

# A CASE STUDY OF CDIO IMPLEMENTATION IN THE COURSE OF HACKING EXPOSED AT DUY TAN UNIVERSITY

Nhan-Van Vo<sup>1</sup>, Duc-Man Nguyen<sup>2</sup>, Nhu-Hang Ha<sup>3\*</sup>

<sup>1</sup> International School, Duy Tan University, Vietnam, vonhanvan@dtu.edu.vn;

<sup>2</sup> International School, Duy Tan University, Vietnam, mannd@duytan.edu.vn;

<sup>3</sup> International School, Duy Tan University, Vietnam, hatnhuhang@dtu.edu.vn

## ABSTRACT

Integration of theoretical knowledge and practical skills in teaching and learning is usually one of the focuses in CDIO implementation. However, it is not always as smooth as it should be for some study subjects. Hacking exposed in Information Technology (IT) is one of such subjects: without the theoretical knowledge about computer networks, it is almost impossible to develop computer hacking skills while learning computer network theories or practices by-the-book only will not yield much benefit when the technology changes. This paper presents a real-world case study for successful learning of the course of Hacking Exposed at Duy Tan University by combining the teaching of an in-school project with the trying-out of at-work practices in attacking and defending computer networks. Specifically, the in-school project is closely structured around related network theories while the at-work practices to be learned at each stage of the project are openly discussed and tried out on various computer platforms and/or with any newly-introduced trick and tip. At-work practices can be learned both at school in computer labs or at companies in the industry which have ties with the university. In addition, CDIO guidelines and criteria for Standard No. 5 and 7 are utilized in the structure of this proposed approach. That way, as much as at-work practices may change in the everyday real world, the structures of the project do not have to change that much as long as related theories still hold their value. If it is no longer necessary to learn a certain theory, instructors may remove that theory and its related at-work practices all together. The validity of this case study is backed by observation the way instructor and students of Hacking exposed class. The results of this study are helpful in leveraging instructors' flexible handling of the course materials and in enabling students to master both hacking skills and knowledge in a shorter amount of time.

## KEYWORDS

CDIO Standard No. 5, 7, Hacking Exposed, practical skills development, project-driven approach

## INTRODUCTION

In recent years, industry began to find that graduating engineering students, while technically adept, lacked many skills and abilities required in real world engineering situations (Lynch, Seery, & Gordon, 2007). Traditional teaching methods often failed to achieve the goals set out by industry. The challenge from industry, and increasingly from government, still remains: to increase the quality of engineering education. It is widely acknowledged that universities must do a better job at preparing engineering students for this future through the reforming engineering education (McMasters, 2004). They seek to enhance the preparation of engineering students through the development of a systematic reform of engineering

education, based on adaptations of the Conceive - Design - Implement - Operate (CDIO) approach in teaching programs (Crawley et al., 2007).

CDIO is an innovative initiative, which offers an alternative educational framework for producing better-prepared and highly skilled engineers (Elamvazuthi et al., 2015). This method aims to provide students with an education that stresses engineering fundamentals based on the life cycle of a product (Lynch et al., 2007). The students learn to solve problems and complete projects following the stages: *Conceive, Design, Implement, and Operate*. CDIO promotes goal orientated, project based learning where the aims and desired learning outcomes are clearly stated prior to the students starting any project or before any instruction is given. It aspires to create challenging experiences in which students design, build and operate product systems.

This teaching method is an open architecture endeavor and is available to all engineering programs to adapt to their specific needs. But the use of CDIO in DUY TAN UNIVERSITY (DTU) is still at an initial stage and needs practical verification. This article illustrates the way to conduct the Hacking Exposed course by leveraging CDIO method for enhancing students' performance. Standard No. 5 and 7 are utilized in the structure of this proposed approach. The purpose of this study is twofold. First, it aims to investigate the different approaching ways of leveraging CDIO in stimulating learning outcome of Hacking Expose course. Second, this study intends to generalize the effective way to teach IT course by using CDIO. This provides a basis for DTU to promote CDIO, and could promote further research on the use of CDIO. Moreover, this study also provides insights to instructors on how to improve their students' performance. The remainder of the study is organized as follows: the following section review theoretical background for developing framework and propositions, the next section describes data collection and analysis, and the last sections presents the results and the implications for researchers and practitioners.

