NUCLEAR CYBERSECURITY EDUCATION: A COLLABORATIVE, MULTI-FORMAT APPROACH USING THE ASHERAH NUCLEAR POWER PLANT SIMULATOR 2.0

P. SMITH
Lancaster University
paul.smith@lancaster.ac.uk

M. ZERPHY
The Pennsylvania State University
mxz206@psu.edu

G. BERMAN
Instituto Balseiro / Comisión Nacional de Energía Atómica

M. BRADBURY
Lancaster University

R. BUSQUIM E SILVA
IAEA

K. EL-KHATIB
Ontario Tech University

R. MARQUES
University of São Paulo

G. MEYERS
The Pennsylvania State University

H. NOLAN
Ontario Tech University

Abstract

The expansion of digital systems in nuclear facilities has created a growing need for professionals with expertise in operational technology (OT) cybersecurity. To address this demand, multiple universities are partnering with the International Atomic Energy Agency (IAEA) to develop and deliver nuclear cybersecurity education using the Asherah Nuclear Power Plant Simulator (ANS). The latest version, ANS 2.0, is a modular, containerized environment that integrates information technology (IT) and OT systems in a representative nuclear facility context, including digital instrumentation and control (I&C), human-machine interfaces (HMI), and Security Information and Event Management (SIEM). It enables learners to explore cyberattack scenarios, analyze network traffic, and practice incident response in a secure, hands-on setting. ANS 2.0 has been incorporated into semester-long graduate and undergraduate courses, micro-credential programs, and short workshops, serving students from nuclear engineering, computer science, information sciences, cybersecurity, and international affairs in both resident and online settings. Instructional content spans from policy and regulatory analysis to technical aspects such as attack scripting, protocol evaluation, and controller resilience design. Pre- and post-course assessments and surveys track learning outcomes and guide improvements. The paper presents an overview of ANS 2.0 and summarizes the wide range of educational initiatives it supports. Lessons learned are discussed, including findings from surveying engaged learners. The aim is to share experiences so that educational institutions in Member States can engage through the IAEA International Nuclear Security Education Network (INSEN) to develop similar programs and expand nuclear cybersecurity workforce capacity.

1. INTRODUCTION

Digital modernization of nuclear facilities—including advanced reactors, digital instrumentation and control (I&C), remote monitoring, and expanded networking—continues to increase the cyber-physical attack

surface of nuclear facility systems. As a result, the nuclear workforce has an increasing demand for competencies that span traditional nuclear engineering, cybersecurity, and operational technology (OT). Hands-on simulation environments complement lecture instruction to convey the tightly coupled interactions between cyber actions and physical impacts for nuclear facility operations by enabling learners to observe how cyber activities affect plant operations, demonstrate defence-in-depth concepts, and understand the consequences of design and operational decisions [1]. The latest version of the Asherah Nuclear Power Plant Simulator (ANS) developed by the IAEA, ANS 2.0, provides this capability with representative nuclear facility behaviour coupled to OT system simulations. ANS was developed to support cybersecurity training and assessment for Member States; ANS 2.0 expands this capability through modular deployment, integration of information technology (IT) and OT systems, and flexibility for both education and research.

This paper presents early experiences from a multi-institution pilot deploying ANS 2.0 in university-level education. Five institutions, representing diverse geographic regions, academic disciplines, and instructional formats are engaged in piloting the use of ANS 2.0 in curricula. Two institutions, Lancaster University and The Pennsylvania State University (Penn State), completed full-semester courses during the 2025 academic year, Ontario Tech University delivered a condensed, event-based introduction to nuclear cybersecurity and plans to deliver a weeklong course, while two others are currently delivering and preparing future offerings. Each institution has developed course designs to fit within their programs; this paper provides comparative insights gained from these varied implementations using ANS 2.0 to provide insights to assist with adoption at other institutions interested in similar course offerings. Details are provided on the courses offered by Lancaster and Penn State, including: academic context and learner population; instructional format and duration; ANS 2.0 usage and learning objectives; assessment and feedback; and lessons learned and next steps. Summaries of ongoing efforts and plans of the other three institutions piloting ANS 2.0 are also provided.

