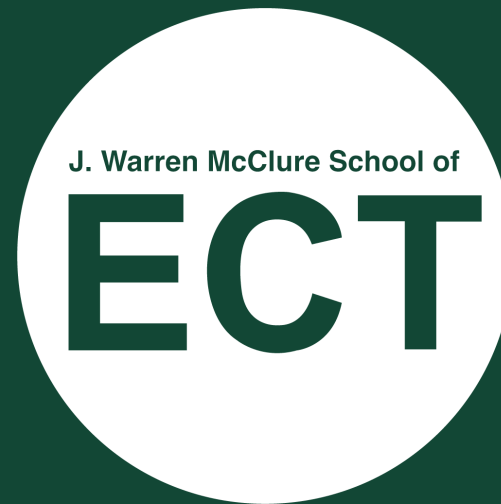


# A Standards-Driven Curriculum for Securing the Network Convergence of Operational Technology (OT) and Information Technology (IT) Infrastructure



*Dr. Rishabh Das*

*Prof. Bruce Tong*

*Prof. Brandon Saunders*

# IT vs OT

IT

## Information Technology

### FORMAL DEFINITION

*"Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency."*

— FIPS 200 (40 U.S.C. §1401)

In other words:

**Anything whose job is to handle information.**

OT

## Operational Technology

### FORMAL DEFINITION

*"A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems."*

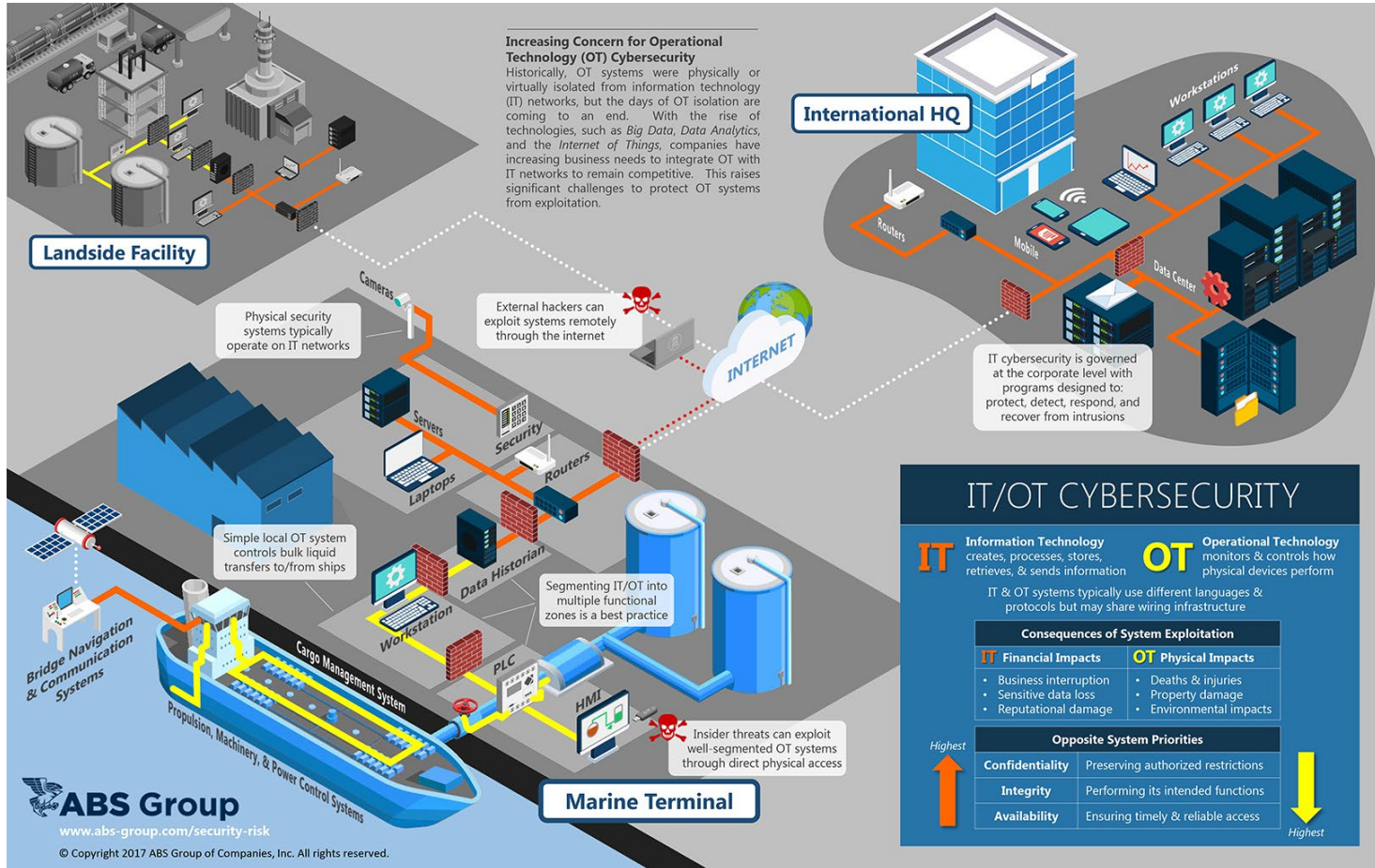
— NIST SP 800-82 Rev. 3

In other words:

**Anything whose job is to sense or move something in the real world.**

**The dividing line is FUNCTION, not hardware.** The same Windows PC is IT in an office and OT on a plant floor. What decides it is whether the machine touches the physical process.