## THE CDIO APPROACH

CDIO is a teaching model developed from 2000, by four universities, including MIT (Berggren et al., 2003). At present, there are more than 90 well-known universities in the world actively promoting CDIO. It works as an education concept and methodological system to guide the reform of the engineering education training model. It combines conception, design, implementation and the entire operation process as the means for developing students' engineering ability. By using the product life cycle model students develop a better appreciation for engineering processes and in doing so also develop the skills listed above. Each stage helps develop different skills in the students required by engineers (Lynch et al., 2007).

- (1) *The Conceive* stage involves defining the needs and problems to be solved and technology required, considering the enterprise strategy and regulations.
- (2) *The Design* stage focuses on creating the design the plans, working drawing, and algorithms that describe what will be implemented in completing the project.
- (3) *The Implement* stage involves transforming the design into the product solution. This includes manufacturing, coding, testing and validating.
- (4) *The Operate* stage involves operating the implemented product to deliver the intended function, including maintaining, evolving and retiring the system.

The CDIO initiative has defined twelve standards that any program set up under the CDIO syllabus must meet in order to ensure the highest standard of education is maintained. However, in this study we focus on Standard 5 "Design - Build Experiences" and Standard 7

“Integrated Learning Experiences”. Because we want to illustrate the way in which instructors provide students with the skills of active learning, practice, problem-analysis and problem-solving, and focus on vocational skills training, professional ethics, and teamwork and communication.

### **Standard 5 — Design-Implement Experiences**

The term design-implement experience describes a range of engineering activities central to the process of developing new products and systems. Included are all of the activities described at the Design and Implement stages, plus appropriate aspects of conceptual design from the Conceive stage. Students develop product, process, and system building skills, as well as the ability to apply engineering science, in design-implement experiences integrated into the curriculum. Design-implement experiences are structured to promote early success in engineering practice. Iteration of design-implement experiences and increasing levels of design complexity reinforce students' understanding of the product, process, and system development process. They also provide a solid foundation upon which to build deeper conceptual understanding of disciplinary skills (Brodeur & Crawley, 2009).

### **Standard 7 — Integrated Learning Experiences**

Integrated learning experiences are pedagogical approaches that foster the learning of disciplinary knowledge simultaneously with personal and interpersonal skills, and product, process, and system building skills. They incorporate professional engineering issues in contexts where they coexist with disciplinary issues. Industrial partners, alumni, and other key stakeholders are often helpful in providing examples of such exercises. Furthermore, it is important that students recognize engineering faculty as role models of professional engineers, instructing them in disciplinary knowledge, personal and interpersonal skills, and product, process, and system building skills. With integrated learning experiences, faculty can be more effective in helping students apply disciplinary knowledge to engineering practice and better prepare them to meet the demands of the engineering profession (Brodeur & Crawley, 2009).

## **RESEARCH FRAMEWORK**

Traditionally engineering modules are taught through the combined use of lectures, tutorials and practical sessions. This structure has many advantages as it provides the students with a cyclical approach to learning (Lynch et al., 2007). This structure can often fail to fully develop the vital problem-solving and project-based skills required in real world engineering projects. However based on Standard 5 and Standard 7 of CDIO approach can easily be integrated into any engineering program. The teachers should create a course plan and good teaching environment. They also make use of the practical training capabilities of applied undergraduate colleges. The practical projects are introduced into the course teaching. Students should master project development and management through the situational teaching model. This will improve students' problem-solving and team co-ordination abilities. The project task is carefully designed with respect to:

- (1) **C** (Conceive): The project deliverable is unconventional in the sense that students have limited prior experience with similar products. A pioneering situation enhances the conceiving phase and encourages students to engage deeply in the main technical challenges and approaches.
- (2) **D** (Design): The task is difficult enough to be a true challenge to students, yet possible to solve if the work is organized and carried out well. One of the main objectives of the course is to encourage students in applying theory, analysis tools,

and methodologies learned in other courses, thereby solidifying their knowledge and gaining confidence in their role as engineers.