2. ANS 2.0 AS AN EDUCATIONAL PLATFORM

ANS 2.0 is a containerized simulation environment representing a pressurized water reactor (PWR) nuclear power plant (NPP) with integrated digital I&C, OT networks, and supporting IT services. The platform uses standard OT protocols (e.g., OPC UA and Modbus) with programmable logic controllers along with human–machine interface (HMI) and Security Information and Event Management (SIEM) views [2]. These components are arranged to reflect common nuclear facility architectures and operations while remaining safe for educational experimentation. From an instructional perspective, ANS 2.0 offers several features particularly relevant to higher education. First, it enables students to observe both operator-facing views and ground-truth process behaviour, illustrating how cyber compromise can distort situational awareness. Second, the platform supports instructor-initiated and scripted attack scenarios, allowing exercises to be aligned with learning objectives rather than technical novelty alone. Third, its modular design permits selective exposure to complexity, enabling use with students who lack prior nuclear engineering, OT, or cybersecurity backgrounds. ANS 2.0 has been used to support a wide range of learning activities, including OT network familiarization, attack implementation, detection and monitoring exercises, and discussions of regulatory and policy implications. Importantly, the platform supports interdisciplinary instruction by enabling students from engineering, computer science, cybersecurity, and policy programs to engage with the same environment while focusing on different analytical perspectives. These characteristics make ANS 2.0 well-suited for IAEA International Nuclear Security Education Network (INSEN) institutions seeking to develop or expand nuclear cybersecurity curricula.

3. INSTITUTIONAL IMPLEMENTATIONS

3.1. Lancaster University

Lancaster University deployed ANS 2.0 within a 10-week undergraduate course on *Secure Cyber Physical Systems*, enrolling 122 students in the final or penultimate year of computer science, software engineering, or cybersecurity degree programs. No participants had a prior background in nuclear systems, making ANS 2.0 the primary mechanism for introducing NPP concepts and cyber-physical system behaviour. Over the 10-week period, students completed a sequence of laboratory exercises designed to prepare them for a comprehensive final assessment. Initial activities focused on familiarization with nuclear power plant operation and identifying

baseline behaviour of the Asherah NPP simulator. While students were not expected to develop nuclear engineering expertise, they were required to build the capability to interact with and analyse complex cyber-physical systems. To support this, students observed plant process variables and normal operational network traffic to understand expected system behaviour.

Building on prior coursework in penetration testing, students applied reconnaissance techniques using tools such as Nmap to identify hosts and services within the ANS 2.0 environment. This activity highlighted important differences between traditional IT and OT environments; in particular, students observed that default reconnaissance tool configurations were ineffective for identifying industrial services, as typical scans failed to detect Modbus and OPC UA servers. This reinforced the need for domain-specific approaches when working in OT contexts. Lancaster hosted Asherah within a virtual machine (VM) which was runnable by students in two ways, either locally on lab machines or via a nested virtual machine hosted in Lancaster's local cloud. Hosting directly on lab machines was more performant, but access via the local cloud allows students to interact with Asherah when off campus. Due to the use of penetration testing tools, the Asherah VM was isolated from the campus network and internet to prevent accidental misuse of these tools while learning.

To develop foundational interaction skills, students wrote simple Python scripts to communicate with OPC UA and Modbus servers. Python was selected to allow students to focus on algorithmic understanding rather than language complexity. Using these scripts, students implemented attacks available within the ANS 2.0 environment, typically by writing applications that repeatedly overwrote OPC UA variables at high rates. Example attacks included manipulating reactor setpoints to values lower than those selected by the operator. Students were required to observe and evaluate the resulting plant behaviour and determine whether observed outcomes aligned with expectations; example outputs for student comparison of normal and attack conditions are shown in Fig 1.

