



Nuclear Engineering Curricula Must Catch Up With Digital Instrumentation and Control

Takeshi Wozniak^{1*}, Mariana Tadesse², Nicolas Yoon³

¹Department of Science, Nejd Institute for Advanced Science, Vietnam

²Department of Science, Carpathian Academy of Science, Tanzania

³Department of Science, Mekong Academy of Science, Qatar

Article Info

Volume 1, Issue 1, 2026

[doi: 10.62715/ijnst.2026.v1.i1.pp27-32](https://doi.org/10.62715/ijnst.2026.v1.i1.pp27-32)

Received: 10 November 2025

Accepted: 12 January 2026

Published: 27 February 2026

Abstract

The instrumentation and control systems of nuclear power plants have changed more in the past three decades than any other part of the plant. Analog relays and hard-wired panels are giving way to microprocessors, programmable logic, data networks and screen-based control rooms. The safety questions this raises, among them software common cause failure, the adequacy of diversity, computer security and the design of the human-system interface, have occupied regulators and standards bodies for years. This Perspective argues that the education of nuclear engineers has not kept pace. Degree programmes remain organised around reactor physics, thermal hydraulics, materials and radiation, and typically treat instrumentation as radiation detection plus classical feedback control. The article sets out why that is no longer sufficient, identifies six areas of competence that graduates need at least in outline, and considers the objections: that the curriculum is full, that digital systems belong to other disciplines, and that employers will train. It proposes that the subject be threaded through existing courses, anchored in one required course with laboratory work, and taught jointly with electrical and computer engineering. The aim is graduates who can take part in safety arguments about digital systems, not graduates who can replace the specialists.

Keywords: Digital instrumentation and control, Nuclear engineering education, Curriculum, Software common cause failure, Computer security, Human factors

© 2026 Takeshi Wozniak et al. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

1. Introduction

A nuclear engineer who graduated in the 1980s entered plants whose protection systems were built from analog trip units, relays and dedicated wiring. The behaviour of such equipment could be followed on a drawing, its failure modes were few and well catalogued, and its independence from other systems was a matter of physical separation. An engineer graduating today will work with protection and control systems built on microprocessors or field programmable gate arrays, exchanging data over networks, configured through software tools and presented to operators on screens. The reactor physics is the same. The means by which the plant is monitored, controlled and shut down is different in kind.

* Corresponding author: Takeshi Wozniak, Department of Science, Nejd Institute for Advanced Science, Vietnam. E-mail: takeshi.wozniak@nejd.edu

© 2026 Takeshi Wozniak et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The argument of this article is that nuclear engineering curricula have responded slowly to that change, and that the gap now matters for safety and for the progress of projects. The claim is a judgement, offered from the standpoint of what regulators, standards and the published record of digital system issues demand of practising engineers. It does not rest on a survey of programmes, and readers in institutions that have already moved will recognise that the description does not fit everywhere.

2. How the Plant Has Changed

The shift to digital technology was driven first by obsolescence. Analog components became hard to obtain, and digital replacements offered self-testing, better accuracy and easier maintenance. A United States National Research Council committee examined the consequences in the 1990s and identified a set of technical issues, including software quality assurance, the potential for common-mode software failure, methods of safety and reliability assessment, human factors, and the dedication of commercial hardware and software, together with strategic concerns about the licensing process and the adequacy of the technical infrastructure ([National Research Council, 1997](#)). The list has aged well. The same topics structure the current IAEA safety guide on instrumentation and control design ([IAEA, 2016](#)) and the principal standards: IEC 61513 for system requirements, IEC 60880 for safety software, and IEEE 603 for safety system criteria ([IEC, 2011](#); [IEC, 2006](#); [IEEE, 2018](#)).