- (3) **I** (Implement): The size and complexity of the product will entail teamwork and coordination, and provide opportunities to obtain practical experience from real manufacturing on a prototype level.
- (4) **O** (Operate): The task is formulated in such a way that the assessment of the results involves operation of the product and evaluation of its performance with respect to technical specifications.

In groups, and driven by the project design, under the guidance of teachers students continuously discover and raise questions related to the project, which strengthens their learning. They develop designs, carry out practical tests, identify defects and summarise their design experience to further deepen their knowledge and practical application ability. On the journey to the final project, their skills have been updated and their performance is improved. Based on the above discussion we propose the research framework as follow (Figure 1):

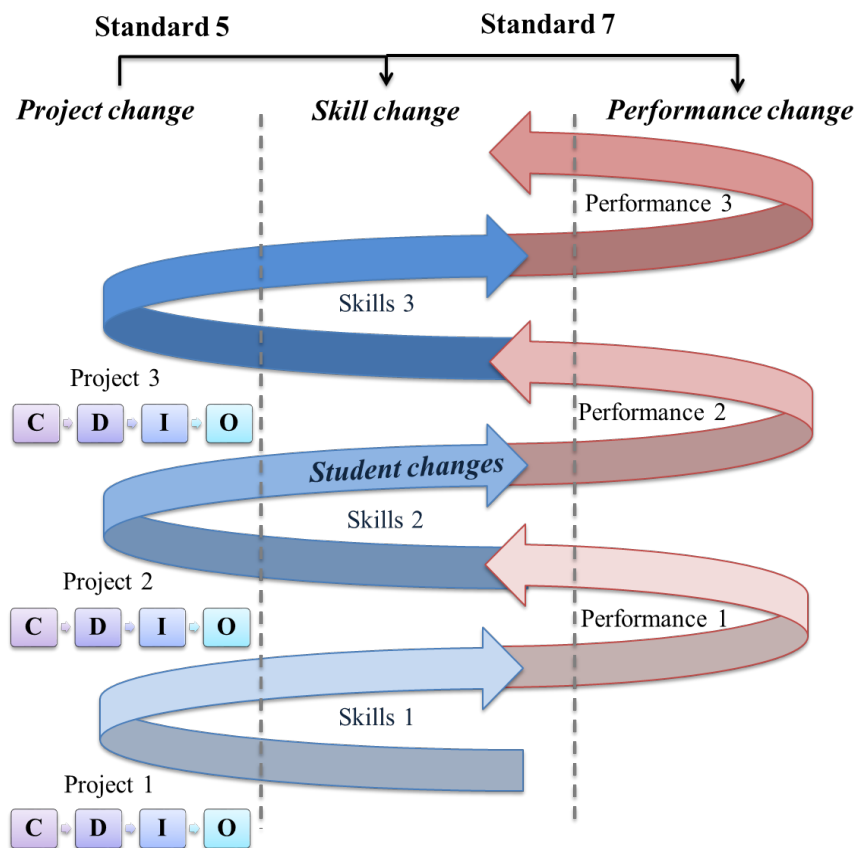


Figure 1. Proposed research framework

## HACKING EXPOSED COURSE AT DUY TAN UNIVERSITY

Located in Danang, Duy Tan University (DTU) is the biggest private university in the Central of Vietnam. A majority of the students are from the local province and 80% of those choose a workplace in cities in Central provinces. By leverage CDIO method DTU can provide students with specialized knowledge to meet the needs of economic and social development. Most of courses in DTU have been conducted in the collaborative way to enhance the

interaction between teacher and students as well as students and students. The Hacking Exposed (HE) course is a mandatory subject for all final-year undergraduate students enrolling in the Network Security of CMU Program in International School at DTU. The purpose of HE course is not to teach students how to be a hacker, but rather to teach students the approaches used by hackers so students can better defend against them. All students have no experience in this field. However, before finishing this course, they are required to submit 3 projects related to *Penetration test (SQL injection)*. SQL Injection can provide an attacker with unauthorized access to sensitive data including, customer data, personally identifiable information, trade secrets, intellectual property and other sensitive information. SQL Injection can be used in a range of ways to cause serious problems. It is necessary that students pursue for the course by solving engineering problems.