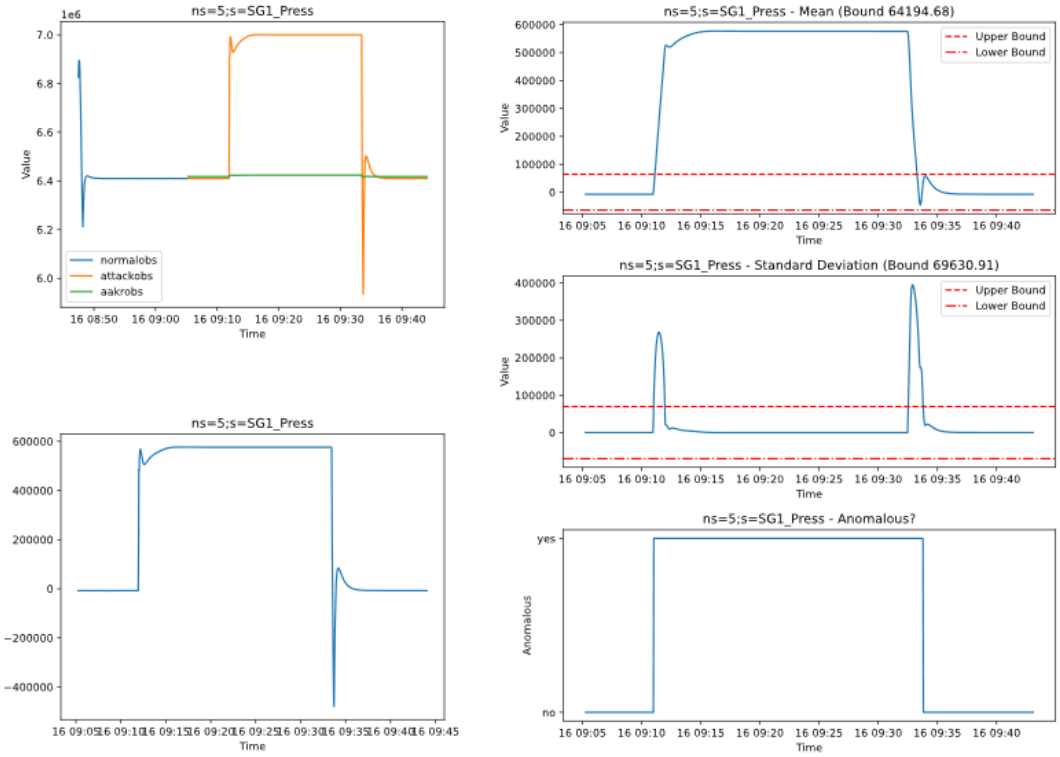

FIG. 1. Sample graphs showing the data gathered when ANS behavior is normal (normalobs) and when ANS is under attack (attackobs). A sliding window of mean and standard deviation is computed over the residual between the expected observations (aakrobs) and actual observations to build a binary classifier.

The final phase of the laboratory sequence focused on attack detection. Students implemented their own data historians by periodically polling OPC UA servers and storing values for all available variables in a database. These datasets were then used to implement and evaluate offline anomaly detection algorithms, including Auto Associative Kernel Regression (AAKR) [3]. Additional detection techniques, such as CUSUM (Cumulative Sum) and Kalman filters, were also introduced and explored by students.

The culminating assessment placed students in a fictional regulatory scenario involving the Republic of Anshar, where the Asherah design was under consideration for export to Great British Energy – Nuclear. Within

this scenario, the United Kingdom's Office for Nuclear Regulation (ONR) raised concerns under Section 3.7.3 (SyDP 7.3) of the Secure Assessment Principles regarding the system's ability to detect stealthy cyber threats. Reflecting the outcomes-focused regulatory regime used by the ONR, students were tasked with developing and presenting claims, arguments, and evidence demonstrating that a self-defined stealthy cyberattack could be detected by their implemented algorithms. Students were required to implement both the attack and the detection mechanism using Python, gather supporting evidence from their historian, and evaluate detection performance.