# Brief note on Network Convergence



- A security weakness in Information Technology (IT) Operational technology (OT) interconnection can enable attackers to laterally pivot from enterprise IT into OT systems like manufacturing plants, power plants, and water utilities.
- The attacker can eventually cause disruption in the physical environment, resulting in loss of life or destruction of property.
- With nearly **48% of networking roles** demanding proficiency in OT or IT security frameworks, the current workforce remains ill-equipped to meet industry needs (Ramezan et al., 2023).
- Thus, there is a **critical need** for a workforce of network-focused cybersecurity professionals with direct **familiarity** and **hands-on experience** implementing formal standards (Dkaidek et al., 2024, Yar et al., 2024)

# Teaching OT security is challenging due to the lack of accessible testbeds

## 1 **Hardware is expensive and single-purpose**

A PLC, HMI and RTU bench serves a handful of students at a time. A cohort of forty cannot share one rack, and the rack teaches one configuration.

## 2 **Vendor lock-in**

Real engineering software is licensed and vendor-specific. Teaching on one vendor's stack teaches that vendor, not the underlying principles or the standards.

## 3 **You cannot break it safely**

The pedagogically valuable exercises: inject, disrupt, recover can damage equipment or void support agreements.

## 4 **There is no maintenance window**

Continuous processes are not available for a Tuesday afternoon lab. Industry partners cannot lend production access on an academic timetable.

## 5 **The protocols are absent from standard labs**

Modbus/TCP, DNP3 and other industrial protocols do not appear in conventional networking curricula or in the equipment most programmes already own.

## 6 **Faculty expertise is concentrated in IT**

Most cybersecurity instructors come from enterprise IT backgrounds. Without a prepared environment, delivering OT content is a research project per instructor.

# Virtualized Industrial Control System environment

## A portable virtual ICS testbed

The testbed provides virtualized programmable logic controllers, HMI software and simulated physical processes.

It runs on a standard desktop, so it travels to a student's own laptop and to another institution without a procurement cycle.

Network layers use open-source tooling: GNS3, pfSense, VyOS with real Windows and Linux nodes.

## Three environments already delivered

Pharmaceutical manufacturing line - browser-based, Module 1

HVAC control loop, full 24-hour cycle - browser-based, Module 1

Advanced water tank - desktop, for monitoring, incident response and capstone work

The web browser-based simulations removes the installation barrier, and introductory classes can use them to provide hands-on experience to the students.

**The Ohio University data center can support 450+ parallel hands-on lab session. This was not possible with physical testbeds**

# Project at a glance

**10**

## REUSABLE MODULES

20 lectures and 10 hands-on lab exercises

**7**

## TARGET COURSES

Core requirements of the cybersecurity operations degree

**300**

## STUDENTS REACHED

Expected at Ohio University over the project period

**4**

## PROJECT GOALS

Curricular · Replication · Effectiveness · Dissemination

### Develop Virtual Industrial

Stand up a portable virtual critical infrastructure testbed (e.g., water tank/pipeline) so students can practice mitigating Information Technology and Operational Technology risks.

### Industry advisory board

American Electric Power · KeyBank · Progressive Insurance · Ohio Governor's Cybersecurity Office

First curriculum review scheduled for Fall2026

### Multi-Channel Dissemination

Disseminate our results through the Consortium of Cybersecurity Clinics, peer-reviewed publication, a website, and a cybersecurity podcast

# Module Design

# Module Structure: Aligned to Bloom taxonomy

## Progressive by design

Introductory courses build foundational knowledge at the lower Bloom levels (remember, understand). Advanced courses target apply, analyze, evaluate and create.

## Iterative by design

Foundational concepts repeat across several courses.

## Complete learning package

Each module carries lecture content referencing specific NIST publications, case studies and a hands-on.

## Realistic environment

Labs use GNS3 for topology emulation, pfSense for perimeter security and VyOS for enterprise routing, with real Windows and Linux nodes and a portable virtual ICS testbed that runs on a standard desktop.



**Additional Mapping:** We also map the modules to CAE-CD Knowledge Units, and NICE work roles to enable broader impact on the cybersecurity community

# Every module is anchored to NIST publications

- The ten instructional modules draw from eleven NIST publications.
- NIST SP 800-82 Rev. 3 and the NIST Cybersecurity Framework serve as the unifying thread across the sequence, providing a consistent foundation for industrial control system security, risk management, and cybersecurity best practices.
- The remaining NIST publications support specific technical and operational topics within individual modules.

|                                      |             |             |             |         |         |            |             |            |             |         |          |
|--------------------------------------|-------------|-------------|-------------|---------|---------|------------|-------------|------------|-------------|---------|----------|
| M1 IT-OT convergence & risk          | •           |             |             |         | •       |            |             |            |             |         | •        |
| M2 ICS architecture & guidelines     | •           | •           |             |         | •       |            |             |            |             |         |          |
| M3 Converged networking fundamentals |             | •           | •           | •       |         |            |             |            |             |         |          |
| M4 Architecture & segmentation       |             |             | •           | •       | •       |            |             |            |             |         |          |
| M5 Controls & detection              | •           | •           |             |         | •       |            |             |            |             |         |          |
| M6 Secure remote access              | •           |             | •           |         |         |            | •           |            |             |         |          |
| M7 Zero Trust Architecture           | •           |             |             |         |         | •          |             |            |             |         |          |
| M8 Monitoring & metrics              | •           |             |             |         |         |            |             | •          | •           |         |          |
| M9 Incident response & recovery      |             |             |             |         | •       |            |             |            |             | •       | •        |
| M10 Capstone design project          | •           | •           |             |         |         |            |             |            |             |         | •        |
|                                      | SP 800-82r3 | SP 800-53r5 | SP 800-41r1 | CSWP 28 | IR 8183 | SP 800-207 | SP 800-77r1 | SP 800-137 | SP 800-55v1 | IR 8219 | CSF Core |

# Three interactive OT environments built

These bring cyber-physical systems into the classroom without requiring physical infrastructure.