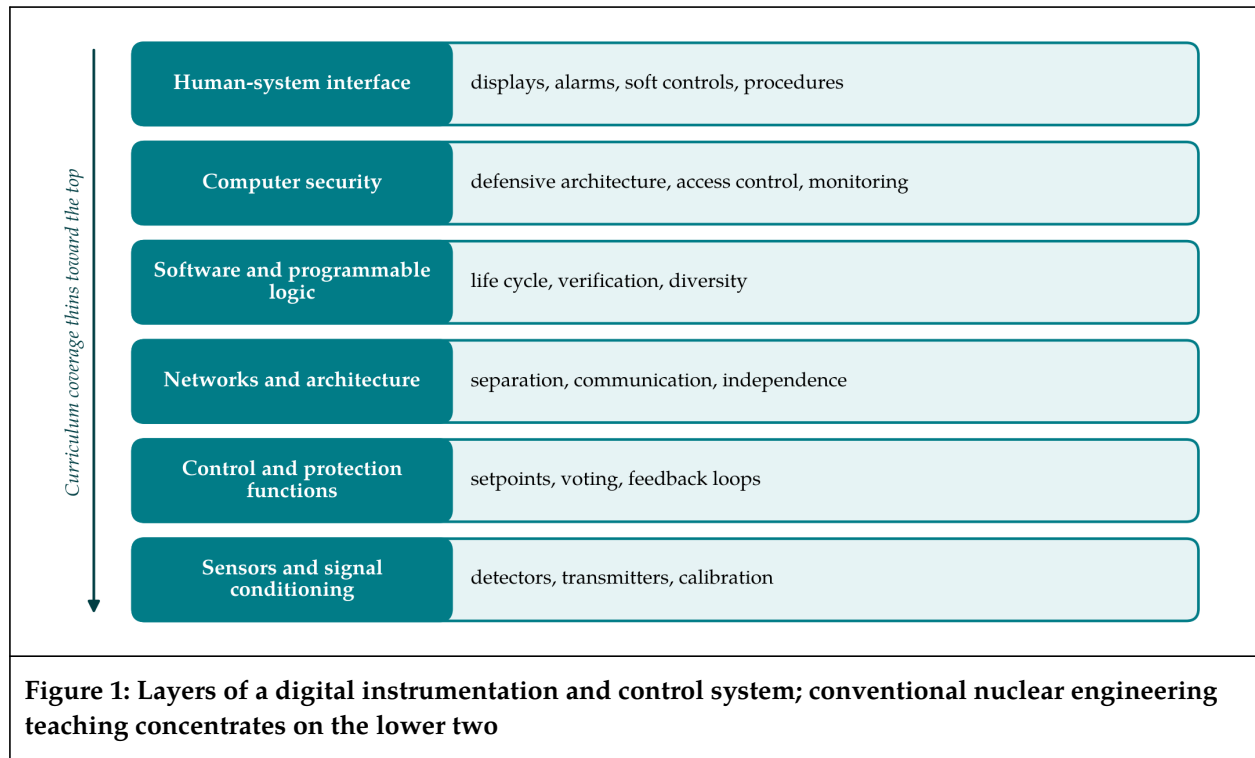
What distinguishes digital systems is that their dominant failures are failures of design. Hardware wears out randomly, and redundancy defends against that. Software does not wear out. An error in requirements or code is present in every redundant channel and will be triggered in all of them by the same input. [Leveson and Turner \(1993\)](#) showed in their study of the Therac-25 radiation therapy accidents how removing hardware interlocks in favour of software, without a corresponding safety analysis, led to fatal overdoses. The nuclear response has been defence in depth and diversity analysis, which asks whether a postulated common cause failure of the digital protection system, combined with each design basis event, can still be coped with by diverse means ([Preckshot, 1994](#); [IAEA, 2009](#)).

Two further changes complete the picture. Networked, programmable equipment can be attacked through its software, and the Stuxnet malware demonstrated that industrial controllers isolated from the internet can be reached and manipulated while reporting normal conditions to their operators ([Langner, 2011](#)). Computer security at nuclear facilities is now the subject of international guidance and national regulation ([IAEA, 2011a](#); [USNRC, 2010](#)). And the control room itself has changed, with computer-based procedures, alarm processing and soft controls that alter how crews form a picture of the plant, a subject treated in regulatory human factors review guidance ([O'Hara et al., 2012](#)).

3. What the Curriculum Still Emphasises

The intellectual core of a nuclear engineering degree was laid down when the reactor was the novel object: neutron transport and diffusion, reactor kinetics, heat removal, fuel and structural materials, shielding and radiation protection. Standard introductory texts follow that order ([Lamarsh and Baratta, 2001](#)). Instrumentation usually enters through radiation detection, taught from the physics of the detector outward ([Knoll, 2010](#)), and through a course in reactor dynamics and control built on transfer functions and point kinetics. Both are necessary. Neither says much about how a measured signal becomes a trip, through what equipment, under what rules of independence, or how one would argue that the equipment is fit for the purpose.