Students need to work hard to find the way to fulfil the requirements. The teacher requires groups to have between 4 to 6 members. Students first had to come up with or *Conceive* ideas and solutions to the problem. They then proceeded to *Design* how to apply theory, analysis tools, and methodologies learned in course to solve problem. At this stage a procedure is produced to assess the success of their design. Once a satisfactory design has been produced, the students then begin to make the execution (*Implement*), using their combined skills and the strengths. On completing the project the students will proceed to *Operate* and test their work. This follows the life cycle of any product and provides the students with clearly distinct stages to follow, developing necessary skills along the way.

By leveraging SQL Injection, an attacker could bypass authentication, access, modify and delete data within a database. In some cases, SQL Injection can even be used to execute commands on the operating system, potentially allowing an attacker to escalate to more damaging attacks inside of a network that sits behind a firewall. In this study we focus on three main ways which an attacker can hack a website, the detailed information of each case is given below (Table 1).

Table 1. Case description

Category		Case 1	Case 2	Case 3
Topic		Use command line to hack a website	Use Havij SQL Injection Tool to hack a website	use SQL MAP to hack a website
Project time		7 days	3 days	10 days
Purpose of case project		Require students understand SQL injection and simple command prompt to hack a website	Require students have ability to leverage existing tool to hack a website	Require students understand more complex command to hack a website and learn a new language (Python)
Operating system		Window	Window	Linux
Process to conduct case project	1. Lecturing	Instructor provides vulnerability of SQL and the way to explore SQL injection	Instructor provides more knowledge of Havij SQL Injection Tool	Instructor provides more knowledge of SQL MAP and Python language
	2. Classroom discussion	Students discuss to explore vulnerability of SQL concepts and to	Students discuss the way to install Havij SQL	Students discuss command lines of Python language

		find tool to figure out SQL injection	Injection Tool	
	3. <i>Out-of-class research, analysis (Conceive, Design)</i>	Students study command prompt to hack and figure out the procedure to hack a website	Students study how to use Havij and figure out the procedure to hack a website	Students study command prompt of Python language to hack in SQL MAP and figure out the procedure to hack a website
	4. <i>Case practice (Implement, Operate)</i>	Students find websites and start to hack		
	5. <i>Submit results</i>	Students submit hacked website with user and password (1 website)	Students submit hacked website with user and password (4 website)	Students submit hacked website with user and password (Cannot hack)
	6. <i>Presentation - discussion</i>	Students present how to do		
	7. <i>Evaluating</i>	Instructor give comments and evaluate performance		
<b>Linking with industry</b>	Students come up with a report and send to companies which have websites were hacked. In case, the company want to fix problem they can contact with them and make sign a real project.			

In case 1, the topic is assigned is “Using command prompt to hack a website”. Students need to understand and follow the following steps to finish their project:

- *Step 1 - Finding Vulnerable Website:* Students find the vulnerable websites by using Google Dork list. The use “inurl:” command for finding the vulnerable websites.
- *Step 2 - Checking the Vulnerability:* Students should check the vulnerability of websites. by adding the single quotes (') at the end of the url and hit enter.
- *Step 3 - Finding Number of columns:* After finding the vulnerable websites, they need to find the number of columns in the table by replacing the single quotes (') with “order by n” statement.
- *Step 4 - Displaying the Vulnerable columns:* Using “union select columns sequence” Students find the vulnerable part of the table. Replace the “order by n” with this statement and change the ID value to negative
- *Step 5 - Finding the Table Name:* Now they have to find the table name of the database. Replace the n with “group\_concat (table\_name) and add the “from information\_schema.tables where table\_schema=database ()”
- *Step 6 - Finding the Column Name:* Then students replace the “group\_concat (table\_name) with the “group\_concat(column\_name)”
- *Step 7 - Finding the Account:* Finally, they get the result – a website with user name and password