## Pharmaceutical manufacturing line

**Prof. Bruce Tong · Module 1**

Browser-based simulation of a realistic OT production environment, hosted on the McClure School Interactive Zone.

<https://www.its.ohio.edu/tong/iz/pharma/index.html>

## HVAC control loop

**Prof. Bruce Tong · Module 1**

Full 24-hour heating and ventilation cycle; students interact with every element of the OT control loop.

<https://www.its.ohio.edu/tong/iz/control-loop/index.html>

## Advanced water tank

**Dr. Rishabh Das · Later modules**

For monitoring, incident response and capstone work. Water systems are among the most cited critical-infrastructure targets.

Desktop application

# Three interactive OT environments built 2

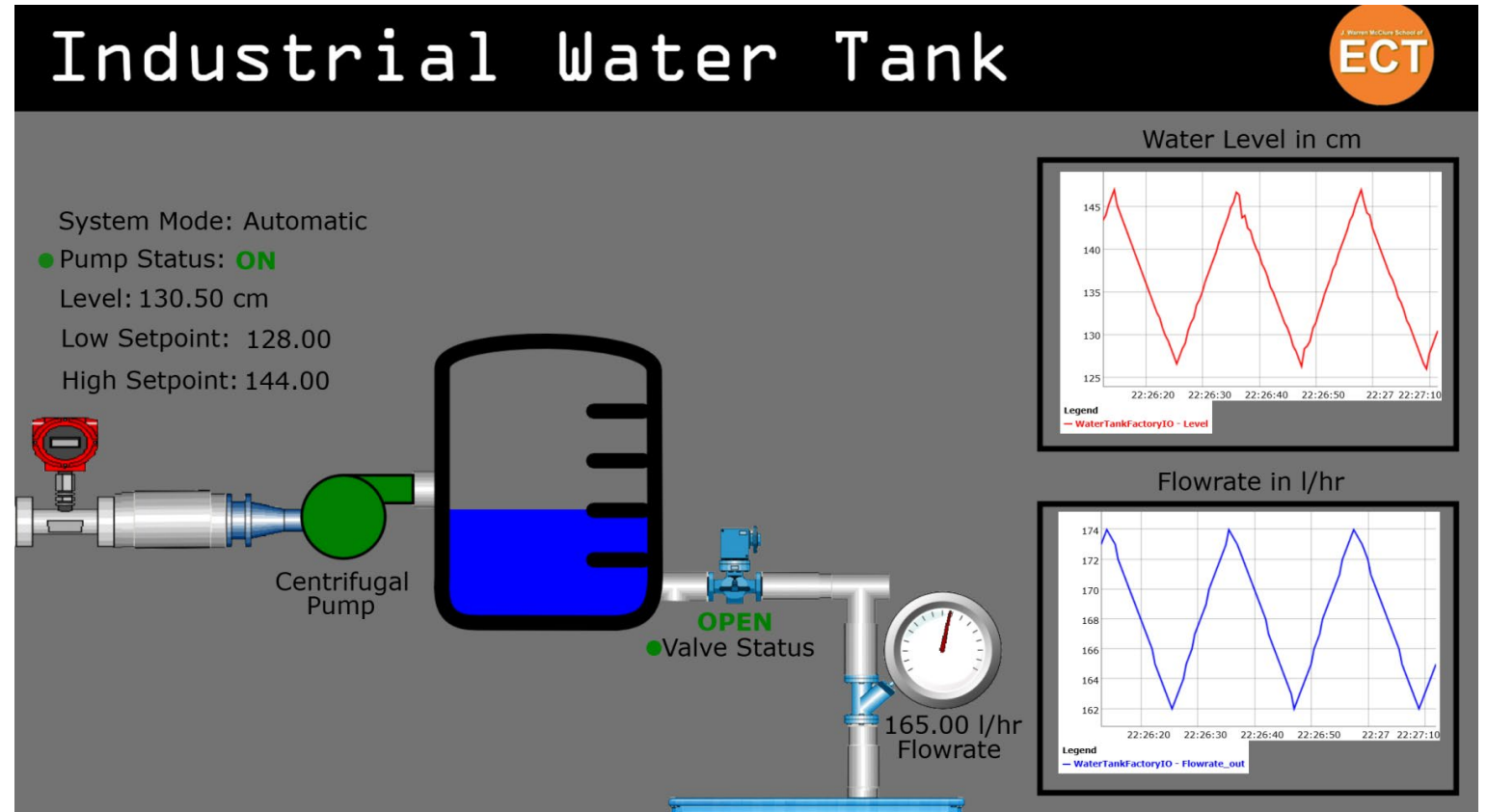
These bring cyber-physical systems into the classroom without requiring physical infrastructure.

## Advanced water tank

Dr. Rishabh Das • Later modules

For monitoring, incident response and capstone work. Water systems are among the most cited critical-infrastructure targets.