The IAEA's guidance on competence-based nuclear engineering curricula lists instrumentation and control among the subjects a programme should cover ([IAEA, 2014](#)), and the Agency has published a compendium of core knowledge on the topic precisely because the material is scattered and unfamiliar to many nuclear professionals ([IAEA, 2011b](#)). The existence of such a document is itself evidence of a gap between what practice requires and what degree courses typically provide. Figure 1 presents the instrumentation and control system as a stack of layers and indicates where conventional teaching is concentrated.



4. The Competence That Is Missing

Six areas stand out, summarised in Table 1. They are chosen because each corresponds to a class of question that a nuclear engineer in design, operation, safety analysis or regulation is now asked, whether or not that engineer is an instrumentation specialist.

Table 1: Areas of digital instrumentation and control competence proposed for nuclear engineering graduates		
Area	What a graduate should be able to do	Anchoring source
System architecture	Read an architecture diagram and explain separation, independence and signal paths	IAEA, 2016; IEC, 2011
Software and logic life cycle	Describe requirements, verification and validation for safety software	IEC, 2006
Common cause failure and diversity	Follow a defence in depth and diversity argument	Preckshot, 1994; IAEA, 2009
Hazard analysis	Apply a systems method to a control function and its unsafe actions	Leveson, 2011
Computer security	Explain graded protection, defensive architecture and insider threat	IAEA, 2011a; USNRC, 2010
Human-system interface	Relate interface design to crew performance and procedures	O'Hara et al., 2012

The emphasis throughout is on reasoning about systems. Much safety analysis in the nuclear curriculum is taught through failure of components: a pump stops, a valve sticks, a pipe breaks. Digital systems fail in other ways as well, through interactions that were never specified, and Leveson (2011) has argued at length that accidents in software-intensive systems are better understood as inadequate control than as chains of component failure. Graduates need at least one analytical method suited to that view alongside fault trees.

They also need an informed scepticism about diversity. It is tempting to suppose that two independently written programs will not share errors. The experiment of [Knight and Leveson \(1986\)](#) found that versions written independently to the same specification failed on the same inputs more often than independence would predict. An engineer who knows this result will ask better questions about a diverse actuation system than one who does not.

5. Objections

The first objection is that the curriculum is already full. That is true, and it is an argument about priorities, not about need. Every generation of the curriculum has displaced something, and few would now defend the hours once given to hand calculation methods that computers have long since replaced. The proposal below does not require a new specialism inside the degree. It asks for one course and for adjustments to several others.

The second objection is that digital systems are the business of electrical, computer and software engineers, and that nuclear engineers should leave the subject to them. Those disciplines do supply the specialists. But the safety case for a protection system is a nuclear safety argument. Someone must connect the behaviour of the logic to the accident analysis, decide which events demand a diverse backup, and judge whether a claimed response time preserves the fuel limits. That person needs to understand both sides, and the embedded-systems graduate has usually met neither reactor kinetics nor the design basis.

The third objection is that employers and vendors train their staff on the specific platforms they use. Platform training teaches how a product is configured. It does not teach why the standards ask for what they ask, and it reaches people after their habits of thought about safety have formed. A related worry is that anything taught will be obsolete within a few years. The products will be. The principles of independence, determinism, verification and diversity have changed little since the National Research Council report, and those are what a university should teach.

A narrower objection is that many graduates go into core design, fuel performance or radiation protection and will never work on a protection system. They will, however, rely on one in every analysis they perform. The core designer's shutdown margin, the fuel analyst's transient limits and the dose assessor's release assumptions all presuppose that signals are measured, processed and acted on within stated times and accuracies. An engineer who understands where those assumptions come from, and how they could fail, writes a better safety analysis in any specialism.

6. What Catching Up Would Involve

Three measures would close most of the gap. The first is to thread the subject through courses that already exist. A thermal hydraulics course that analyses a loss-of-flow transient can ask how the trip is generated and what delay the analysis assumes. A safety analysis course can include a common cause failure of the protection system among its postulated events. A reactor laboratory can have students trace a channel from detector to actuation device.

The second is one required course on plant instrumentation and control, covering architecture, the software life cycle, diversity, computer security and human factors at the level of Table 1, with the IAEA core knowledge publication and the principal standards as reading. Laboratory work matters here. Programming a small protection function on an industrial controller or a gate array, then trying to verify it and to defeat it, teaches what no lecture can about the distance between a specification and its implementation.

The third is to teach the course jointly with electrical and computer engineering, and to open it to their students. Mixed project teams anticipate the way the work is done in industry, and they address the second objection from both directions: the nuclear student learns what a real-time system is, and the computing student learns what a safety limit is. Simulators, which many departments already possess for reactor operations teaching, provide a natural shared platform.

