design adaptive online learning experiences involving static, interactive, and dynamic content elements created with conventional web authoring tools and within CAPE itself. [8] The design representation employed by CAPE is a domain-specific visual language, where icons and connections represent concepts and relationships that can be organized hierarchically. CAPE can be used to incorporate adaptations into designs that alter the flow of materials, or the materials themselves, based on knowledge about a particular learner and his or her current situation in an activity. A key aspect of support provided by CAPE for the authoring task is the ability to represent and use *instructional design patterns*. These are abstract design representations that capture commonalities among collections (or families) of designs and design elements supporting their reusability. CAPE provides an integrated web-based repository for storing and sharing design patterns, as well as completed designs and content resources. The repository can be searched using metadata specifications, by taxonomy associations, or by element names used as keywords.

The eLMS learning platform is used to enact adaptive designs with learners. The heart of the platform is a model-based delivery engine that understands CAPE designs and applies the adaptations they define. Since some of these adaptations address the flow of materials, eLMS provides a toolbar-based navigation interface (Figure 5) that presents learners with options for proceeding through an online learning activity. This allows navigation to be separated from the learning materials themselves, thereby increasing the reusability of the materials. eLMS creates detailed records of the deliveries of online assignments, including all navigation decisions that a learner makes and the outcomes of all interactive elements of assignments. These *delivery records* support reflection by instructors and authors on how learners actually use the assignments.

The module developed in this pilot effort is based on a CAPE instructional design pattern for anchored instruction. (Figure 6) The pattern reflects the organization of the inquiry cycle into phases. It provides an adaptable navigation scheme for controlling how the learner can proceed through the cycle, including support for such details as the iteration between the “Research and Revise” and “Test Your Meddle” phases. The pattern also provides sample content that can be used to control the “look and feel” of the individual content elements of phases, including a graphical rendering of the cycle indicating the current phase (see Figure 5).

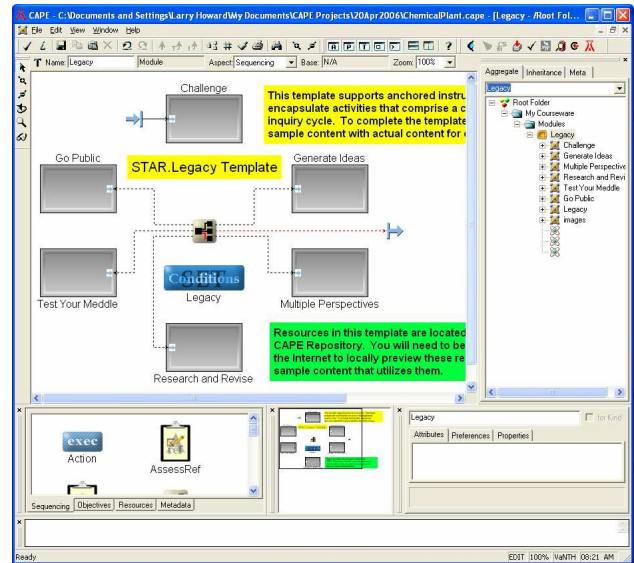


FIGURE 6: CAPE DESIGN PATTERN FOR ANCHORED INSTRUCTION

The availability of this design pattern, which can be instanced by a wizard component of CAPE, greatly simplifies the authoring task when creating modules that employ the anchored instruction pedagogical style. The effort in completing the pattern is primarily focused on creating the content elements that support each of the phases. The content examples provided by the pattern serve as guides. Each design element in the pattern that corresponds to a phase in the cycle provides annotations that explain the phase’s role. The example content is sensitive to this role. For example, the “Generate Ideas” phase is used to elicit the initial thoughts of the learner on the challenge problem, and so the example content utilizes an interaction design element in CAPE for querying information from the learner. (Figure 7)

The phases of the cycle requiring the most effort are the “Research and Revise” and “Test Your Meddle” phases, as these provide the primary instructional materials for the module. For “Research and Revise”, a graduate student prepared a tutorial resource on role-based access control and a page of selected resources available on the internet addressing aspects of RBAC. Value was added to these resources through their organization and by descriptions that help the learner understand the kinds of information each resource



FIGURE 5: COURSEWARE DELIVERY WITH ELMS

provides. For the “Test Your Meddle” phase, a set of interactive exercises addressing aspects of RBAC were also developed by the graduate student. These exercises can diagnose learner difficulties and provide the learner feedback on their performance on each exercise.