Feedback from the course indicated that students developed a strong appreciation for the limitations of traditional IT-centric security approaches when applied to OT systems and the importance of understanding cyber-physical interactions. Lancaster identified the need for explicit instructional scaffolding early in the course to support students unfamiliar with nuclear systems and industrial protocols. Future iterations of the course will refine this early support and explore the use of ANS 2.0 in postgraduate research and advanced cyber-physical security applications.

3.1. Penn State

Penn State incorporated ANS 2.0 into a full-semester course on *Cybersecurity for Nuclear Facilities*, offered to undergraduate and graduate students across multiple colleges. The course enrolled students from nuclear engineering, computer science and engineering, information sciences and technology (cybersecurity), and international affairs, reflecting the diverse technical, operational, and policy communities involved in nuclear cybersecurity. Instruction was delivered in a hybrid format, with resident students at University Park and online participation through Penn State World Campus. ANS 2.0 was integrated throughout a 15-week semester, with simulation activities introduced early and revisited repeatedly to reinforce foundational concepts while supporting progressively more complex assignments. Rather than reserving the simulator for isolated laboratory exercises, ANS 2.0 was used throughout the course to connect lectures, readings, and applied activities [4]. This approach enabled students with varied backgrounds to build a shared understanding of nuclear facility systems, digital instrumentation and control (I&C), and operational technology (OT) networks before examining cybersecurity threats and defences. ANS 2.0 was made available to students on non-persistent VMs via the Penn State College of Engineering VDI platform, which enabled on-demand global access, essential for Penn State World Campus students. Resident students could access the VM via their personal computing devices or in the classroom, a computer lab outfitted with zero-client workstations with direct access to the course VM.

Instruction emphasized scenario-based operational analysis, with students using ANS 2.0 to observe how representative cyberattacks against OT systems could cause physical system responses. Exercises were designed to highlight the distinction between operator-facing views and underlying ground-truth process behaviour, illustrating how cyber compromise can distort situational awareness and decision-making in nuclear facility operations. Particular attention was given to understanding why physical responses occurred following cyber actions, rather than focusing solely on the mechanics of individual exploits. ANS 2.0 activities were complemented by a visit to the Penn State Breazeale Reactor (PSBR) and Radiation Science and Engineering Center (RSEC), allowing students to compare simulated architectures with real-world IT and OT implementations at an operating research reactor facility. These experiences reinforced connections between abstract cybersecurity concepts, regulatory requirements, and practical system design and operation. IAEA Nuclear Security Series guidance and the U.S. domestic regulatory framework were integrated into course discussions to provide context for cybersecurity obligations and defence-in-depth expectations for nuclear facilities.

A team-based instructional approach was used to leverage the interdisciplinary composition of the class. Students with nuclear engineering backgrounds contributed insight into reactor physics and thermal-hydraulic behaviour, while those from cybersecurity and information sciences provided classmates with insights on network architectures and attack details; and those from international affairs examined guidance and regulatory implications. ANS 2.0 served as a common environment for these perspectives to converge around shared scenarios and observations. Assessment methods included pre- and post-course surveys to evaluate changes in student confidence and understanding of nuclear cybersecurity topics, along with project-based assignments that required reflection on ANS 2.0 scenarios and the observed cyber-physical impacts. Students indicated limited experience with OT or I&C and a high desire to learn about cybersecurity for these systems. Student feedback consistently highlighted the value of being able to observe consequences of cyber actions within a nuclear-specific context, particularly for those without prior nuclear experience. The immersive and hands-on nature of ANS 2.0

was cited as critical to connecting cybersecurity concepts with real operational considerations, contributing to an increase in OT and I&C understanding. Key lessons from the Penn State implementation included the importance of introducing the simulator early in the semester, the value of sustained engagement with a single shared environment, and the effectiveness of interdisciplinary discussion enabled by scenario-based use of ANS 2.0. The course will be formally adopted and listed as an elective for both the Nuclear Engineering and Cybersecurity programs at Penn State, and course content is being developed to offer stackable micro-credentials. The curriculum for future offerings will expand the use of ANS 2.0 within the course and further align instructional content with IAEA guidance to support broader adoption across INSEN institutions.