Desktop application



# Three interactive OT environments built 3

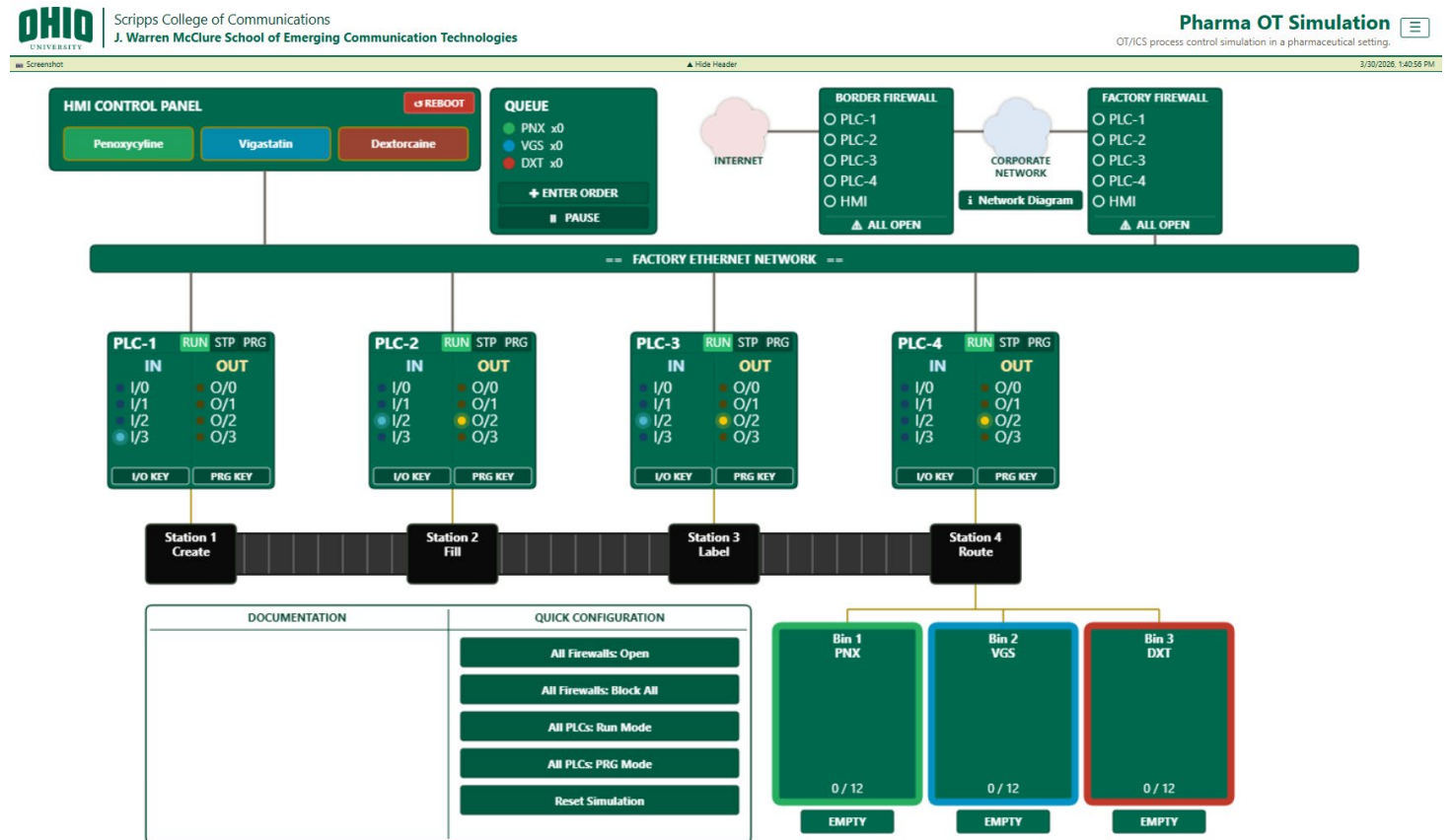
These bring cyber-physical systems into the classroom without requiring physical infrastructure.