Figure 2. Result of Case 1

In case 2, the assigned topic is “Using Havij SQL Injection Tool to hack a website”. Students need to follow the below steps:

- *Step 1 – Run Havij.exe*
- *Step 2 – Find Database name:* Havij will start SQL injection to the target provided URL. It perform queries to analyze IP, web server, PHP version, Database MySQL version. Then, using Insertion type (') string, it proceeds to find column count, column string, finally Database name. After it finds out Database name, Status becomes Idle saying “I’m IDLE”.
- *Step 3 – Find Tables:* Havij Pro will fetch all the tables for the selected Database.
- *Step 4 – Get columns:* Tick the table which you finds important regarding your aim and click Get Columns button. This step reveals all the columns in selected table.
- *Step 5 – Finally, select important columns of a table (for ex., admin) and click “Get Data” button.* The result that name, email, password, user ID everything is revealed.

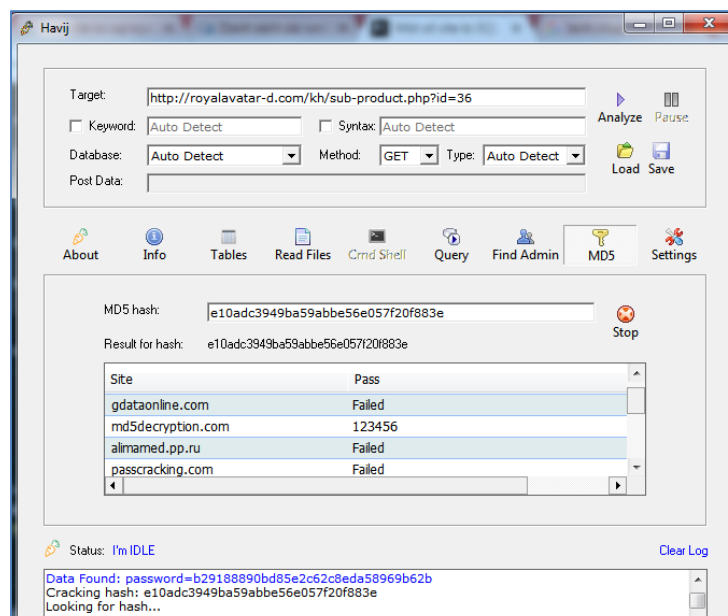
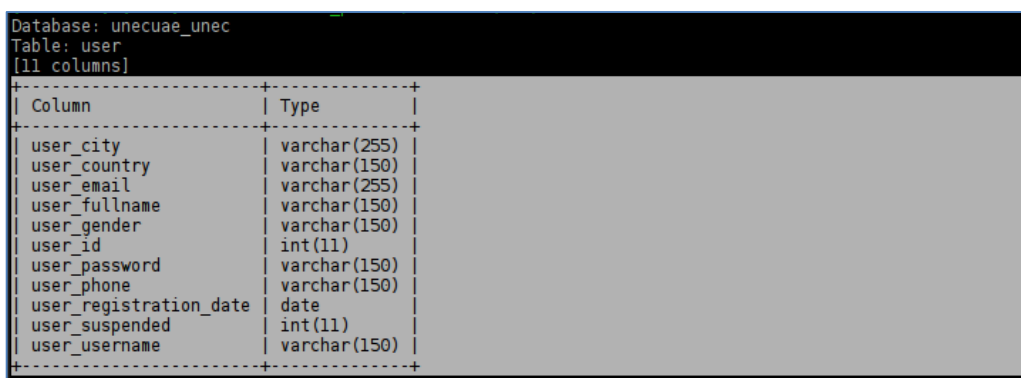