3.2. Ontario Tech University

Ontario Tech University used ANS 2.0 to deliver a condensed, event-based introduction to nuclear cybersecurity for students in the Networking and IT Security program. The half-day format targeted students with no prior exposure to nuclear security, OT, or I&C. Pre-event survey data confirmed that participants were overwhelmingly IT-focused (96%) and largely unfamiliar with OT and ICS environments, with only 3.9% reporting prior experience. While students demonstrated conceptual awareness of IT vs. OT distinctions, they lacked familiarity with industrial protocols, industrial network traffic analysis, I&C systems, and nuclear-specific cybersecurity challenges; thus, there was a high interest in learning about nuclear cybersecurity.

The instructional design combined expert-led educational sessions—delivered by professionals from the Canadian Nuclear Safety Commission (CNSC), Ontario Power Generation (OPG), and Bruce Power—with hands-on simulation activities. This approach provided necessary domain context before transitioning students into applied learning. ANS 2.0 functioned as the primary experiential learning platform, offering students hands-on exposure to a simulated nuclear OT environment. Students began with open-ended exploration to understand baseline system behaviour prior to adversarial activity. Facilitators then launched live attack simulations at undisclosed intervals, generating alerts in an integrated SIEM. Students were tasked with detecting, investigating, and reporting malicious activity, after which facilitators explained the attack mechanics and investigation methodology before resetting the environment. Learning objectives emphasized understanding how attacks manifest in OT systems, familiarity with OT monitoring technologies, and the real-time decision-making demands of OT cybersecurity roles.

Effectiveness was evaluated using pre- and post-event surveys. Pre-event results confirmed substantial OT-specific knowledge gaps alongside strong baseline interest. Post-event responses demonstrated measurable gains across all assessed areas, including IT-OT understanding, nuclear-specific cybersecurity awareness, industrial network traffic analysis, I&C systems, and OT incident response. Feedback indicated high engagement and perceived instructional value. The majority of participants agreed that the hands-on simulations using ANS 2.0 effectively demonstrated nuclear cybersecurity concepts, and qualitative responses highlighted the value of practical attack investigation, realism, and in-person engagement. Suggested improvements focused on additional scaffolding and guided debriefs, reinforcing the overall pedagogical approach rather than challenging its design.

Ontario Tech University is planning to use ANS 2.0 in a condensed, one-week course consisting of full-day instructional sessions for undergraduate students in the Networking and IT Security program and graduate professional students in the Master of Information Technology Security program, expanding use and integration for regular course offerings.

3.3. Instituto Balseiro / Comisión Nacional de Energía Atómica

At Instituto Balseiro, in collaboration with Argentina's Comisión Nacional de Energía Atómica, ANS 2.0 was integrated into resident instruction for undergraduates studying Telecommunication Engineering and used to emphasize foundational exposure to OT networks, industrial protocols, and nuclear facility cybersecurity concepts for students with general engineering backgrounds. Coming into the course with some knowledge of computer networks (mainly Ethernet), frame switching concepts, and TCP/IP layer 2 protocols (VLAN 802.1q, STP, LACP, and LLDP), and basic knowledge of IP address and address resolution protocol (ARP), students first explored layer 3 protocols, routing protocols, and common IT upper-layer protocols. ANS 2.0 was then used to introduce OT network topology and protocols. ANS 2.0 implementation leveraged predefined scenarios with attacks and guided exercises to introduce cyber-physical interactions in nuclear systems. This approach helped build on early capacity and support future expansion into more advanced coursework and professional training.