## Pharmaceutical manufacturing line

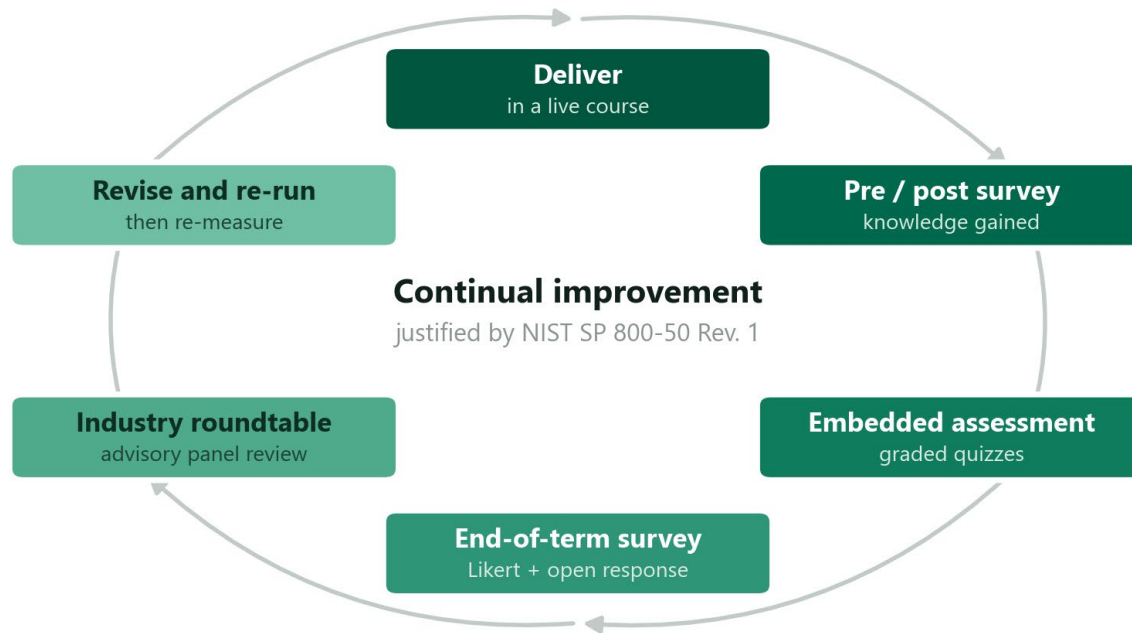
Prof. Bruce Tong · Module 1

Browser-based simulation of a realistic OT production environment, hosted on the McClure School Interactive Zone.

[its.ohio.edu/tong/iz/pharma](https://its.ohio.edu/tong/iz/pharma)



# Evaluation loop to refine Modules



|                                                                               | TARGET   |                                                    |
|-------------------------------------------------------------------------------|----------|----------------------------------------------------|
| <b>Student performance improvement</b><br>pre / post instructional survey     | ≥ 25%    | 60–87% in the Spring 2026 pilot                    |
| <b>Module-specific assessment average</b><br>embedded quizzes and assignments | ≥ 80%    | first measurement due with the next delivery       |
| <b>Student satisfaction rating</b><br>end-of-term Likert survey               | ≥ 4 of 5 | first measurement due with the next delivery       |
| <b>Industry recommendations implemented</b><br>advisory roundtable minutes    | ≥ 85%    | first review cycle will be scheduled for Fall 2026 |
| <b>Modules through a refinement cycle</b><br>project evaluation report        | 100%     | revision follows each term of delivery             |
|                                                                               | Measured | Scheduled                                          |

## Evaluation Loop:-

- Every term of delivery generates three kinds of student evidence. Additionally, the team will collect feedback from an industry review.
- Feedback is translated into content changes. The revised module is re-run the following term and measured again.
- Every refinement and its rationale goes into the project evaluation report, and the updated module is re-uploaded to the public site.

# Project timeline

# Project timeline 2

## G1 Curricular Goal

- a. Course template, lab setup, stakeholder alignment
- b. Instructional material and hands-on labs
- c. Integrate and deliver courses

## G2 Replication Goal

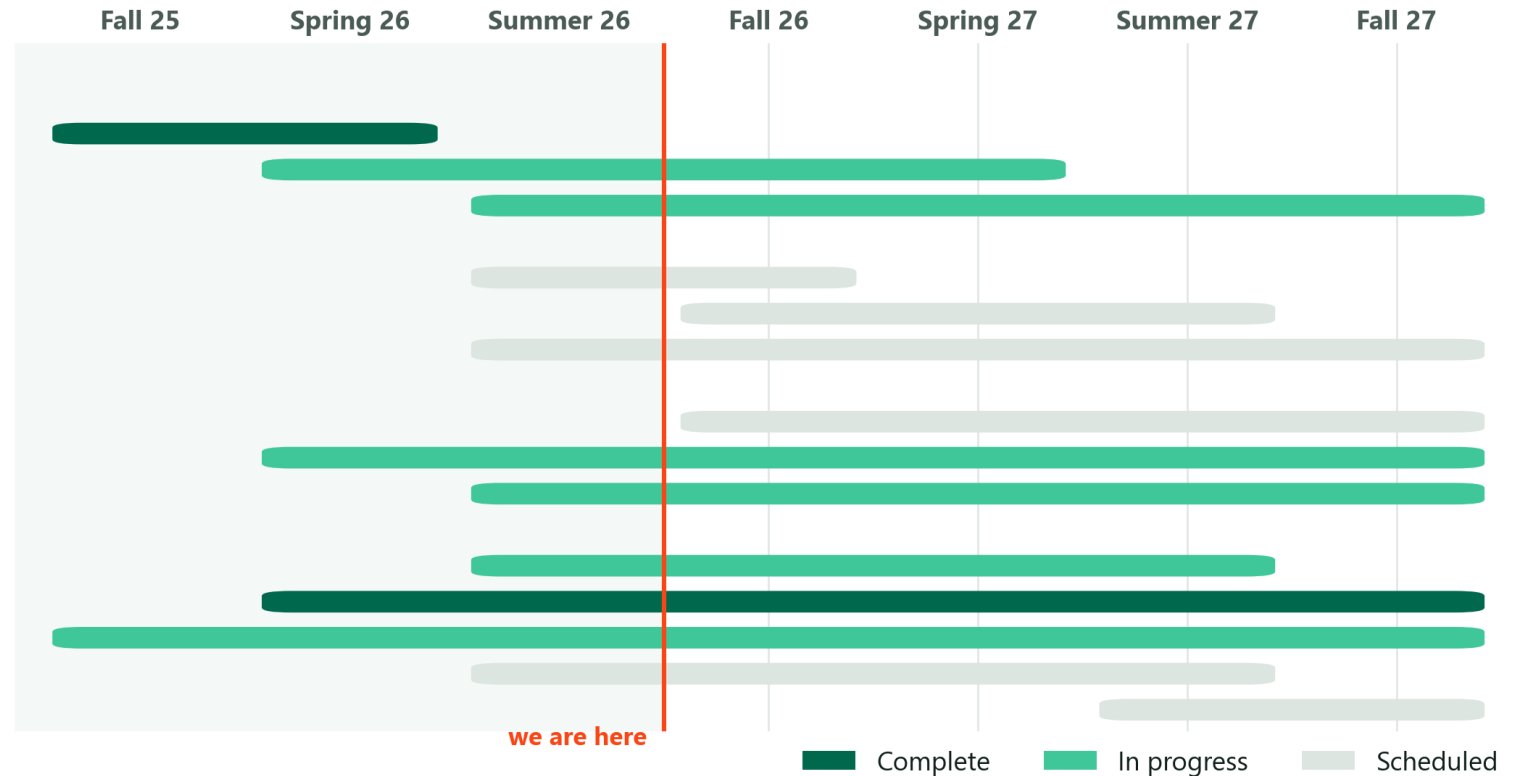
- a. Map modules to Bloom's, CAE-CD KUs, NICE work roles
- b. Train-the-trainer videos and documentation
- c. Document OHIO integration experience