7. Implications

If the argument is accepted, several parties have something to do. Departments would review where instrumentation and control sits in their programmes and who is qualified to teach it, which in many cases will mean recruiting from industry or from neighbouring departments. Accreditation bodies and professional societies could name the subject explicitly among expected outcomes. Utilities, vendors and regulators, who bear the cost of the present gap in the form of long in-house training and difficult licensing reviews, are well placed to offer case material, guest teaching and laboratory equipment.

The same reasoning extends beyond large light water reactors. Small modular and advanced designs propose higher levels of automation, multi-unit control rooms and remote monitoring, each of which moves more of the safety argument into digital systems. Engineers who will license and operate those plants are being educated now.

8. Conclusion

Digital instrumentation and control is no longer a peripheral technology in nuclear plants. It is the medium through which every safety function is initiated and every operator decision informed, and it brings failure modes that the traditional curriculum was not designed to explain. Nuclear engineering programmes do not need to produce software engineers. They need to produce graduates who can read an architecture, follow a diversity argument, recognise a security weakness and ask the right questions of the specialists. A single well-designed course, reinforced across the rest of the degree and shared with neighbouring disciplines, would go a long way toward that.

Conflict of interest

To be declared by the author(s) before publication.

Funding

To be declared by the author(s) before publication.

References

- IAEA (2009). [Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants](#). IAEA Nuclear Energy Series No. NP-T-1.5. International Atomic Energy Agency, Vienna.
- IAEA (2011a). [Computer Security at Nuclear Facilities](#). IAEA Nuclear Security Series No. 17. International Atomic Energy Agency, Vienna.
- IAEA (2011b). [Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants](#). IAEA Nuclear Energy Series No. NP-T-3.12. International Atomic Energy Agency, Vienna.
- IAEA (2014). [Nuclear Engineering Education: A Competence Based Approach to Curricula Development](#). IAEA Nuclear Energy Series No. NG-T-6.4. International Atomic Energy Agency, Vienna.
- IAEA (2016). [Design of Instrumentation and Control Systems for Nuclear Power Plants](#). IAEA Safety Standards Series No. SSG-39. International Atomic Energy Agency, Vienna.
- IEC (2006). [IEC 60880: Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions](#). International Electrotechnical Commission, Geneva.
- IEC (2011). [IEC 61513: Nuclear power plants - Instrumentation and control important to safety - General requirements for systems](#). International Electrotechnical Commission, Geneva.
- IEEE (2018). [IEEE Std 603-2018: IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations](#). Institute of Electrical and Electronics Engineers, New York.
- Knight, J.C. and Leveson, N.G. (1986). [An experimental evaluation of the assumption of independence in multiversion programming](#). *IEEE Transactions on Software Engineering*, SE-12(1): 96-109. <https://doi.org/10.1109/TSE.1986.6312924>

- Knoll, G.F. (2010). [Radiation Detection and Measurement](#), 4th edition. John Wiley & Sons, Hoboken.
- Lamarsh, J.R. and Baratta, A.J. (2001). [Introduction to Nuclear Engineering](#), 3rd edition. Prentice Hall, Upper Saddle River.
- Langner, R. (2011). [Stuxnet: Dissecting a cyberwarfare weapon](#). *IEEE Security & Privacy*, 9(3): 49-51. <https://doi.org/10.1109/MSP.2011.67>
- Leveson, N.G. (2011). [Engineering a Safer World: Systems Thinking Applied to Safety](#). MIT Press, Cambridge, MA.
- Leveson, N.G. and Turner, C.S. (1993). [An investigation of the Therac-25 accidents](#). *Computer*, 26(7): 18-41. <https://doi.org/10.1109/MC.1993.274940>
- National Research Council (1997). [Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues](#). National Academy Press, Washington, DC. <https://doi.org/10.17226/5432>
- O'Hara, J.M., Higgins, J.C., Flegler, S.A. and Pieringer, P.A. (2012). [Human Factors Engineering Program Review Model](#). NUREG-0711, Revision 3. U.S. Nuclear Regulatory Commission, Washington, DC.
- Preckshot, G.G. (1994). [Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems](#). NUREG/CR-6303. U.S. Nuclear Regulatory Commission, Washington, DC.
- USNRC (2010). [Cyber Security Programs for Nuclear Facilities](#). Regulatory Guide 5.71. U.S. Nuclear Regulatory Commission, Washington, DC.