Issue 2 2025

Engineering Without Cyber Awareness Creates Safety Risks We Can't Afford

BY GEORGIANNA SHEA, D.SC., AND ELAINE LY

PE Community: Education

GEORGIANNA SHEA, D.SC.

ELAINE LY

GEORGIANNA SHEA, D.SC., IS THE CHIEF TECHNOLOGIST OF THE CENTER ON CYBER AND TECHNOLOGY INNOVATION (CCTI) AT THE FOUNDATION FOR DEFENSE OF DEMOCRACIES. SHE HAS NEARLY 30 YEARS OF EXPERIENCE ACROSS THE FEDERAL AND COMMERCIAL SECTORS. **ELAINE LY** IS AN INTERN AT THE CCTI AND IS CURRENTLY PURSUING A DOCTORATE DEGREE AT NORTHEASTERN UNIVERSITY. SHE HAS A MASTER'S DEGREE IN CYBERSECURITY IN COMPUTER SCIENCE FROM GEORGE WASHINGTON UNIVERSITY.

> "AS POWER GRIDS, WATER TREATMENT PLANTS, TRANSPORTATION SYSTEMS, AND OTHER CRITICAL INFRASTRUCTURE BECOME DEEPLY INTEGRATED WITH DIGITAL CONTROLS, THE RISKS TO PUBLIC WELFARE GROW NOT ONLY IN SCALE BUT ALSO IN COMPLEXITY.

Engineers have a formal code of ethics, as outlined by NSPE, to "hold paramount the safety, health, and welfare of the public." In today's digitally connected world, engineers must consider an expanded risk landscape that goes beyond traditional physical vulnerabilities. However, colleges and universities are failing to provide the next generation of engineers with the training they need to address threats targeting connected systems. They need "Cyber-Informed Engineering" (CIE).

Malicious actors have repeatedly demonstrated that they can use cyber means to cause dangerous effects in the real world. In 2017, the Triton malware targeted the safety instrumented systems of a petrochemical plant in Saudi Arabia, disabling the very mechanisms designed to prevent catastrophic accidents. Had operators not intervened in time to manually restore the systems, an explosion or toxic chemical release could have put thousands of lives and surrounding communities at risk.

As power grids, water treatment plants, transportation systems, and other critical infrastructure become deeply integrated with digital controls, the risks to public welfare grow not only in scale but also in complexity. Cybersecurity concerns are no longer solely the domain of IT departments. When cyber-physical systems fail, the consequences can be catastrophic.

Yet, despite these growing risks, most engineering education programs remain ill-equipped to prepare future engineers to design systems that are resilient and safe from cyber threats. Cybersecurity is often just another elective among many, and in most traditional engineering disciplines, it is barely even considered. At best, engineering curricula introduce basic programming for graphing and simulations, not the concept that malicious actors could intentionally sabotage devices. A cybersecurity elective, while informative, is not sufficient to teach students how to integrate cyber risk planning into engineering design.

Cyber-Informed Engineering is an approach that encourages engineers to integrate cyber risk considerations into their design processes. Digital elements are central to modern systems, and a deep understanding of the tolerance and resilience of these digital components is now a critical aspect of engineering. To be clear, CIE does not aim to turn engineers into cybersecurity specialists. Rather, it teaches engineers how to apply traditional engineering principles to mitigate the operational consequences of digital risks.

Integrating CIE Into Engineering Education is Essential

Integrating the concepts and principles of CIE into modern engineering education is analogous to incorporating safety and hazard analysis. Just as safety principles are embedded into engineering design, CIE extends this mindset to the digital domain, which increasingly empowers modern infrastructure. CIE is not optional, it is essential.

> THE MOST EFFECTIVE WAY TO ENSURE UNIFORM TRAINING IN THIS AREA IS BY UPDATING ABET'S ACCREDITATION CRITERIA FOR ENGINEERING PROGRAMS. ABET, A NONGOVERNMENTAL ORGANIZATION, ACCREDITS COLLEGE AND UNIVERSITY PROGRAMS IN ENGINEERING, COMPUTING, AND APPLIED SCIENCES.

Controls to provide resilience to digital risk must be integrated into engineering systems from the start. CIE concepts help engineers design systems that can withstand cyber threats without compromising performance. A CIE-enhanced curriculum would blend core engineering principles with adversarial thinking and system resilience analysis, enabling students to model potential threat vectors and apply secure-by-design strategies in control systems.

strategies in control systems.

The most effective way to ensure uniform training in this area is by updating ABET's accreditation criteria for engineering programs. ABET, a nongovernmental organization, accredits college and university programs in engineering, computing, and applied sciences. It accredits approximately 5,000 degree programs at 1,000 institutions, reaching more than 200,000 students each year. The necessary change to ABET criteria could be modest—simply adding cyber risk and CIE as core competencies. Once these are required, universities will adjust their curricula to teach future engineers how to model, analyze, and mitigate risks from malicious cyber actors.

Just as safety should not be an afterthought, education that effectively addresses cyber risk should not be relegated to piecemeal training after engineers enter the workforce. It must be embedded from the beginning. With this foundational knowledge, engineers will be able to anticipate design weaknesses that could be exploited by cyber threats and implement robust physical and digital safeguards—such as authentication protocols, network segmentation, and fail-safe mechanisms.

CIE is more than a technical approach—it is a mindset for evaluating the risks introduced by digital technologies in engineering design. It improves the resilience of critical infrastructure and ensures that engineers can continue to fulfill their ethical obligation to protect public safety.