## G3 Educational Effectiveness Goal

- a. Gather feedback from industry leaders
- b. Gather continual student feedback
- c. Continual improvement and documentation

## G4 Dissemination Goal

- a. Share content with Consortium of Cybersecurity Clinics
- b. Develop and maintain project website
- c. NIST workshops and publication
- d. Two podcast sessions
- e. Final summary paper



# Student evaluation

# The modules have reached the classroom at scale

These bring cyber-physical systems into the classroom without requiring physical infrastructure.

**148**

**STUDENTS TAUGHT**

Across 4 courses in Spring 2026

**101**

**STUDENTS ENROLLED**

Across 3 courses in Fall 2026

**83%**

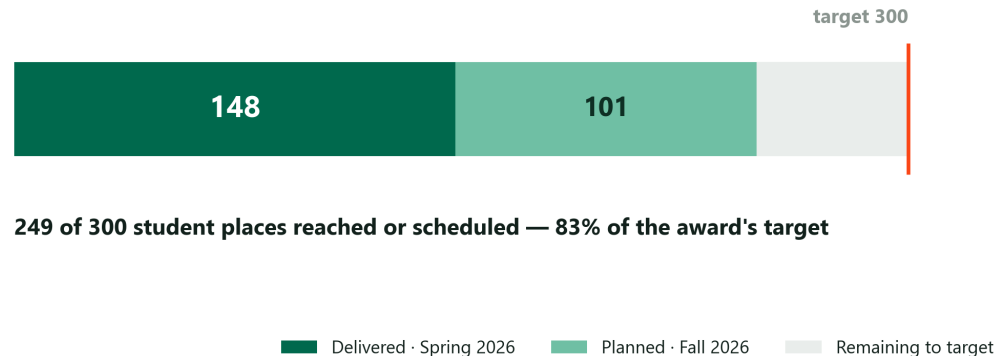
**OF THE AWARD TARGET**

249 of the 300 students the proposal committed to reach

**6 of 10**

**MODULES IN USE**

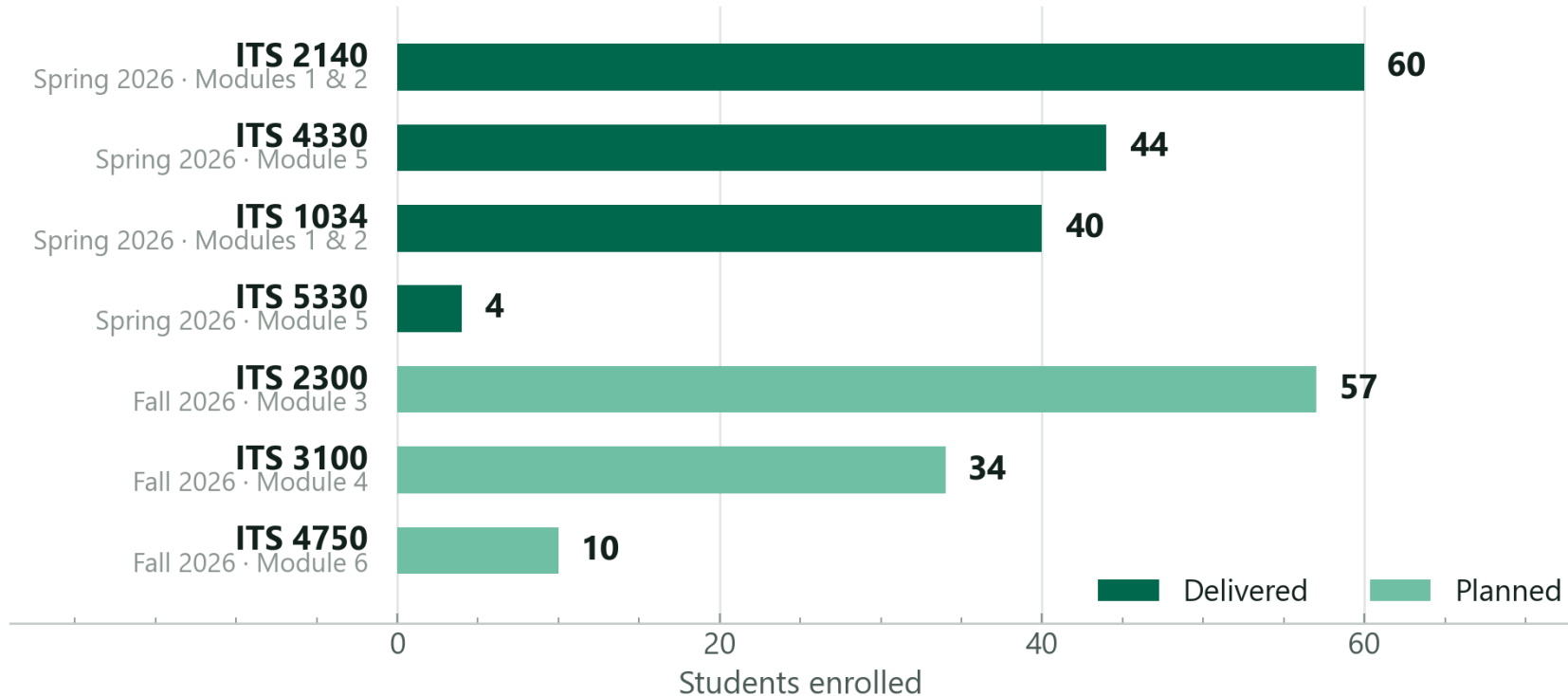
Modules 1-6 have run or are scheduled; 7-10 are scheduled for Spring 2027 delivery