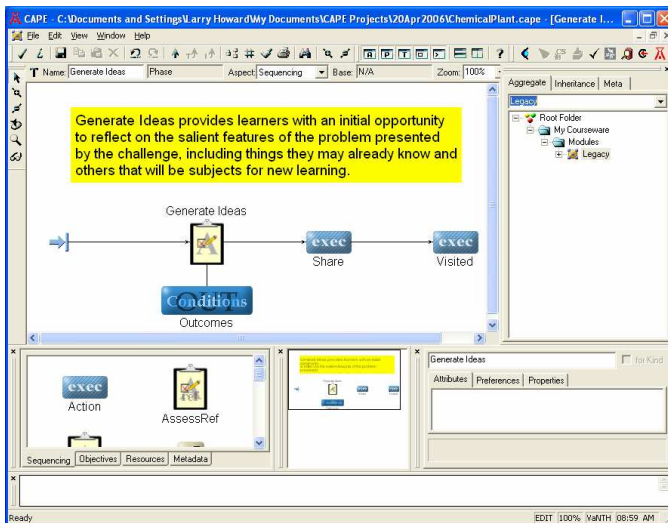


FIGURE 7: GENERATE IDEAS PHASE FROM THE DESIGN PATTERN

Other than the development of content resources for a module, the only remaining design decisions that need to be made concern supporting the learner’s progress through the phases of the cycle. The pattern provides a default set of decisions that support sequentially moving through the phases up to the “Test Your Meddle” phase, and then allowing the learner to revisit “Multiple Perspectives”, “Research and Revise” and “Test Your Meddle” in any order and as often as he or she wishes. At any time after initially visiting the “Test Your Meddle” phase, the learner can proceed to “Go Public” to declare their solution to the challenge. These sequencing choices can be easily altered by changing simple logical expressions that serve as preconditions for entering or revisiting a phase.

CAPE allows these sequencing controls to be dynamically altered as the module is being delivered to the learner. Further, particular learning or reflection resources can be emphasized or exclusively offered based on knowledge of the learner’s current situation. While we do not plan to initially employ these features in the module, we will be guided by learner feedback in defining appropriate future roles for them.

## DISCUSSION

We set out to design an online module to teach security concepts, based on role-based access control, to chemical engineering students in a capstone design course. Further, we were interested in the process of developing this module, and what it could tell us about the prospect of creating other such modules for dissemination as part of the education program of the TRUST STC. In this paper, we have been primarily concerned with these process aspects. The module is currently

being completed and will then go through several validation steps on its way to initial use by learners in the Fall semester of next year. Validation will include trial use by learners, and their feedback, elicited using surveys and observations from eLMS delivery records, will be used to fine-tune content and to refine the delivery strategy.

What we have learned from the design and implementation process is that, with scaffolding provided by the available learning technologies, there can be an effective division of labor between subject matter experts and graduate students. Subject matter expertise can be addressed as a collaboration between TRUST faculty and faculty from the targeted domain for the learning materials. With a pedagogical strategy such as anchored instruction, the primary roles for the subject matter experts are the selection of appropriate challenges and the identification of relevant concepts and skills from the security domain. Thereafter, graduate students, in consultation with faculty, can perform the tasks of selecting learning materials, creating interactive reflection activities, and completing to module design with these resources.

This approach offers a certain economy, but there are additional economies that TRUST can seek to leverage. For example, we anticipate cases in which the same security concepts, and learning materials that address them, will be relevant in multiple application domains. Adaptation features of CAPE, initially developed to support dynamic adaptation of content for individual learners, can also be used to adapt content to an application domain. Using these features, a single module could be built around a set of common resources, adapting their presentation and scaffolding for the targeted context. Alternatively, the common resources could be provided as reusable design elements and incorporated into domain-specific module designs with CAPE.

Another potential aspect of adaptability concerns adapting modules to the learning situation in which they will be used. This context is influenced by dependencies on the learner’s prior knowledge (and skills) in addressing a module’s learning objectives. CAPE can be used to express these dependencies, and its adaptation features can be used to offer different sets of learning resources in response to differing learning situations. These features could be used to support either “late design” or dynamic adaptation, depending on how prior knowledge varies among targeted learners.

Once adaptable learning modules have been created, there are issues of how to make them available and how to support adapting them to particular learning situations. The TRUST Academy Online (TAO) is a scaffolded dissemination portal that will provide access to the center’s educational materials. Interoperation with authoring environments like CAPE will allow educators to further adapt selected learning materials. However, the reuse of adaptable learning materials is even less well understood than the reuse of learning materials, *per se*. Additional pilot projects will be used to better understand how to structure the materials and adaptation processes to enable possible reuse by educators for multiple domains, for differing educational levels, or for varied learner populations.

**ACKNOWLEDGMENTS**

This work is supported in part by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422).

**REFERENCES**

- [1] "Guidance for Addressing Cybersecurity in the Chemical Sector," Version 2.1 Copyright 2004, 2005 Chemical Industry Data Exchange.
- [2] "Chemical Industry Seeks Cyber Security", Chemical Engineering Progress, August, 2002, p15.
- [3] Ferraiolo, D. and Kuhn, R. "Role-based access control". *15th NIST-NCSC National Computer Security Conference*, pages 554--563, Baltimore, MD, October 13-16 1992.
- [4] Bransford, J. et al. (1990) "Anchored instruction: Why we need it and how technology can help". In D. Nix & R. Sprio (Eds), *Cognition, education and multimedia*. Hillsdale, NJ: Erlbaum Associates.
- [5] Harris, T.R., Bransford, J.D. and Brophy, S.P. "Roles for Learning Sciences and Learning Technologies in Biomedical Engineering Education: A Review of Recent Advances". *Annual Review of Biomedical Engineering* 4: 29-48, 2002.
- [6] Howard, L. "CAPE: A Visual Language for Courseware Authoring". *Second Workshop on Domain-Specific Visual Languages*, Seattle, WA, November 4, 2002.
- [7] Howard, L. "Adaptive Learning Technologies for Biomedical Education". *IEEE Engineering in Medicine and Biology Magazine* 22: 58-65, 2003.
- [8] Howard L., Remenyi Z., and Pap G., "Adaptive Blended Learning Environments", International Conference on Engineering Education, July 23-28, 2006, San Juan Puerto Rico. (accepted)