Figure 3. Result of Case 2

In case 3, the assigned topic is “Using SQL map to attack a website”. Students need to follow the below steps:

- *Step 1 - Find a Vulnerable Website:* This is usually the toughest bit and takes longer than any other steps.
- *Step 2 - List DBMS databases using SQLMAP SQL Injection:* Students find SQL Injection vulnerable website and need to list all the databases with vulnerable database.
- *Step 3 - List tables of target database using SQLMAP SQL Injection:* Now they need to know how many tables this SQL dummy website database got and what are their names.
- *Step 4 - List columns on target table of selected database using SQLMAP SQL Injection*
- *Step 5 - List usernames from target columns of target table of selected database using SQLMAP SQL Injection.* However, in this case students cannot find any user or password, since the limited time and experience.



```
Database: unecucae_unec
Table: user
[11 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user_city | varchar(255) |
| user_country | varchar(150) |
| user_email | varchar(255) |
| user_fullname | varchar(150) |
| user_gender | varchar(150) |
| user_id | int(11) |
| user_password | varchar(150) |
| user_phone | varchar(150) |
| user_registration_date | date |
| user_suspended | int(11) |
| user_username | varchar(150) |
+-----+-----+
```

Figure 4. Result of Case 3

Based on the case study, we found that CDIO-based pedagogy is penetrated into the whole teaching process. Lecture is conducted before executing the classroom discussion, out-of-class research and analysis, case practice, etc. Classroom discussion emphasizes on the inspiration of professional knowledge, its content is characterized by the concept of SQL injection. Teachers are offered a leading role in the class process. Students are required to answer many questions on the concept of SQL injection and its specific details, e.g., why SQL injection should be studied? Which method should be used for hacking a website? How about its specific requirement? How to analyze the application of SQL injection and how about the practical process? What principles should be followed? All these questions facilitate teacher’s seeking for the practical situation of student’s knowledge- understanding, and they also prompt student’s thinking in class and prepare for following case discussion.

After the instruction of basic concepts is completed, students are separated into several studying groups; several case questions of teacher and predetermined tasks are discussed and conceived in each group respectively. Students of each group should reach their own consensus and the discussion conclusions are recorded in detail and submitted after the class is finished. Furthermore, a student representative from each study group is requested for stating the basic viewpoints of his group, and debating can take place when other groups have their respective viewpoints. During this process it is teacher’s responsibility that the discussion should be guided correctly and student’s initiative should be fully promoted. This task will be more detailed and complex than the traditional classroom discussion. The analysis of a practical case is a new teaching step and pedagogy method by which the



grouped students select an appropriate example for studying and practicing by themselves. With the accumulated knowledge obtained by different projects, the capability of independent analysis is established in students, and through the group discussion and classroom debate the preliminary conception and design of the whole knowledge system of SQL injection are obtained.

## REFLECTIONS AND DISCUSSION

Through practical operation students can learn basic concepts of SQL injection. The practice process will lead students to understand different methods to attack a website and preventing solutions. The whole process is characterized by case evaluation and student's participation, teacher is only regarded as an academic advisor, and he gives a necessary advice only when practical difficulties exist. On the other hand, teacher can also put forward some technical requirements during the building attacking procedure and solution, which makes the projects developed, be more practical and feasible. Different case, teachers figure disadvantages and advantages to help students get un-depth understanding (Table 2).

Table 2. Case study comparison

	<b>Advantages</b>	<b>Disadvantages</b>
<b>Case 1</b>	Students understand the rules of SQL injection and procedure of hacking a website by using command prompt (step by step)	It takes time to understand technical problems.
<b>Case 2</b>	It is easy for students to execute this method by using GUI. Student learns a new and efficient technique "Bypass" in SQL". With diversified hacking methods, students can attack more website	It not Student no need to understand SQL injection well, just use available tool
<b>Case 3</b>	Students understand the way to use open source, and study new language - Python	It takes time to understand new language