*"Students" counts course enrolments; a student taking two of these courses is counted in both.*

# Module integration across ITS courses

These bring cyber-physical systems into the classroom without requiring physical infrastructure.



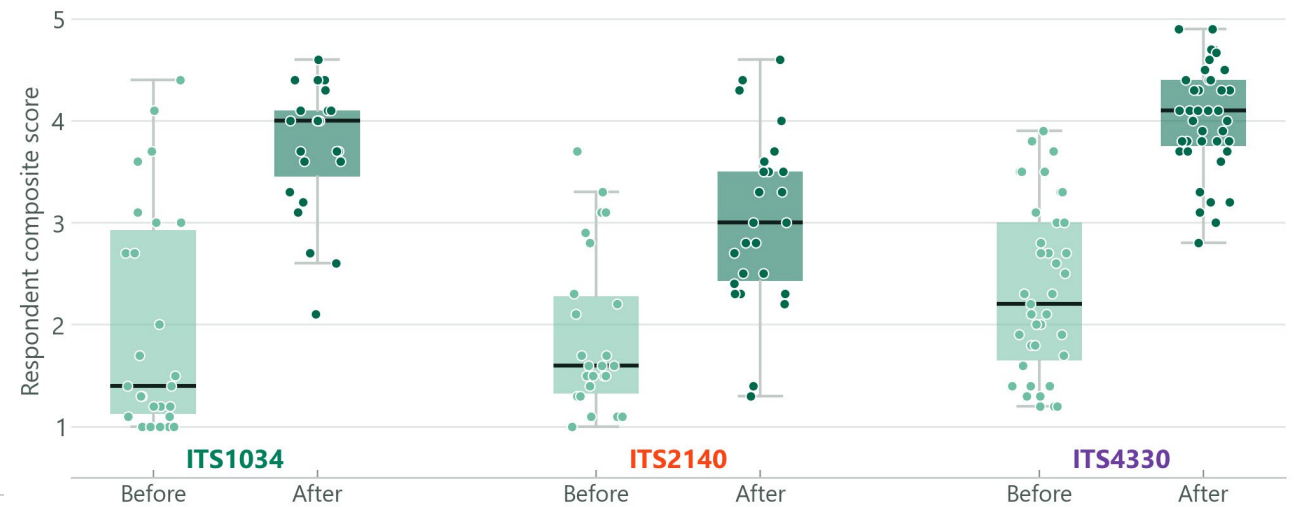
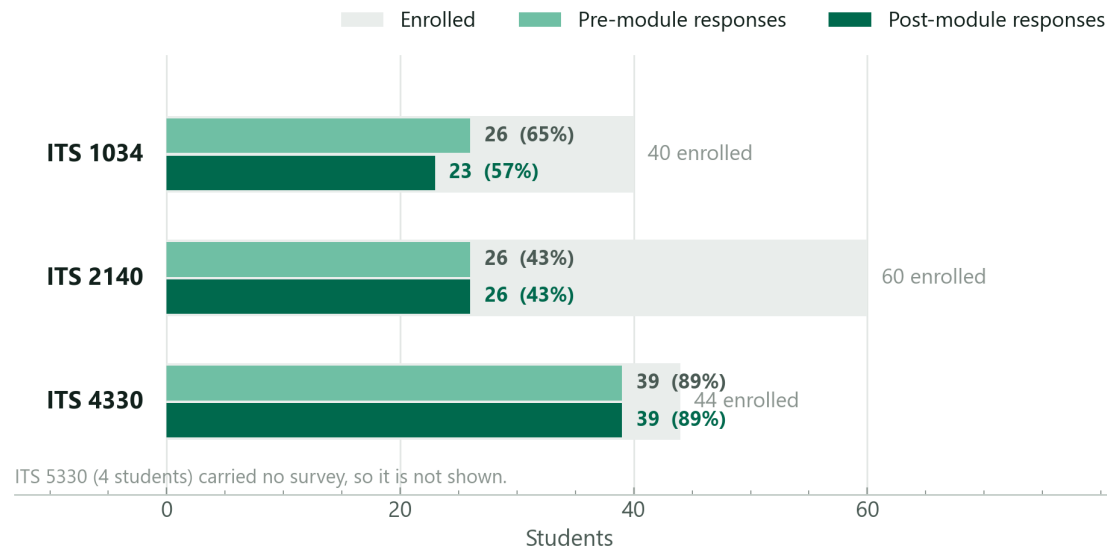
## Module Integration and delivery

- Spring 2026 delivered the modules to **148 students across four courses**, from the introductory level through to a graduate section.
- **Fall 2026 adds 101 more across three further courses.**
- Seven distinct courses now carry module content
- ITS 5330 is the graduate section paired with ITS 4330; both took Module 5 in the same term.