3.4. University of São Paulo

The University of São Paulo (USP) is planning a computer security short activity, tailored to undergraduate students in Nuclear Engineering as part of a course on safety and security of nuclear facilities. The activity is structured in three half-day sessions: (i) an introductory half-day covering foundational concepts in nuclear security, core principles of computer security, and practical exposure to commonly used tools in network analysis (e.g., Wireshark); followed by (ii) two additional half-days dedicated to an exercise-based component based on ANS 2.0 with scenarios derived from the simulator use in Brazil's Cyber Guardian Exercise over the years [5]. The practical sessions are intended to consolidate concepts through guided tasks that mirror realistic workflows in monitoring, identifying, and interpreting security-relevant events in networked environments, while keeping the scope aligned with the students' academic level and the nuclear domain context. The main challenge for this activity is balancing the complexity of a computer security exercise context with the specific background of the students, who have a clear understanding of nuclear facilities and nuclear safety and security in general, but lack deeper understanding of several relevant computer topics (like networking, protocols, etc.) and computer security. Stage (i) was envisioned to present the basic concepts and tools and reduce the students' knowledge gap.

4. CROSS-INSTITUTIONAL COMPARISON, LESSONS LEARNED, AND FUTURE DIRECTION

Across all five institutions, ANS 2.0 supported experiential learning that would be difficult to achieve using IT-only cyber ranges or abstract classroom instruction. Common benefits included visualization of cyber-physical consequences (e.g., reactor power and steam generator pressure changes), engagement of students without nuclear backgrounds, and facilitation of interdisciplinary discussion. The deployment flexibility of ANS 2.0 enabled a variety of implementations to best support institutional missions, learner populations, and course durations. Full-semester deployments enabled deeper assessment and iterative skill development, while short-format events demonstrated that meaningful learning gains could be achieved even within limited timeframes. Institutions with primarily non-nuclear student populations emphasized protocol literacy and detection concepts, whereas nuclear-focused programs leveraged ANS 2.0 to include the exploration of operational and safety implications.

Key lessons from the pilot include the importance of early simulator engagement, the need for scaffolding for non-nuclear learners, and the value of aligning scenarios with explicit learning objectives. ANS 2.0 proved adaptable across educational formats and disciplines, supporting its use as a shared INSEN resource.

Future work will focus on modular curriculum development, expanded assessment instruments, and accelerating access to ANS 2.0 for additional Member State institutions via INSEN. These efforts aim to strengthen nuclear cybersecurity workforce development through scalable, hands-on education.

REFERENCES

[1] CHOWDHURY, N., GKIOLIOS, V., Cyber security training for critical infrastructure protection: a literature review, Comput. Sci. Rev. 40 (2021) 100361.

[2] BUSQUIM E SILVA, R., SMITH, P., BERMAN, G., MOUTENOT, L., MARQUES, R., EL-KHATIB, K., NOLAN, H., "Outcomes from the use of a security information and event management tool for operational technology in a computer security exercise", Proceedings of the Institute of Nuclear Materials Management, INMM, 65th Annual Meeting (2024).

[3] ALLISON, D., SMITH, P., MCLAUGHLIN, K., ZHANG, F., COBLE, J., BUSQUIM E SILVA, R., "PLC-based cyber-attack detection: a last line of defence", International Conference on Nuclear Security: Sustaining and Strengthening Efforts, IAEA, Vienna (2020).

[4] ZERPHY, M., MEYERS, G., BEAMER, J., DUNBAR, R., MYATT, K., "Nuclear cybersecurity education using Asherah and ARCADE simulation environments", 14B, presented at the Institute of Nuclear Materials Management 66th Annual Meeting, Portland OR, 2025.

[5] BUSQUIM E SILVA, R.A., CORREA, D.A., ANTUNES, F.R., SOUZA, F.C.S., PIQUEIRA, J.R.C., MARQUES, R.P., "The Asherah Nuclear Power Plant Simulator (ANS) as a training tool at the Brazilian Cyber Guardian Exercise", International Conference on Nuclear Security: Sustaining and Strengthening Efforts, IAEA, Vienna (2020).