By leverage the concept of Standard 5 and 7, we found that CDIO-based method serve as vehicles for developing students' engineering skills while at the same time deepening their understanding of technical knowledge. It is obvious that relevant skills such as Self-learning ability, Problem-solving, Communication, Teamwork, Knowledge acquisition are improved during implementation case project. Although, CDIO method provides effective and motivating design-implement experiences for students, it also makes instructors face some challenges:

- Learning outcomes for design-implement experiences need to distinguish between product performance and learning performance.
- The task of the design-implement experience must be sufficiently complex, yet limited in scope, to ensure successful outcomes for students. Instructors and students sometimes see the achievement of a good technical solution as the real learning outcome. Failure in the task can be perceived as failure in learning.
- Design-implement experiences require teaching and assessment practices that are different from traditional instruction.
- Few instructors are prepared to assume responsibility for technically challenging projects. In a typical engineering department, only a few faculty and staff have personal, practical experience of developing complex systems.

## CONCLUSION

Implementing the CDIO model of practical teaching is not complicated, and is an innovative model for engineering and science education within universities. Specifically, it was used to establish a reasonable and complete teaching system in computer major. The basic principles of CDIO are fairly simple, with wide application, and can be adopted for the teaching of most courses. We found that the overall quality of students had been improved significantly and the employment situation was getting better. In the teaching practice, the pedagogy method and learning organization are improved and optimized continuously through extensive assessing and scientific evaluating; finally the goal of fully mobilizing student's learning initiative and developing his practical ability by CDIO-based teaching theory can be reached.

## REFERENCES

- Berggren, K. F., Brodeur, D., Crawley, E. F., Ingemarsson, I., Litant, W. T., Malmqvist, J., & Östlund, S. (2003). CDIO: An international initiative for reforming engineering education. *World Transactions on Engineering and Technology Education*, 2(1), 49-52.
- Brodeur, D. R., & Crawley, E. F. (2009). Cdio and quality assurance: Using the standards for continuous program improvement *Engineering Education Quality Assurance* (pp. 211-222): Springer.
- Crawley, E., Malmqvist, J., Ostlund, S., & Brodeur, D. (2007). Rethinking engineering education. *The CDIO Approach*, 302, 60-62.
- Dillon, J. (2008). A review of the research on practical work in school science. *King's College, London*, 1-9.
- Elamvazuthi, I., Lee, H., Ng, J., Song, H., Tiong, Y., Parimi, A., & Swain, A. (2015). Implementation of a New Engineering Approach for Undergraduate Control System Curriculum using a Robotic System. *Procedia Computer Science*, 76, 34-39.
- Lynch, R., Seery, N., & Gordon, S. (2007). *An evaluation of CDIO approach to engineering education*. Paper presented at the International Symposium for Engineering Education, ISEE-07, Dublin, Ireland.
- McMasters, J. H. (2004). Influencing Engineering Education: One (Acrospace) Industry Perspective. *International Journal of Engineering Education*, 20(3), 353-371.

## BIOGRAPHICAL INFORMATION

**Nhan-Van Vo** has been taught and researched at Duy Tan University. His research interests include information security, physical layer secrecy, RF-EH and other advanced communication systems security. He is member of Cisco System, Juniper System, ComPTIA System.

**Duc-Man Nguyen** is the Acting Dean of the International School - Duy Tan University. His majors are in Software Engineering and Information Systems Management. He has more than 12 years of experience in software development and mentoring for Capstone projects. His interests are in software testing, mobile application testing, and large-scale data processing.

**Nhu-Hang Ha** is working in International School, Duy Tan University as researcher. She received Ph.D. in Information Management from Yuan Ze University in Taiwan. Her research interests involve: Knowledge Management, Project Management, Collaboration, and IT application.

### Corresponding author

Dr. Nhu-Hang Ha  
International School - Duy Tan University  
254 Nguyen Van Linh Str., Thanh Khe  
Danang, Vietnam



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

+841207121301  
[hatnhuhang@dtu.edu.vn](mailto:hatnhuhang@dtu.edu.vn)

[Commons Attribution-NonCommercial-  
NoDerivs 3.0 Unported License.](#)