*"Students" counts course enrolments; a student taking two of these courses is counted in both. Delivery record supplied by the project team, September 2026.*

# Results from Spring 2026 Student evaluation

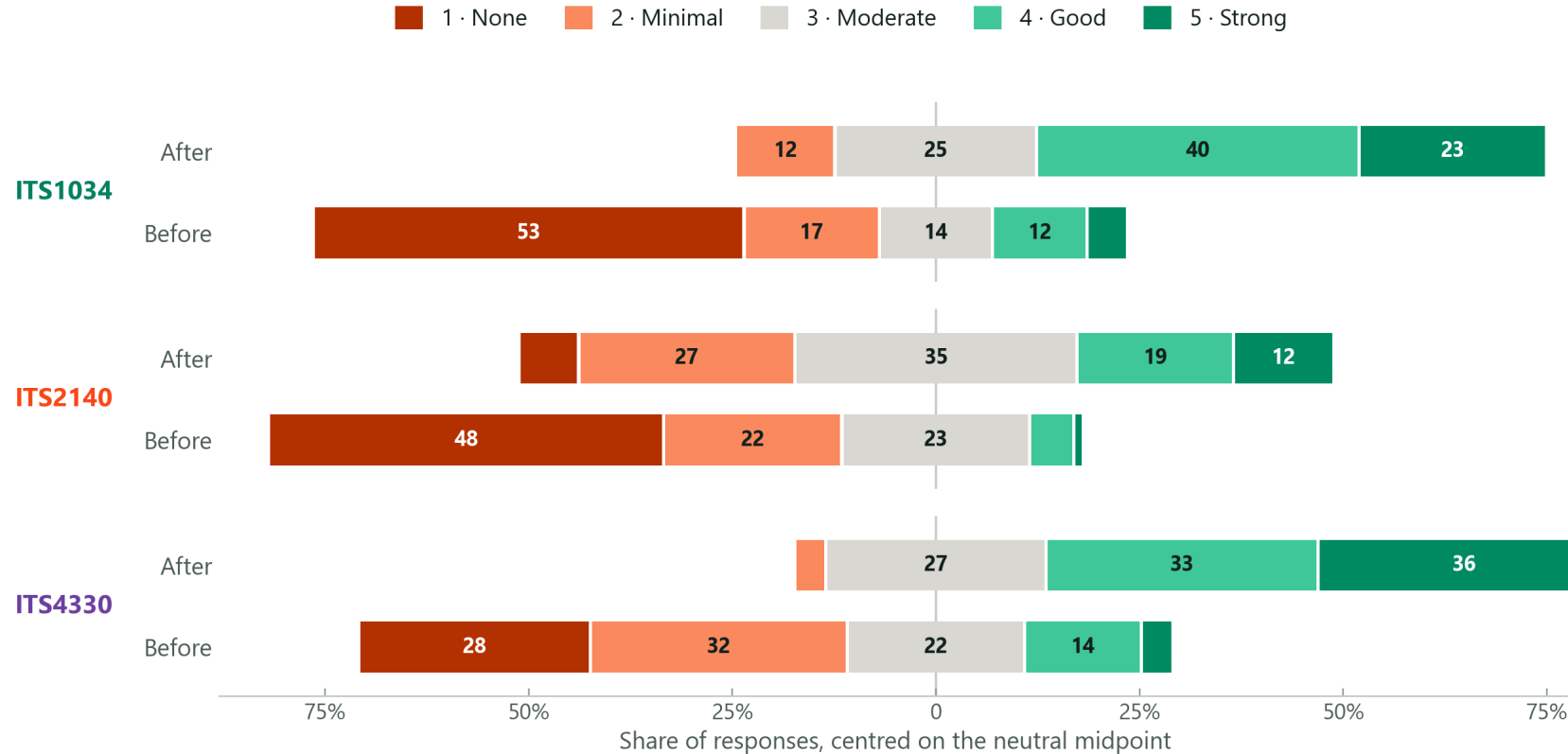
The Spring 2026 results in this deck are based on the students who responded



*Pre and post responses are unlinked, so all comparisons remain independent-samples.  
Spring 2026 knowledge surveys.*

# Results from Spring 2026 Student evaluation 2

Bars are centered on the neutral midpoint, so movement from left to right is movement from 'no knowledge' toward 'strong knowledge'.



*Pre and post responses are unlinked, so all comparisons remain independent-samples. Spring 2026 knowledge surveys.*

# Next Steps

# The next six months

- 1 Complete the CAE-CD and NICE mapping**  
Move the draft shown today through project-team and advisory-board review (Goal 2, Objective 2.1.1).
- 2 Hold the first industry curriculum review**  
AEP, KeyBank, Progressive and the Governor's Cybersecurity Office, by end of Fall 2026.
- 3 Continue module development and delivery**  
Instructional material and hands-on labs, with continued pre/post evaluation. (All lecture materials are complete. Team is working on refining the hands-on lab exercises)
- 4 Begin podcast recording and train-the-trainer videos**  
Anchored to finalized module content. (Team performed a mock recording setup in Spring 26 to check equipment readiness)

# Thank you!